# *Prestige 128MH*

# *User's Manual*

Version 1.0

ZyXEL

TOTAL INTERNET ACCESS SOLUTION

# *Prestige 128MH*

## PSTN Router/Hub

### Copyright

### Disclaimer

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

### Trademarks

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

# Federal Communications Commission (FCC) Interference Statement

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

1. This device may not cause harmful interference.

2. 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:

1. Reorient or relocate the receiving antenna.

2. Increase the separation between the equipment and the receiver.

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

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

**Notice 1**

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

**Notice 2**

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

## Information for Canadian Users

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

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

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

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

**Caution**

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

**Note**

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

## 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 which vary from state to state.

## Customer Support

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

### North America

**ZyXEL Communications Inc.**

4920 E. La Palma Avenue

Anaheim, CA 92807

USA

Telephone: (714) 693-0808    (call between 8:00 AM and 5:00 PM PST)

Facsimile: (714) 693-8811

E-mail:    - Sales Inquiries: sales@zyxel.com

- Technical Support: support@zyxel.com

### Worldwide Support

**ZyXEL Communications Corporation**

6, Innovation Road II, Science-Based Industrial Park

Hsinchu, Taiwan 300, R.O.C.

Telephone: 886-3-578-3942   Ext.: 266  (call between 8:00 AM and 5:00 PM [Taiwan time GMT+8:00])

Facsimile: 886-3-578-2439

E-mail:    - Sales Inquiries: sales@zyxel.com.tw

- Technical Support: support@zyxel.com.tw

## Product Information

For product information, visit our site on the **World Wide Web**: http://www.zyxel.com.

## FTP Information

Information such as ZyXEL software and ROM updates is available for download at these FTP addresses:

**North America**: ftp.zyxel.com

**Europe**: ftp.zyxel.co.at

# Table of Contents

**Chapter 4**

**Chapter 5**

**Chapter 6**

**Chapter 7**

**Chapter 8**

# List of Figures

# List of Tables

# Preface

## About Your Router/Hub

Congratulations on your purchase of the *Prestige 128MH* PSTN Router/Hub.

The *Prestige 128MH* is a high-performance bridge/router that offers a complete solution for your WAN (Wide Area Network) applications such as Internet access, multi-protocol LAN-to-LAN connections, telecommuting and remote access over regular phone lines, or PSTN (Public Switched Telephone Network).

The *Prestige 128MH* supports multi-protocol routing for TCP/IP and Novell IPX, as well as transparent bridging for other protocols. With the built-in 4-port Ethernet 10Base-T hub, you get the added benefit of eliminating the clutter caused by an external hub.

Your *Prestige 128MH* is easy to install and to configure since you do not need to set any switch. All functions of the *Prestige 128MH* are software configurable via the SMT (System Management Terminal) Interface. The SMT is a menu-driven interface that you can access from either a VT100 compatible terminal or a terminal emulation program on a PC.

## About This User's Manual

This user's manual shows you how to configure and manage your router.

This manual consists of fourteen chapters and is designed to guide you through the configuration of your *Prestige 128MH* for the various applications.

## Structure of this Manual

This manual is divided into five parts:

Step 1. *Getting Started* (Chapters 1-2) is structured as a step-by-step guide to help you connect, install and setup your *Prestige 128MH* to operate on your network.

Step 2. *The Internet* (Chapter 3) describes how to configure your *Prestige 128MH* for Internet access.

Step 3. *Setting Up Advanced Applications* (Chapters 4-8) describes how to use your *Prestige* for more advanced applications such as LAN-to-LAN connectivity for TCP/IP and Novell IPX, and transparent bridging for other protocols.

Step 4. *Management & Maintenance* (Chapters 9-13) provides information on management and maintenance facilities for network administrators.

Step 5. *Troubleshooting* (Chapter 14), provides information about solving common problems.

Regardless of your particular application, it is important that you follow the steps outlined in *Chapters 1-2* to connect your *Prestige 128MH* to your LAN. You can then refer to the appropriate chapters of the manual, depending on your applications.

## Syntax Conventions

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

# Chapter 1
# Getting to Know Your Router/Hub

This chapter describes the key features and applications of your *Prestige 128MH* PSTN Router/Hub.

## 1.1 *Prestige 128MH* PSTN Bridge Router

Your *Prestige* is a bridge/router with an integrated 4-port Ethernet 10Base-T hub and two high-speed 56K modems. The *Prestige* is ideal for everything from Internet browsing to receiving calls from remote dial-in users to making LAN-to-LAN connections to remote networks.

## 1.2 Features of *Prestige 128MH*

The following are the key features of the *Prestige* 128MH.

### *Dual Built-in 56K Modems*

Your *Prestige* 128MH features two built-in 56K high-speed modems. The built-in modems allow you to connect your *Prestige* directly to the PSTN (Public Switched Telephone Network).

### *The WAN Port*

For added expandability, the *Prestige* 128MH features a WAN port that allows you to connect a dial-up/leased line modem or an ISDN TA (Terminal Adapter) to your *Prestige.* The WAN port can be used independently, or it can be bundled with the built-in modems to support bandwidth-on-demand.

### *Multiple Protocol Support*

- ♦ TCP/IP (Transmission Control Protocol/Internet Protocol) network layer protocol.

- Novel IPX (Internetwork Packet eXchange) network layer protocol.
- Transparently bridging for unsupported network layer protocols.
- PPP/MP (Point-to-Point Protocol/Multilink Protocol) link layer protocol.
- SUA™ (Single User Account) for NAT (Network Address Translation) functionality.

### *Integrated 4-Port Ethernet Hub*

The built-in 4-port Ethernet 10Base-T hub saves you the cost and the clutter of an external hub.

### *Dial-On-Demand*

The Dial-On-Demand feature allows the *Prestige* to automatically place a call to a remote gateway based on the triggering packet's destination without user intervention.

### *PPP Multilink*

The *Prestige* can bundle multiple links in a single connection using PPP Multilink Protocol (MP). The number of links can be either statically configured or dynamically managed based on traffic demand.

### *Bandwidth-On-Demand*

The *Prestige* dynamically allocates bandwidth by dialing and dropping connections according to traffic demand.

### *Full Network Management*

Your *Prestige* supports SNMP (Simple Network Management Protocol) and allows menu-driven network management via the console port or a telnet connection. Your *Prestige* is also equipped with a Call Detail Record to help to analyze and manage your telephone bill.

### *RADIUS Support*

RADIUS (Remote Authentication Dial-In User Service) is the most popular protocol for user authentication on dial-up lines. RADIUS support allows you to use an external server for unlimited number of users and the ease of centralized management.

### *PAP and CHAP Security*

The *Prestige* supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms.

### *DHCP Support*

DHCP (Dynamic Host Configuration Protocol) allows the workstations on your LAN to obtain the configuration from the *Prestige* at start-up.

### *Call Control*

Your *Prestige* provides budget management for outgoing calls and maintains a blacklist for unreachable phone numbers in order to save you the expense of unnecessary charges.

### *Data Compression*

Your *Prestige* incorporates Stac data compression to speed up data transfer. Stac is the de facto standard of data compression over PPP links.

### *Networking Compatibility*

Your *Prestige* is compatible with remote access products from other manufacturers such as Ascend, Cisco, and 3Com. Furthermore, it supports Microsoft Windows 95 and Windows NT remote access capability.

## 1.3 The Built-In Modems

The built-in modems are capable of maximum throughput of 56 Kilobits per second (kbps). Please note that due to the local telephone regulations and the line quality of your local loop, your *Prestige* may or may not achieve the theoretical maximum throughput.

The modems support either K56flex™ or X2™ standard, depending on the modem module installed in your *Prestige*. In either case, the modem is firmware upgradable to V.90, which is the latest international standard sanctioned by the ITU (International Telecommunication Union). Please visit ZyXEL’s web site at *www.zyxel.com* for the availability of the firmware upgrade for your model.

Modems of either model also support V.42bis compression to speed up data transfer.

### 1.3.1 WAN Terminology

- **DCE & DTE**

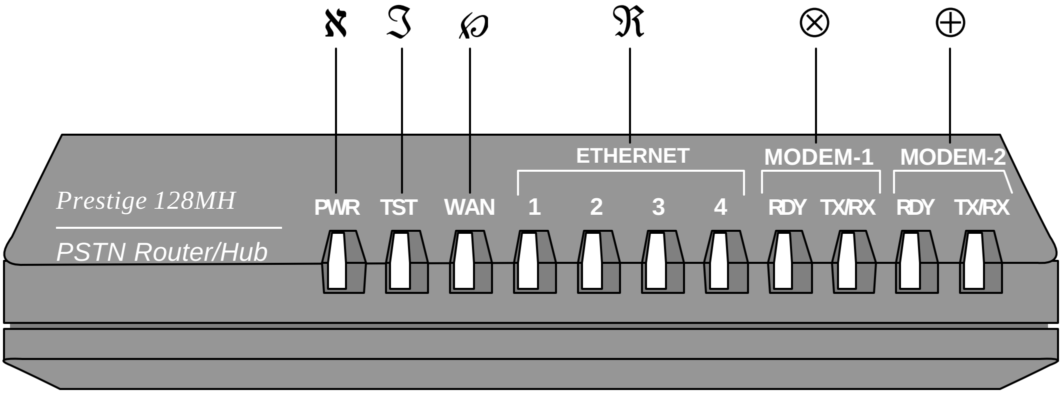
On the two ends of an RS-232 connection, the equipment closest to the telephone line is called the DCE (Data Communications Equipment) and the other the DTE (Data Terminal Equipment). In our case, the modem or the ISDN TA is the DCE, and the *Prestige* is the DTE.

- **PSTN & POTS**

Collectively, the interconnected network of the voice grade networks of the individual telephone companies is called PSTN (Public Switched Telephone Network), and a regular telephone line is often referred to as a POTS (Plain Old Telephone Service) line.

# 1.4 Front Panel LEDs and Back Panel Ports

## 1.4.1 *Prestige 128MH* Front Panel



ℵ : PWR = Power Indicator

ℑ : RUN = Running status Indicator (Blinking)

ℜ : ETHERNET (1, 2, 3, 4) = 4-port 10Base-T hub (active Ethernet port #)

℘ : WAN = WAN port ready, transmit/receive

⊗ : MODEM-1 (RDY, TX/RX) = Internal Modem-1 ready, transmit/receive

⊕ : MODEM-2 (RDY, TX/RX) = Internal Modem-2 ready, transmit/receive

**Figure 1-1. *Prestige 128MH* Front Panel LEDs**

### 1.4.2 Front Panel LEDS

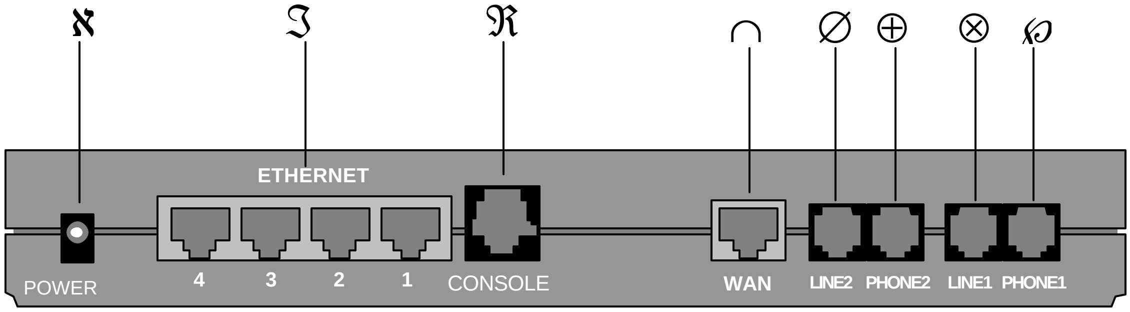
The LED indicator lights on the front panel of your *Prestige* indicate the router/hub functional status. The following Table 1-1 describes the LED functions:

**Table 1-1. LED Functions**

| **LEDs** | | **Function** | **Indicator Status** | **Active** | **Description** |
|---|---|---|---|---|---|
| PWR | | Power Indicator | Green | On | The *Prestige* is powered on. |
| RUN | | Running status indicator | Green | Blinking | The *Prestige* is functioning properly. |
| WAN | | Ready | Green | On | The modem or IDSN TA connected to WAN port is ready for service. |
| | | Transmit/Receive | Green | Blinking | Traffic is being transmitted or received on WAN port. |
| ETHERNET | 1,2,3,4 | LAN Transmit<br>LAN Receive | Green | On | An active station is connected to the port. |
| | | | | Blinking | The connected station is transmitting. |
| MODEM-1,2 | RDY | Ready | Green | On | The modem is ready for service. |
| | TX/RX | Transmit/Receive | Green | Blinking | Traffic is being transmitted or received on the modem. |

### 1.4.3 *Prestige 128MH* Back Panel

Figure 1-2 shows the rear panel of your *Prestige 128MH*. Refer to this diagram when making connections.



ℵ : POWER = AC power inlet.

ℑ : ETHERNET = 4 x RJ-45 Ethernet 10Base-T port (metallic).

ℜ : CONSOLE = RJ-45 console port (off-white).

℘ : PHONE1 = RJ-11 port for a phone or fax on line 1.

⊗ : LINE1 = RJ-11 port for modem 1 to wall jack.

⊕ : PHONE2 = RJ-11 port for a phone or fax on line 2.

∅ : LINE2 = RJ-11 port for modem 2 to wall jack.

∩ : WAN = RJ-45 WAN port for external modem or ISDN TA (black).

**Figure 1-2. *Prestige 128MH* Rear Panel**

## *1.5* Applications for *Prestige 128MH*

The following sections show you the possible applications that you can use your *Prestige* for.

### 1.5.1 Internet Access

The *Prestige 128MH* is the ideal high-speed Internet access solution. Your *Prestige* supports the TCP/IP protocol, which the Internet uses exclusively. It is also compatible with access servers manufactured by major vendors such as Cisco and Ascend.  A typical Internet Access application is shown in Figure 1-3.

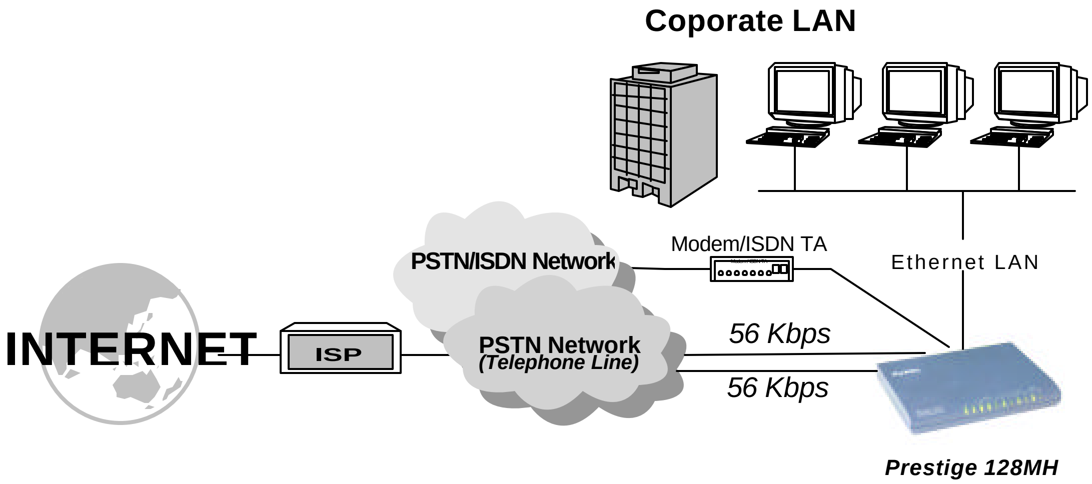


**Figure 1-3. Internet Access Application**

#### *Internet Single User Account*

For a SOHO (small office/Home Office) environment, your *Prestige* offers a Single User Account (SUA) feature that allows multiple users on the LAN (Local Area Network) to access the Internet concurrently for the cost of a single user.  Single User Account address mapping can also be used for other LAN to LAN connections.

## 1.5.2 Multi-Protocol/Multilink LAN-to-LAN Connection

You can use the *Prestige* to connect two geographically dispersed networks over the WAN connection. The *Prestige* supports TCP/IP and Novell IPX routing, as well as transparent bridging for other network layer protocols. Your *Prestige* can also bundle multiple links in a single connection for greater bandwidth. A typical LAN-to-LAN application for your *Prestige* is shown in Figure 1-4.

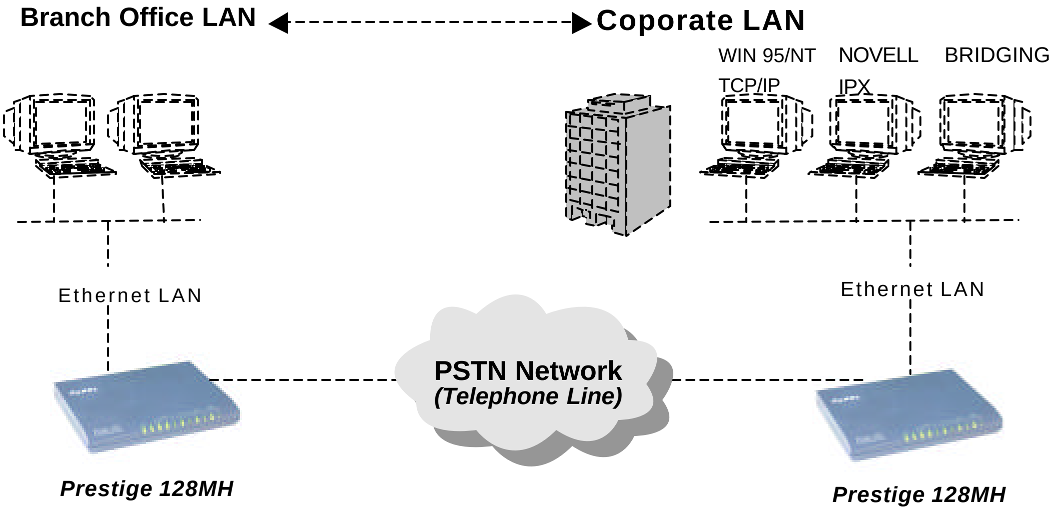


**Figure 1-4. LAN-to-LAN Connection Application**

### 1.5.3 Remote Access Server

Your *Prestige* allows remote users to dial-in and gain access to your LAN. This feature enables users that have workstations with remote access capabilities, e.g., Windows 95, to dial in to access the network resources without physically being in the office. Either PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) authentication can be used to control the access from the remote users. You can also use callback for security and/or accounting purposes. Figure 1-5 shows how a remote user can connect to the corporate office.

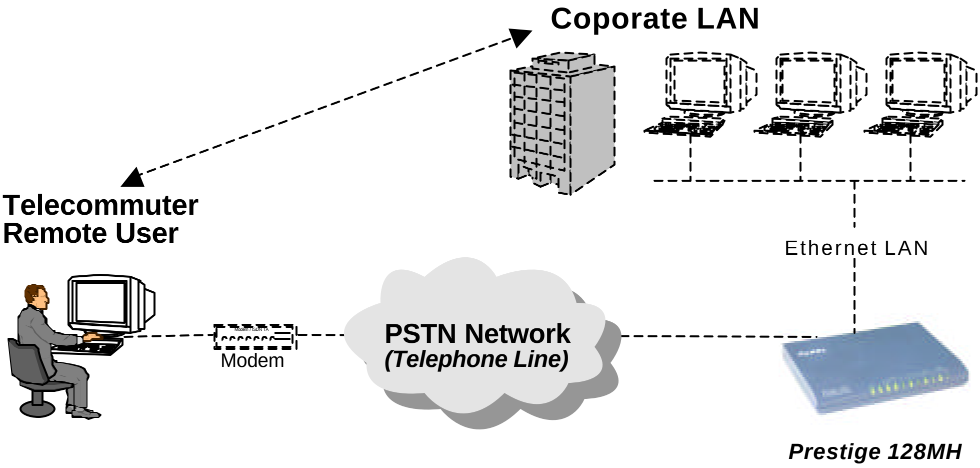


**Figure 1-5. Telecommuting/Remote Access Server Application**

# Chapter 2

# Hardware Installation & Initial Setup

## 2.1 Unpacking your Router/Hub

Before you proceed further, check all items you received with your *Prestige* against this list to make sure nothing is missing. The complete package should include:

**Table 2-1. Item Checklist**

| Package Contents | *Prestige 128MH* |
|---|---|
| *Prestige 128MH* PSTN Router/Hub | 1 |
| Power Adapter | 1 |
| RS-232 cable | 1 |
| DB-25(female)/RJ-45 console cable | 1 |
| DB-25(male)/DB-9(female) converter | 1 |
| LAN straight through cable (white tag) | 1 |
| RJ-11 PSTN telephone cable | 2 |
| Warranty Card | 1 |
| This *Prestige 128MH* User's Manual | 1 |
| Quick Start Guide | 1 |

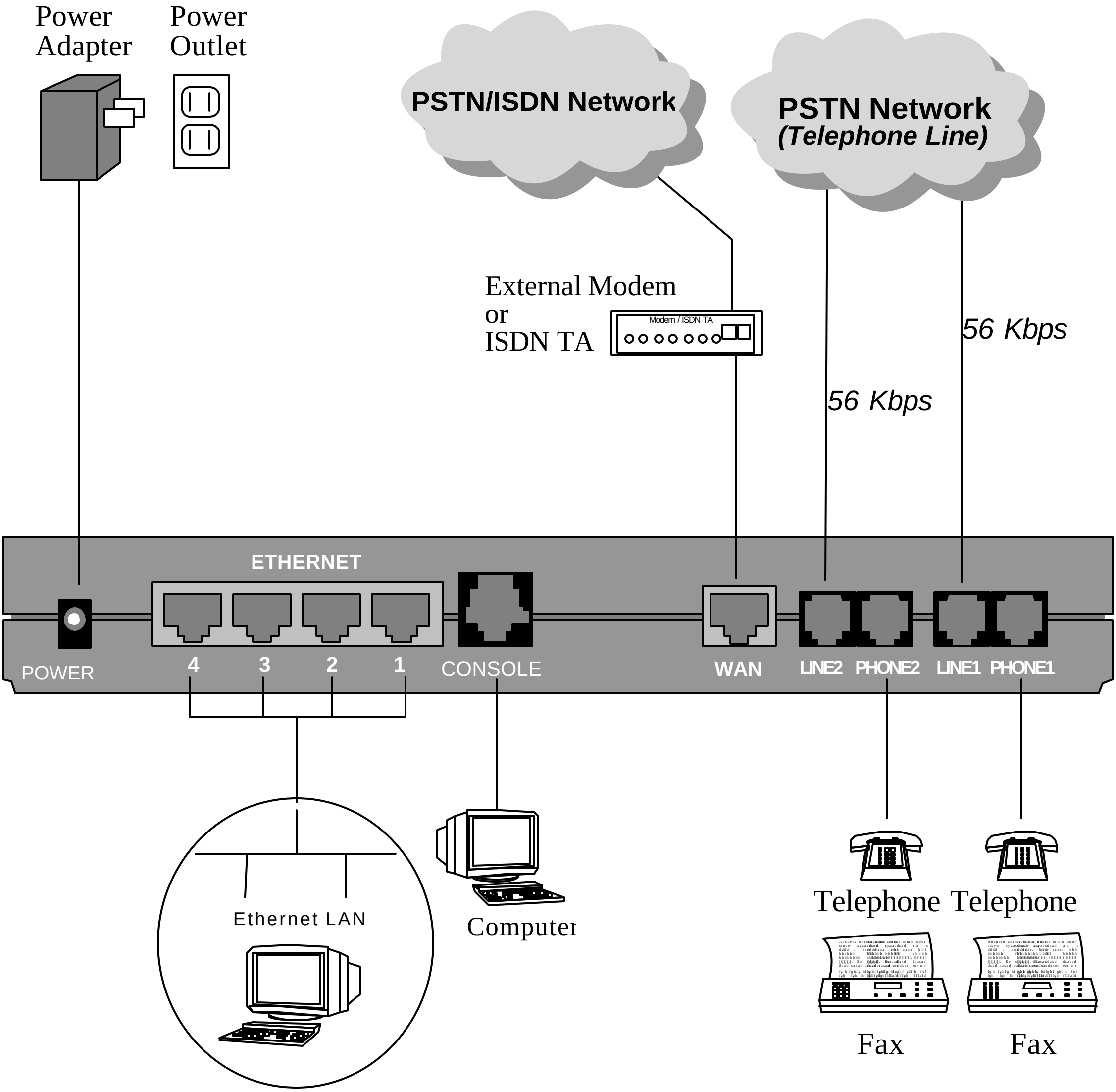
## 2.2 Additional Installation Requirements

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

- A computer with Ethernet 10Base-T NIC (Network Interface Card).
- A computer equipped with communications software configured to the following parameters:
  - VT100 terminal emulation.
  - 9600 Baud.
  - No parity, 8 Data bits, 1 Stop bit.
- An (optional) external modems or ISDN TA.

After the *Prestige* is properly set up, you can make future changes to the configuration through telnet connections.

## 2.3 Connect your *PSTN Router/Hub*



### 2.3.1 *Prestige 128MH* Connections

**Figure 2-1. Connecting *Prestige 128MH***

This section outlines how to connect your *Prestige 128MH* to the LAN and to the telephone network. Refer to Figure 1-2 to identify all of the ports on your device. Then see Figure 2-1 when you make the connections. To minimize confusion over the various RJ-45 ports, they are color-coordinated as follows:

| Port | Color |
|---|---|
| Ethernet 10Base-T Ports | Metallic |
| Modem/WAN Ports | Black |
| Console Port | Off-White |

The enclosed cables are of the same color as the ports for which they are intended, however, it is still important for you to make sure that the correct cable is used for each connection; otherwise, your *Prestige* could be damaged.

### Step 1. Connecting Your Computer to Your Prestige

For the initial configuration of your *Prestige*, you need to use a terminal emulator software on a workstation and connect it to the *Prestige* through the console port. Connect the RJ-45 end of the enclosed console cable to the console port of the *Prestige* and the other end to a serial port (COM1, COM2 or other COM port) of your workstation. Use the enclosed DB-25/DB-9 converter if necessary.

After your *Prestige* has been configured, you can modify the setup remotely through telnet connections. See *Chapter 12 - Telnet Configuration and Capabilities* for detailed instructions on using telnet to configure your *Prestige*.

### Step 2. Connecting the Modem Ports

Connect modem 1 and modem 2 to the telephone network using the included telephone cables. Plug one end of the cable into the modem port labeled LINE 1 and LINE 2 and the other to the telephone wall jack.

### Step 3. *Connecting the Phones or Faxes*

The telephone lines can be shared between the internal modems and other equipment, e.g., a telephone, an answering machine or a fax machine. Use the PHONE port to connect other telephony machines to the *Prestige*. Be sure to follow the instructions of other machines when connecting them to the *Prestige.*

### Step 4. Connecting the WAN Port (Optional)

Hook up an external modem or ISDN TA to the *Prestige* by connecting one end of an RS-232 cable to the WAN port of the *Prestige* and the other end to the DTE port of the external device. Connect the external device to the PSTN/ISDN using an appropriate cable. Please refer to the documentation of your device for connection information.

### Step 5. Connecting a Workstation to the Prestige

Connect a workstation to the built-in hub on the *Prestige* to create an Ethernet network. Connect one end of a straight through Ethernet cable to the NIC on the workstation and the other end to one of the 4 Ethernet ports. Ethernet 10Base-T networks use Unshielded Twisted Pair (UTP) cable with RJ-45 connectors that look like a bigger telephone plug with 8 pins.

### Step 6. Connect the Power Adapter to your *Prestige*

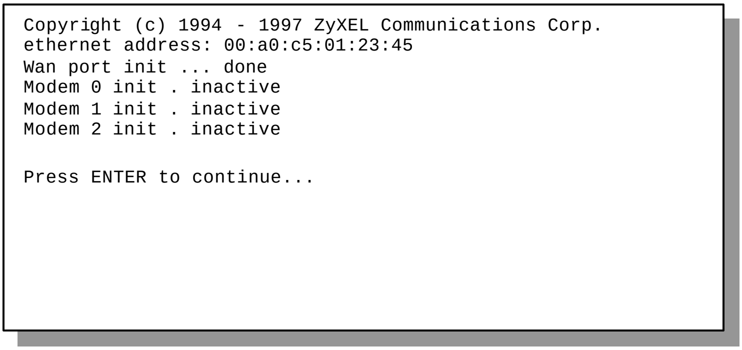
Connect the power adapter to the port labeled POWER on the rear panel of your *Prestige.*

## 2.4 Power On Your *Prestige*

At this point, you should have connected the console port, the modem ports, the WAN port, the Ethernet port and the power port to the appropriate devices or lines. You can now power on your *Prestige* by plugging the AC adapter to a power outlet of the correct voltage.

### Step 1. *Initial Screen*

When you power 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 in Figure 2-2.



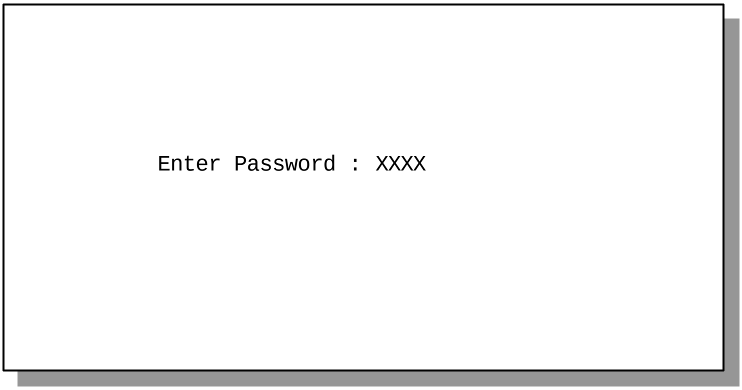
```
Copyright (c) 1994 - 1997 ZyXEL Communications Corp.
ethernet address: 00:a0:c5:01:23:45
Wan port init ... done
Modem 0 init . inactive
Modem 1 init . inactive
Modem 2 init . inactive

Press ENTER to continue...
```

**Figure 2-2. Power-On Display**

### Step 2. *Entering Password*

The login screen appears after you press Enter, prompting you to enter the password, as shown in Figure 2-3.

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



```
Enter Password : XXXX
```

**Figure 2-3. Login Screen**

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.

## 2.5 Navigating the SMT Interface

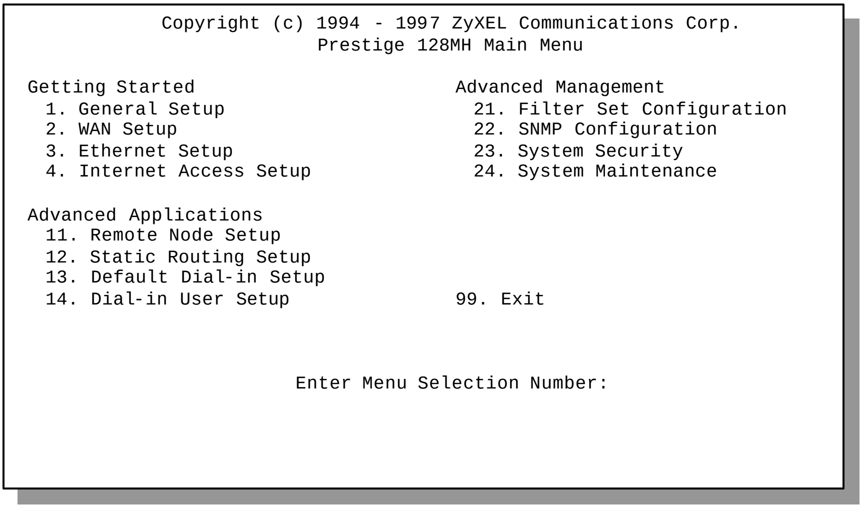
The SMT (System Management Terminal) is the interface that you use to configure your *Prestige.*

Several operations that you should be familiar with before you attempt to modify the configuration are listed in Table 2-2.

**Table 2-2. Main Menu Commands**

| **Operation** | **Press/<read>** | **Description** |
|---|---|---|
| Move forward to another menu | [Enter] | To move forward to a sub-menu, type in the number of the desired sub-menu and press [Enter]. |
| Move backward to a previous menu | [Esc] | Press the [Esc] key to move back to the previous menu. |
| Move the cursor | [Enter] or<br>[Up]/[Down] arrow keys | Within a menu, press [Enter] to move to the next field. You can also use the [Up]/[Down] arrow keys to move to the previous and the next field, respectively. |
| Enter information | Fill in, or<br>Press the [Space bar] to toggle | There are two types of fields that you will need to fill in. The first requires you to type in the appropriate information. The second gives you choices to choose from. In the second case, press the [Space bar] to cycle through the available choices. |
| Required fields | <?> | All fields with the symbol <?> must be filled in order be able to save the new configuration. |
| N/A fields | <N/A> | Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is not available. |
| 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 in Figure 2-4.



```
              Copyright (c) 1994 - 1997 ZyXEL Communications Corp.
                            Prestige 128MH Main Menu

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

Advanced Applications
  11. Remote Node Setup
  12. Static Routing Setup
  13. Default Dial-in Setup
  14. Dial-in User Setup                 99. Exit



                          Enter Menu Selection Number:
```

**Figure 2-4. SMT Main Menu**

## *System Management Terminal Interface Summary*

**Table 2-3. Main Menu Summary**

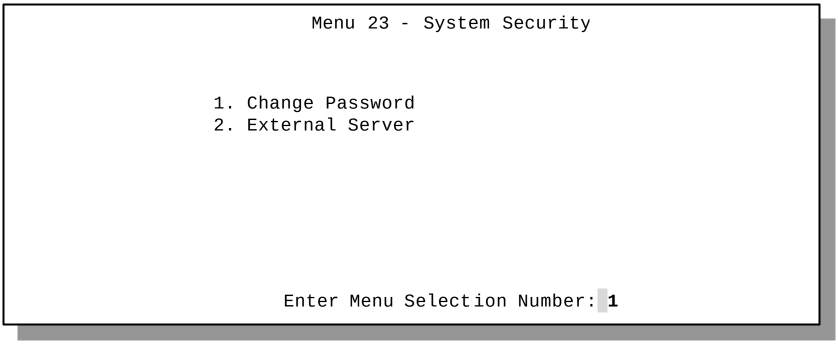
| # | Menu Title | Description |
|---|---|---|
| 1 | General Setup | Use this menu to setup general information and to enable routing for specific protocols and bridging. |
| 2 | WAN Setup | Use this menu to setup the modem ports and the WAN port. |
| 3 | Ethernet Setup | Use this menu to setup Ethernet. |
| 4 | Internet Access Setup | A quick and easy way to setup Internet connection. |
| 11 | Remote Node Setup | Use this menu to setup the Remote Node for LAN-to-LAN connection, including Internet connection. |
| 12 | Static Routing Setup | Use this menu to setup static route for different protocols. |
| 13 | Default Dial-in Setup | Use this menu to setup default dial-in parameters so that your *Prestige* can be used as a dial-in server. |
| 14 | Dial-in User Setup | Use this menu to setup dial-in users. |

| | | |
|---|---|---|
| 21 | Filter Set Configuration | Use this menu to setup filters to provide security, call control, etc. |
| 22 | SNMP Configuration | Use this menu to setup SNMP related parameters |
| 23 | System Security | Use this menu to setup security related parameters. |
| 24 | System Maintenance | This menu provides system status, diagnostics, firmware upload, etc. |
| 99 | Exit | To exit from SMT and return to the blank screen. |

## 2.6 Changing the System Password

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

**Step 1.** Select option **[23. System Security]** in the Main Menu. This will open Menu 23 - System Security as shown in Figure 2-5.

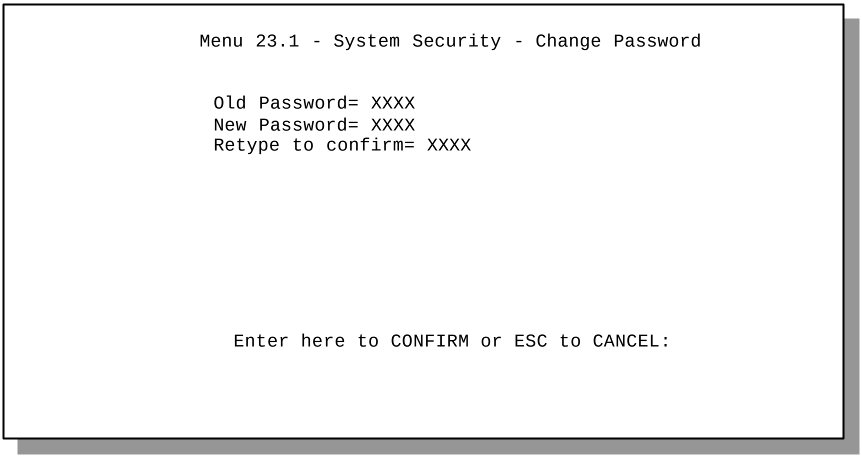


```
                    Menu 23 - System Security



             1. Change Password
             2. External Server








                  Enter Menu Selection Number: 1
```

**Figure 2-5. Menu 23 - System Security**

**Step 2.** From the System Security Menu, select option **[1. Change Password]** to open Menu 23.1 - System Security - Change Password.

**Step 3.** When the Submenu 23.1- System Security-Change Password appears, as shown in Figure 2-6, type in your existing system password, i.e., **`1234`**, and press [Enter].



```
                    Menu 23.1 - System Security - Change Password


                     Old Password= XXXX
                     New Password= XXXX
                     Retype to confirm= XXXX









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

**Figure 2-6. Menu 23.1 - System Security - Change Password**

**Step 4.** Enter your new system password and press [Enter].

**Step 5.** Re-type your new system password for confirmation and press [Enter].

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

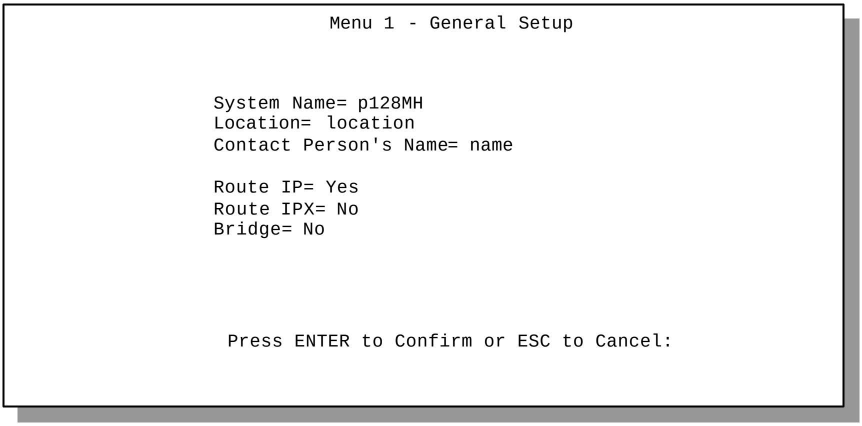
## 2.7 General Setup

The 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.** Select option **[1. General Setup]** in the Main Menu by typing 1 at the menu selection number prompt.

**Step 2.** The Menu 1 - General Setup screen appears, as shown in Figure 2-7. Fill in the required fields marked [?] and turn on the individual protocols for your applications, as explained in Table 2-4.



```
                            Menu 1 - General Setup


                System Name= p128MH
                Location=  location
                Contact Person's Name= name

                Route IP= Yes
                Route IPX= No
                Bridge= No




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

**Figure 2-7. 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 8 alphanumeric characters long. Spaces are not allowed, but dashes “-” and underscores "_" are accepted. This name can be retrieved remotely via SNMP, used for CHAP authentication, and will be displayed at the prompt in the Command Mode. | P128MH |
| Location (optional) | Enter the geographic location (up to 31 characters) of your *Prestige.* | MyHouse |
| Contact Person's Name (optional) | Enter the name (up to 8 characters) of the person in charge of this *Prestige*. | JohnDoe |
| Protocols : | Turn on or off routing for the individual protocols. | Press space-bar to toggle |
| Route IP | Set this field to [Yes] to enable IP routing. You must enable IP routing for Internet access. | [Yes/No] |
| Route IPX | Set this field [Yes] to enable IPX routing. | [Yes/No] |
| Bridge | Turn on/off bridging for protocols not supported (for example, SNA) or not turned on in the previous Route fields. | [Yes/No] |

## *Note on Bridge*

When bridging is enabled, your *Prestige* forwards any packet that it does not route. Without bridging, the packets that the *Prestige* does not route are simply discarded. Compared to routing, bridging generates far more traffic for the same network protocol and consumes more CPU cycles and memory.

## 2.8 WAN Port Setup

This section describes how to configure the built-in modems and the WAN port on your *Prestige* using Menu 2- WAN Setup.  We will use the term "WAN device" to mean either the built-in modems or the external modem/TA on the WAN port from now on.

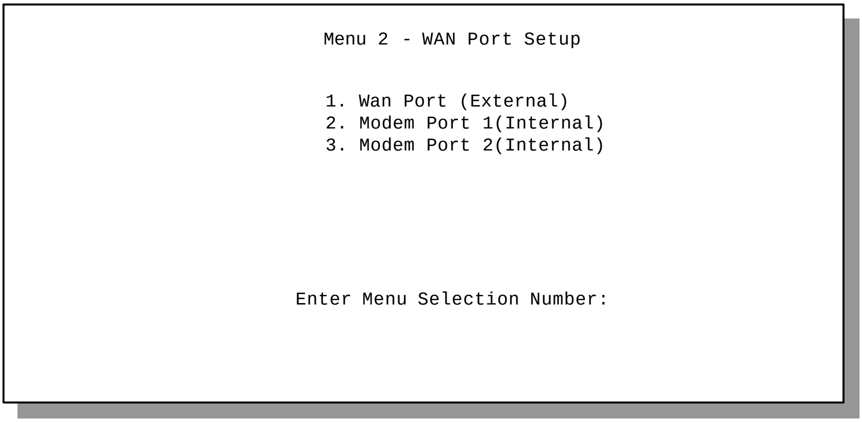
Select a WAN port (modem 1, 2 or the WAN port) that you wish to configure first.  Then configure the WAN port from Submenu 2.1. If advanced setup is required, go into Menu 2.2. Your *Prestige* will use this information to initialize the port and the attached WAN device.

### 2.8.1 *Prestige 128MH* WAN Port Setup

To configure a WAN port on *Prestige 128MH*, follow these steps:

**Step 1.** Select option **[2. WAN Setup]** in the Main Menu by typing 2 at the menu selection number prompt.

**Step 2.** In Menu 2 - WAN Port Setup, as shown in Figure 2-8, enter the number (1, 2 or 3) of the WAN port you wish to configure.

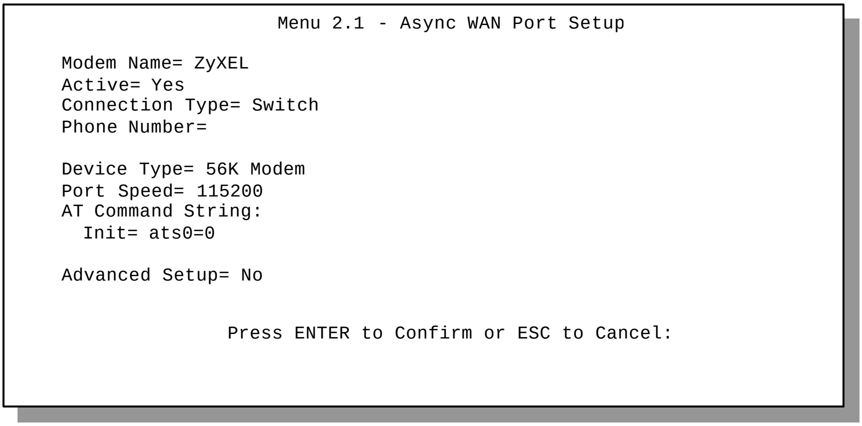


```
                              Menu 2 - WAN Port Setup


                              1. Wan Port (External)
                              2. Modem Port 1(Internal)
                              3. Modem Port 2(Internal)






                           Enter Menu Selection Number:
```

**Figure 2-8. Menu 2 - WAN Port Setup**

**Step 3.** This will bring up Menu 2.1 - Async WAN Port Setup, as shown in Figures 2-9, 2-10. In Menu 2.1 you can set the configuration parameters for the selected WAN port.

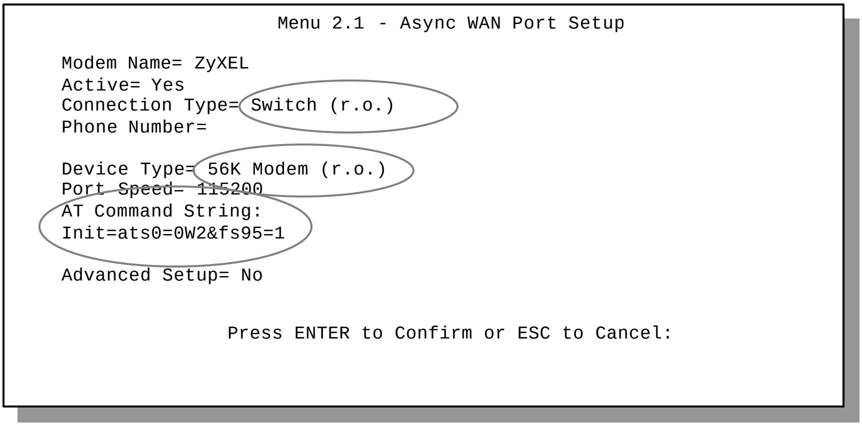
- Figure 2-9 shows how to configure the WAN port with an external modem or ISDN TA.



```
                      Menu 2.1 - Async WAN Port Setup

    Modem Name= ZyXEL
    Active= Yes
    Connection Type= Switch
    Phone Number=

    Device Type= 56K Modem
    Port Speed= 115200
    AT Command String:
      Init= ats0=0

    Advanced Setup= No


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

**Figure 2-9. Menu 2.1 - Async WAN Port Setup for the WAN Port**

- Figure 2-10 displays Menu 2.1 when configuring modem 1 and modem 2.



```
                          Menu 2.1 - Async WAN Port Setup

     Modem Name= ZyXEL
     Active= Yes
     Connection Type= Switch (r.o.)
     Phone Number=

     Device Type= 56K Modem (r.o.)
     Port Speed= 115200
     AT Command String:
     Init=ats0=0W2&fs95=1

     Advanced Setup= No


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

**Figure 2-10. Menu 2.1 - Async WAN Port Setup for Modem 1/2**

Table 2-5 describes how to configure the WAN ports.

**Table 2-5. Async WAN Port Setup Menu Fields**

| Field | Description | Example |
|---|---|---|
| Modem Name | Enter a descriptive name for the Modem or ISDN TA connected to this WAN Port. | ZyXEL |
| Active | Set to [Yes] to activate a WAN port, then your *Prestige* will initialize the WAN Port and the attached Modem or ISDN TA. | Press space-bar to toggle<br>[Yes/No] |
| Connection Type | For the WAN Port, select the type of your telephone line; [Switch] for a dial-up line and [Leased] for leased line.  The connection types for the internal modems are switched by default. | Press space-bar to toggle<br>[Switch/Leased] |

**Table 2-5. Async WAN Port Setup Menu Fields (continued)**

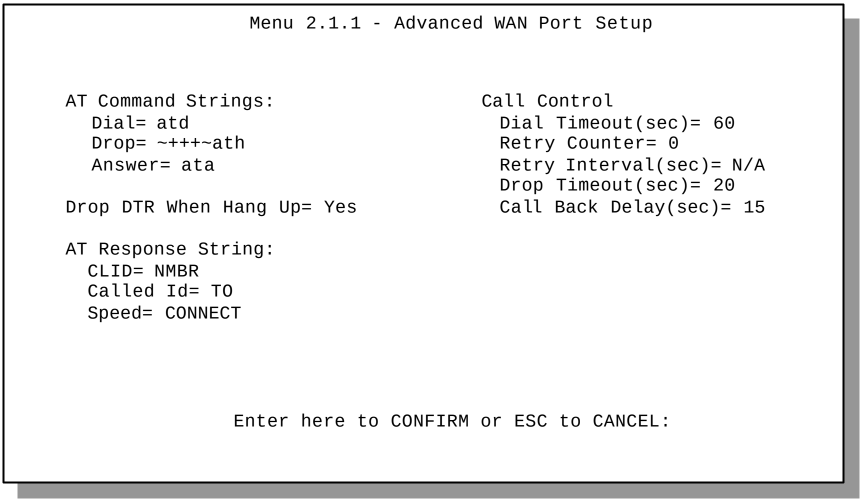
| | | |
|---|---|---|
| Phone Number | Enter the telephone number assigned to your telephone line by your telephone company. Note that your *Prestige* only accepts digits; do not include dashes and spaces in this field. | 5551212<br>(example) |
| Device Type | For WAN Port, use the space bar to select one of the following types: [Modem / ISDN TA / X.25 PAD / 56K Modem]. A Device Type is selected for the WAN Port such that a Remote Node only picks up a free device of the selected type to dial out. Only the WAN Ports of the same device type can be bundled. This field is not applicable if the Connection Type is set to [Leased]. The device types for the internal modems are Modem by default. | Space-bar to toggle<br>[Modem]<br>[ISDN TA]<br>[X.25 PAD]<br>[56K Modem] |
| Port Speed | Use the space bar to select the speed between the WAN port and the external device. Available speeds are:<br>9600 / 19200 / 38400 / 57600 / 115200 / 230000 bps | 115200<br>(default) |
| AT Command String: Init | Enter an AT command string to initialize the modem or ISDN TA. When the Connection Type is set to [Switch], you must include AT command “s0=0” to disable modem auto-answer; the Prestige will decide when to answer an incoming call.<br>**Note the default AT command string [at&fs0=0w2s95=1] for the internal modems.** | (Default: ats0=0) |
| Advanced Setup | To edit the Advanced Setup for this Modem/ISDN TA, move the cursor to this field, use the space bar to select [Yes] and press [Enter]. This will bring you to Menu 2.1.1 - Advanced Setup. | [Yes/No] |
| When you complete this menu, press [Enter] to save your configuration, or [Esc] to cancel. After you press [Enter], the *Prestige* uses the information you have saved to initialize the WAN Port and the connected Modem/ISDN TA. | | |

### 2.8.2 Advanced WAN Port Setup

The Advanced WAN Port Setup Menu allows you to enter the AT Commands for the WAN devices and the call control parameters.

**Step 1.** In Menu 2.1, move the cursor to the Advanced Setup field and press the space bar to select [Yes], then press [Enter].

**Step 2.** When Menu 2.1.1 appears, fill in the appropriate AT commands and call control parameters for the internal modems and the external modem or ISDN TA, as shown in Figure 2-11.



```
                      Menu 2.1.1 - Advanced WAN Port Setup



     AT Command Strings:                     Call Control
       Dial= atd                               Dial Timeout(sec)= 60
       Drop= ~+++~ath                          Retry Counter= 0
       Answer= ata                             Retry Interval(sec)= N/A
                                               Drop Timeout(sec)= 20
     Drop DTR When Hang Up= Yes                Call Back Delay(sec)= 15

     AT Response String:
       CLID= NMBR
       Called Id= TO
       Speed= CONNECT




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

**Figure 2-11. Menu 2.1.1 - Advanced WAN Port Setup**

Refer to Table 2-6 for details on how to fill in the AT commands fields.

**Table 2-6. Advanced WAN Port Setup AT Commands Fields**

| Field | Description | Default |
|---|---|---|
| AT Command Strings : | | |
| Dial | Enter the AT Command string to make a call. | [atdt] |
| Drop | Enter the AT Command string to drop a call. [~] represents a one second wait. | [~+++~ath] |
| Answer | Enter the AT Command string to answer a call. | [ata] |
| Drop DTR When Hang Up | When [Yes] is selected, your *Prestige* will drop the DTR signal after sending out [AT Command String: Drop]. | Toggle<br>[Yes/No]<br>(Default=[Yes]) |
| AT Response Strings: | | |
| CLID (Caller Line Identification) | Enter the keyword preceding the CLID in the response from the WAN device if present. CLID is required for CLID authentication. | [NMBR] |
| Called ID | Enter the keyword preceding the dialed number. | [TO] |
| Speed | Enter the keyword preceding the connection speed from AT Response String. | [CONNECT] |
| When you have completed this menu, press [Enter] to return to Menu 2.1. | | |

### AT Command Strings

For the regular telephone lines, the default "Dial" string tells the modem that the line uses tone dialing. If your switch still requires pulse dialing, change the string to "`atdp`". For ISDN lines, there are far more protocols and operational modes. Please consult the documentation of your TA, for you may need additional commands in both "Dial" and "Init" strings.

### DTR Signal

The majority of WAN devices default to hanging up the current call when the DTR (Data Terminal Ready) signal is dropped by the DTE. When "Drop DTR When Hang Up" is set to yes, the *Prestige* will use this hardware signal to force the WAN device to hang up, in addition to issuing the drop command (ATH).

### Response Strings

The response strings tell the *Prestige* the tags, or labels, immediately preceding the various call parameters sent from the WAN device. The response strings have not been standardized; please consult the documentation of your WAN device to find the correct tags.

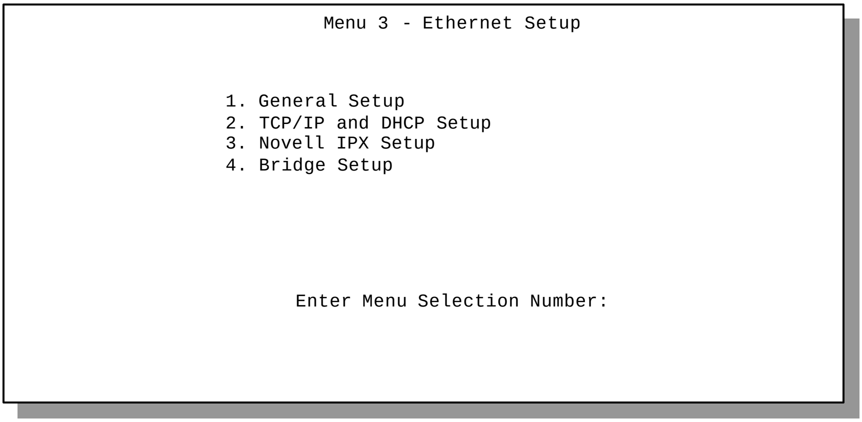
Table 2-7 below describes the call control parameters.

**Table 2-7. Advanced WAN Port Setup Call Control Parameters**

| **Field** | **Description** | **Default** |
|---|---|---|
| Dial Timeout (sec) | The *Prestige* will timeout if it can not set up an outgoing modem call within the timeout value. | [60] seconds |
| Retry Count | How many times a busy or no-answer phone number is retried before it is put on the blacklist. | [0] to disable the blacklist control |
| Retry Interval (sec) | Elapsed time after a call fails before another call may be retried. Applies before a phone number is blacklisted. | |
| Drop Timeout (sec) | The *Prestige* will drop the DTR signal if it does not receive a positive confirmation of disconnect within the timeout period. | [20] seconds |
| Call Back Delay (sec) | Elapsed time between dropping a callback request call and dialing a callback call. | [15] seconds |

## 2.9 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.

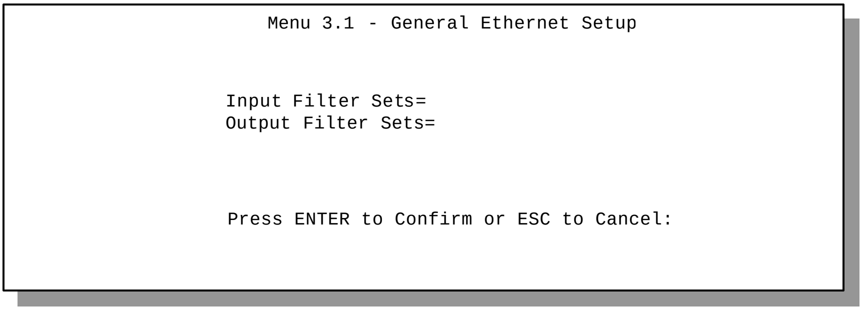


```
                              Menu 3 - Ethernet Setup


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






                          Enter Menu Selection Number:
```

**Figure 2-12. Menu 3 - Ethernet Setup**

### 2.9.1 General Ethernet Setup

This menu allows you to specify the filter sets 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=
                    Output Filter Sets=




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

**Figure 2-13. Menu 3.1 - General Ethernet Setup**

If you need to define filters, please read *Chapter 9- Filter Set Configuration*, then return to this menu to define the filter sets.

## 2.10 Protocol Dependent Ethernet Setup

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

- For TCP/IP Ethernet setup refer to *Chapter 3 - Internet Access Application*.
- For Novell IPX Ethernet setup refer to Section 7.4 - IPX Ethernet Setup in *Chapter 7 - Novell IPX Configuration for LAN-to-LAN*.
- For bridging Ethernet setup refer to *Chapter 8 - Bridge Configuration for LAN-to-LAN*.

# Chapter 3

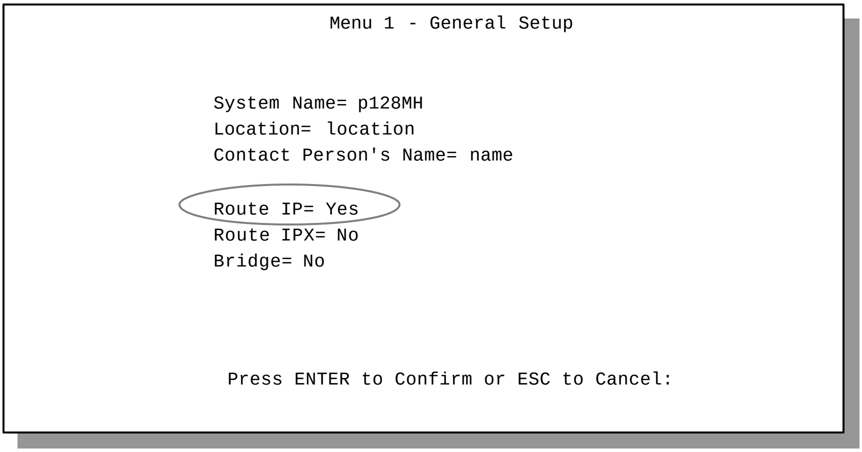
# Internet Access

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

## 3.1 Route IP Setup

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

To edit Menu 1, enter 1 in the Main Menu to select **[1. General Setup]** and press [Enter]. Set the ***Route IP*** field to [Yes] by pressing the space bar as shown in Figure 3-1.



```
                         Menu 1 - General Setup


                System Name= p128MH
                Location= location
                Contact Person's Name= name

                Route IP= Yes
                Route IPX= No
                Bridge= No




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

**Figure 3-1. Menu 1 – General Setup**

# 3.2 TCP/IP Parameters

## 3.2.1 IP Address and Subnet Mask

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

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 (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 3 numbers specify the network number while the last number identifies an individual workstation on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, e.g., 192.168.1.1, for your *Prestige*.

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.

## 3.2.2 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to both, the *Prestige* will broadcast its routing table periodically and incorporate the RIP information that it receives; when set to none, it will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the *Prestige* sends (it recognizes both formats when receiving). RIP-1 is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have a unusual network topology.

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

By default, RIP direction is set to both and the version set to RIP-1.

### 3.2.3 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 the DHCP server capability built-in and is enabled by default.

#### *IP Pool Setup*

The *Prestige* is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the *Prestige* itself) in the lower range for other server machines, e.g., server for mail, FTP, telnet, web, etc., that you may have.

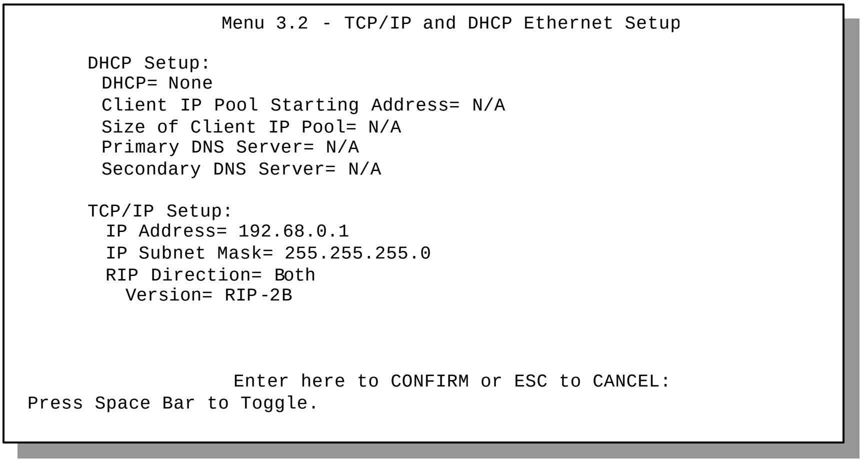
#### *DNS Server Address*

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, e.g., the IP address of *www.zyxel.com* is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. 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. Make sure that you obtain the IP address of the DNS servers from your ISP. Your workstations will need this information even if you don't use the *Prestige*'s DHCP server.

## 3.3 TCP/IP Ethernet Setup and DHCP

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

To edit Menu 3.2, select the menu option **[3. Ethernet Setup]** in the Main Menu. When Menu 3 appears, select the submenu option **[2. TCP/IP and DHCP Setup]** and press [Enter]. The screen now displays Menu 3.2 - TCP/IP and DHCP Ethernet Setup, as shown in Figure 3-2.



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

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

     TCP/IP Setup:
       IP Address= 192.68.0.1
       IP Subnet Mask= 255.255.255.0
       RIP Direction= Both
         Version= RIP-2B



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

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

Follow the instructions in Table 3-1.on how to configure the DHCP fields.

**Table 3-1. DHCP Ethernet Setup Menu Fields**

| Field | Description | Example |
|---|---|---|
| DHCP | | |
| DHCP= | This field enables/disabled the DHCP server. If it is set to [**Server**], your *Prestige* will act as a DHCP server. If set to [None], DHCP server will be disabled.<br>When DHCP is used, the following four items need to be set: | [None]<br>[Server] (default) |
| Client IP Pool Starting Address | This field specifies the first of the contiguous addresses in the IP address pool. | 192.168.1.33 |
| Size of Client IP Pool | This field specifies the size, or count, of the IP address pool. | 32 |
| Primary DNS Server<br>Secondary DNS Server | Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mas k.. | |

Follow Table 3-2 to configure TCP/IP parameters for the Ethernet port.

**Table 3-2.  TCP/IP Ethernet Setup Menu Fields**

| Field | Description | Example |
|---|---|---|
| TCP/IP Setup | | |
| IP Address | Enter the IP address of your *Prestige* in dotted decimal notation | 192.168.1.1<br>(default) |
| IP Subnet Mask | Your *Prestige* will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the *Prestige* | 255.255.255.0 |
| RIP Direction | Press the space bar to select the RIP direction from [Both]/[In Only]/[Out Only]. | [Both]<br>(default) |
| Version | Press the space bar to select the RIP version from [RIP-1]/[RIP-2B]/[RIP-2M]. | [RIP-1]<br>(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. | | |

## 3.4 Internet Access Configuration

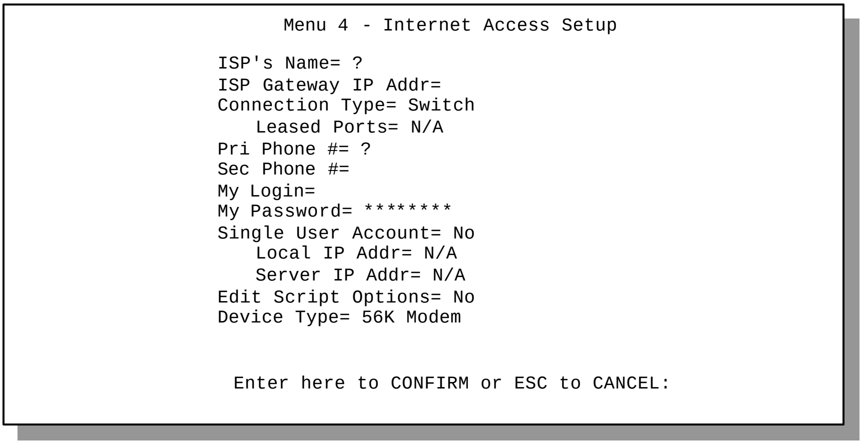
Menu 4 allows you to enter the Internet Access information in one screen. Menu 4 is actually a simplified setup for one of the remote nodes that you can access in Menu 11. Before you configure your *Prestige* for Internet access, you need to collect your Internet account information from your ISP.

Use Table 3-3 to record your Internet Account Information.

**Table 3-3. Internet Account Information**

| **Internet Account Information** | **Write your account information here** |
|---|---|
| IP Address of the ISP's Gateway (Optional) | — |
| Telephone Number(s) of your ISP | — |
| Login Name | — |
| Password for ISP authentication | — |
| (DNS server address(es) for your workstation | — |

From the Main Menu, enter option **[4. Internet Access Setup]** to go to Menu 4 - Internet Access Setup, as displayed in Figure 3-3.



```
      Menu 4 - Internet Access Setup

ISP's Name= ?
ISP Gateway IP Addr=
Connection Type= Switch
   Leased Ports= N/A
Pri Phone #= ?
Sec Phone #=
My Login=
My Password= ********
Single User Account= No
   Local IP Addr= N/A
   Server IP Addr= N/A
Edit Script Options= No
Device Type= 56K Modem


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

**Figure 3-3. Menu 4 - Internet Access Setup**

Table 3-4 contains instructions on how to configure your *Prestige* for Internet access.

**Table 3-4. Internet Access Setup Menu Fields**

| **Field** | **Description** | **Observation** |
|---|---|---|
| ISP's Name | Enter the name of your Internet Service Provider. (This information is for identification purposes only.) | Myisp |
| ISP IP Addr | Enter the IP Address of the remote gateway at the ISP's site. If you do not have this data, just leave it blank. | (optional) |
| Connection Type | Select [Switch] if you connect to your ISP via a dial-up line. Select [Leased] if through a leased line. | Space-bar to toggle<br>[Switch/Leased] |
| Leased Ports | If [Leased] is selected in Connection Type, this field shows the WAN port. It shows N/A if the WAN port is not a leased line port. | [1 (r.o.)] |
| Pri(mary) Phone # | The first number your *Prestige* will dial to connect to the ISP if it is a dial-up line. | (required) |
| Sec(ondary) Phone # | If the Primary Phone number is busy or does not answer, your *Prestige* will call the Secondary Phone number if available. | (optional) |
| My Login Name | Enter the login name assigned to you by your ISP. | (required) |
| My Password | Enter the password associated with the login name above. Note that this login name/password pair is only for your *Prestige* to connect to the ISP's gateway. For TCP/IP applications, e.g., FTP, you will need a separate login name and password for each server. | (required) |

**Table 3-4. Internet Access Setup Menu Fields (continued)**

| **Field** | **Description** | **Observation** |
|---|---|---|
| Single User Account | See Section 3.5 for a more detailed discussion on the Single User Account feature. | [Yes/No] |
| Edit Script Option | To edit the parameters, select [Yes] and press [Enter]. This will bring you to Menu 4.1 – Internet Setup Script. This field is not applicable if the Connection Type is [Leased]. | |
| Device Type | The *Prestige* only chooses a free device of the selected Device Type to dial out. This field is not applicable if the Connection Type is [Leased]. Selections:[Modem/ISDN TA/X.25 PAD/56K Modem] | Space-bar to toggle |
| Press [Enter] at the message [Press ENTER to Confirm ...] to confirm your configuration, or press [Esc] at any time to cancel. | | |

At this point, the SMT will ask if you wish to test the Internet connection. If you select [Yes], your *Prestige* will call the ISP to test the Internet connection. If the test fails, note the error message that you receive on the screen and take the appropriate troubleshooting steps.

## 3.5 Single User Account

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

The Single User Account (SUA) feature allows you to have the same benefits as having multiple legal addresses, but only pay for one IP address, thus saving significantly on the subscription fees. (Check with your ISP before you enable this feature).

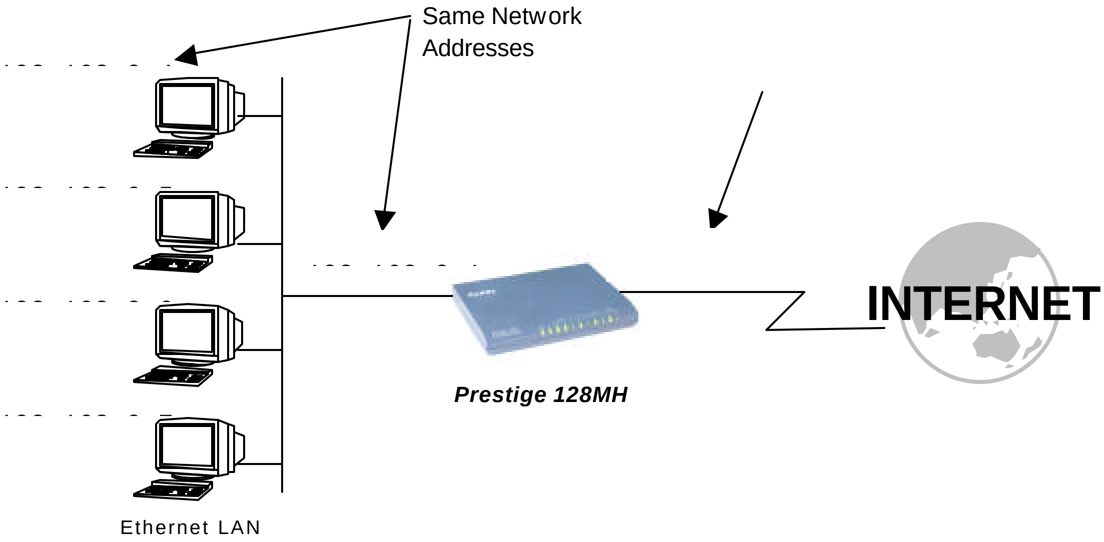


Figure 3-4 illustrates a typical Single User Account topology.

**Figure 3-4. Single User Account Topology**

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

The IP address for the SUA can be either fixed or dynamically assigned when a call is connected. In addition, you can designate a server, e.g., a web server, on your local network and make it 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* and thus preventing intruders from probing your network.

Your *Prestige* accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. For more information on IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT).*

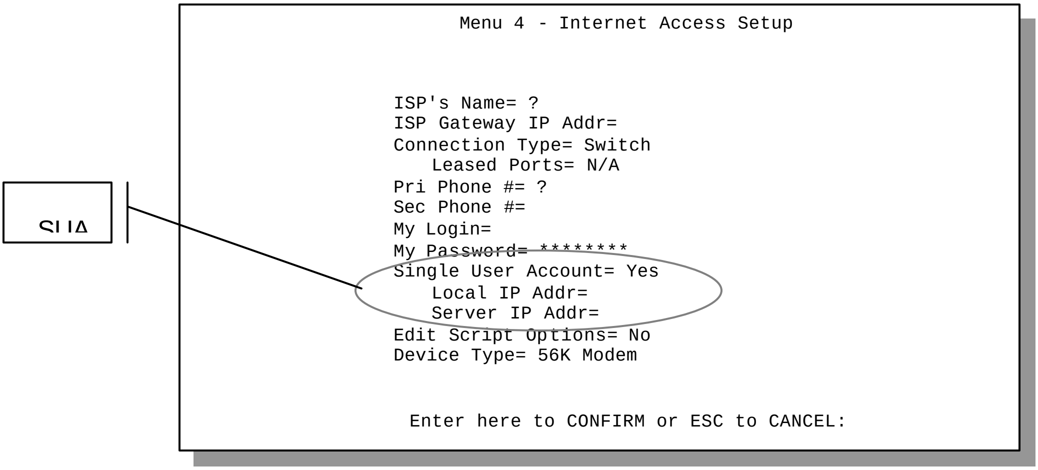
### 3.5.1 Advantages of SUA

In summary:

- SUA is a cost-effective solution for small offices with less than 20 hosts to access the Internet or other remote TCP/IP networks.
- SUA supports one server to be accessible to the outside world.
- SUA can provide firewall protection if you do not specify a server.  All incoming inquiries will be filtered out by your *Prestige*.
- UDP and TCP packets can be routed. In addition, partial ICMP is supported.

### 3.5.2 Single User Account Configuration

The steps for configuring your *Prestige* for Single User Account are identical to the conventional Internet access (see configuration instructions in Table 3-4) with the exception that you need to fill in three extra fields in Menu 4 - Internet Access Setup, as shown in Figure 3-5.



```
                         Menu 4 - Internet Access Setup



                   ISP's Name= ?
                   ISP Gateway IP Addr=
                   Connection Type= Switch
                      Leased Ports= N/A
                   Pri Phone #= ?
                   Sec Phone #=
                   My Login=
                   My Password= ********
                   Single User Account= Yes
                      Local IP Addr=
                      Server IP Addr=
                   Edit Script Options= No
                   Device Type= 56K Modem


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

**Figure 3-5. Menu 4 - Internet Access Setup for Single User Account**

To enable the SUA feature in Menu 4, move the cursor to the [Single User Account] field and select [Yes] (or [No] to disable SUA). Then follow the instructions on how to configure the SUA fields in Table 3-5.

**Table 3-5. Single User Account Menu Fields**

| Field | Description |
|---|---|
| Single User Account | Select [Yes] to enable SUA. |
| Local IP Addr. | If your ISP did *not* assign you a static IP address, enter [0.0.0.0] here; otherwise, enter that IP address here. |
| Server IP Addr. | If you want to make a single server accessible to outside users, enter that server's IP address here; otherwise, enter 0.0.0.0 in this field |
| Press [Enter] at the message [Press ENTER to Confirm ...] to save your configuration, or press [Esc] at any time to cancel. | |

At this point, your *Prestige* will ask if you wish to test the Internet connection. If you select [Yes], the *Prestige* will call the ISP and test the configuration. If the test fails, note the error messages on the screen and take the appropriate troubleshooting steps.

## 3.6 Configuring Backup ISP Accounts

If you have more than one ISP account, you can configure the secondary ISP as a backup. You can switch to the backup ISP in the event that the primary ISP is out of service. The SUA feature can be enabled for all these accounts.

### 3.6.1 Configure a Backup ISP

To configure a backup ISP Account, follow these steps:

**Step 1.** Configure your primary ISP using Menu 4, as described earlier in this chapter.

**Step 2.** Enter Menu 11, then select an unused remote node.

**Step 3.** In Menu 11.1, choose a name for your backup ISP account, then set the Active field to [No], and enter your outgoing login name, password, and phone number(s). The Remote IP Address field should be set to [1.1.1.1].

**Step 4.** In Menu 11.3, set the remote node's subnet mask to [0.0.0.0], and set RIP to [None].

**Step 5.** Save the new configuration.

Please note that the remote IP address of 1.1.1.1 is only a placeholder to avoid conflicting with that of the primary ISP, which is implicitly set at 0.0.0.0. When the backup ISP is activated, the remote IP address of 1.1.1.1 combined with the subnet mask of 0.0.0.0 creates a default route that is equivalent to the one derived form the primary ISP.

### 3.6.2 To Switch ISP

Follow these steps when you need to switch from your primary ISP to a backup ISP:

**Step 1.** Enter Menu 11 and select your Primary ISP.

**Step 2.** In Menu 11.1, set the Active field to [No].

**Step 3.** Enter Menu 11 again and select your Backup ISP.

**Step 4.** In Menu 11.1, set the Active field to [Yes].

You will now be able to access the Internet through the backup ISP Remote Node.

## 3.7 Editing Login Script

Some ISPs requires text login before it starts PPP negotiation. If this is the case for your ISP, please refer to section 4.1.6 *Editing Login Script* on how to create a login script.

# Chapter 4
# Remote Node Configuration

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 the remote nodes. Once a remote node is configured correctly, traffic to the remote network will trigger your *Prestige* to make a call automatically, i.e., Dial On Demand.

In this chapter, we will discuss the parameters that are protocol independent. The protocol-dependent configuration will be covered in subsequent chapters. For TCP/IP, *see Chapter 5*, for IPX, see *Chapter 6* and for Bridging, see *Chapter 7*.

## 4.1 Remote Node Setup

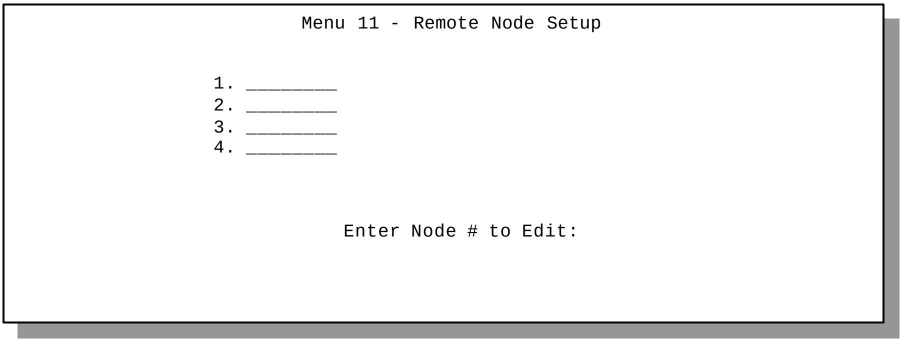
This section describes the protocol-independent parameters for a remote node.

### 4.1.1 Remote Node Profile

To configure a remote node, follow these steps:

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

**Step 2.** When Menu 11 appears, as shown in Figure 4-1, enter the number of the remote node that you wish to configure.

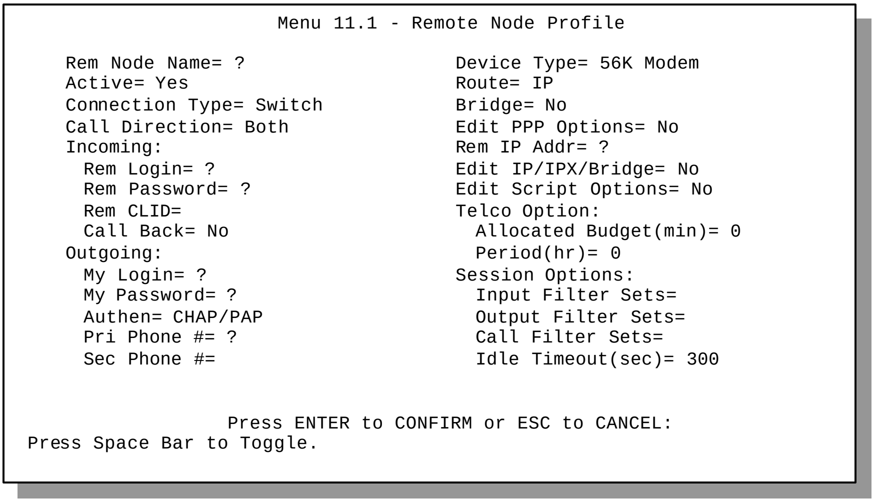


```
                        Menu 11 - Remote Node Setup

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



                            Enter Node # to Edit:
```

**Figure 4-1.      Menu 11 – Remote Node Setup**

**Step 3.** When Submenu 11.1. - Remote Node Profile appears, select the type of line that will be used (dial-up line or leased line).  Set the Connection Type to one of the following values:

- [Switch]: for dial-up lines.
- [Leased]: for leased lines. Selecting [Leased] will bring you to the Submenu 11.1.2 - Remote Node Profile for leased line.



```
                        Menu 11.1 - Remote Node Profile

   Rem Node Name= ?                   Device Type= 56K Modem
   Active= Yes                        Route= IP
   Connection Type= Switch            Bridge= No
   Call Direction= Both               Edit PPP Options= No
   Incoming:                          Rem IP Addr= ?
     Rem Login= ?                     Edit IP/IPX/Bridge= No
     Rem Password= ?                  Edit Script Options= No
     Rem CLID=                        Telco Option:
     Call Back= No                      Allocated Budget(min)= 0
   Outgoing:                            Period(hr)= 0
     My Login= ?                      Session Options:
     My Password= ?                     Input Filter Sets=
     Authen= CHAP/PAP                   Output Filter Sets=
     Pri Phone #= ?                     Call Filter Sets=
     Sec Phone #=                       Idle Timeout(sec)= 300


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

**Figure 4-2. Menu 11.1 - Remote Node Profile for Dial-up Lines**

Table 4-1 contains the instructions on how to configure the Remote Node Menu for dial-up lines.

**Table 4-1. Remote Node Profile Menu Fields for Dial-up Lines**

| Field | Description | Options |
|---|---|---|
| Rem Node Name | This is a required field [?]. Enter a descriptive name for the remote node, for example, Corp.<br>This field can be up to eight characters. This name must be unique from any other remote node name or remote dial-in user name. | |
| Active | Press the space bar to toggle between [Yes] and [No]. Inactive nodes are displayed with a minus sign (-) at the beginning of the name in Menu 11. | Press space bar to toggle<br>[Yes/No] |
| Connection Type | Use the space bar to toggle between [Switch] and [Leased]. If [Leased] is selected, moving the cursor to the next field will bring you to Submenu 11.1.2 for leased line configuration. | Press space bar to toggle<br>[Switch/Leased] |
| Call Direction | ● If this parameter is set to [Both], your *Prestige* can both place and receive calls to/from this remote node.<br>● If set to Incoming, your *Prestige* will not place a call to this remote node.<br>● If set to Outgoing, your *Prestige* will drop any incoming calls from this remote node.<br>Several other fields in this menu depend on this parameter. For example, in order to enable [Callback], the Call Direction must be [Both]. | [Both]<br>[Incoming]<br>[Outgoing] |

**Table 4-1. Remote Node Profile Menu Fields for Dial-up Lines (continued)**

| Field | Description | Options |
|---|---|---|
| Incoming: Rem Node Login Name | Enter the login name that this remote node will use when it calls your *Prestige*.<br>The login name in this field combined with the Rem Node Password will be used to authenticate this node. | |
| Incoming: Rem Node Password | Enter the password used when this remote node calls your *Prestige*. | |
| Incoming: Rem CLID | This field is applicable only if [Call Direction] is either [Both] or [Incoming]. Otherwise, an [N/A] appears in the field.<br>This is the Calling Line ID (the telephone number of the calling party) of this remote node.<br>If you enable the CLID Authen field in Menu 13 – Default Dial In, your *Prestige* will check the CLID in the incoming call against the CLIDs in the database. If no match is found and CLID Authen is Required, the call will be dropped. | |
| Incoming: Callback | This field is applicable only if [Call Direction] is [Both]. Otherwise, an [N/A] appears in the field.<br>This field determines whether or not your *Prestige* will call back after receiving a call from this remote node.<br>If this option is enabled, your *Prestige* will disconnect the initial call from this node and call it back at the Outgoing Primary Phone Number (see below). | [Enable]<br>[Disable] |
| Outgoing: My Login Name | This is a required field [?] if [Call Direction] is either [Both] or [Outgoing]. Enter the login name for your *Prestige* when it calls this remote node. | |

**Table 4-1. Remote Node Profile Menu Fields for Dial-up Lines (continued)**

| Field | Description | Options |
|---|---|---|
| Outgoing: My Password | This is a required field [?] if [Call Direction] is either [Both] or [Outgoing]. Enter the password for your *Prestige* when it calls this remote node. | |
| Outgoing: Authen | This field sets the authentication protocol used for outgoing calls.<br>Options for this field are: | |
| | ● CHAP/PAP - Your *Prestige* will accept either CHAP or PAP when requested by this remote node. | [CHAP/PAP] |
| | ● CHAP - accept CHAP only. | [CHAP] |
| | ● PAP - accept PAP only. | [PAP] |

**Table 4-1. Remote Node Profile Menu Fields for Dial-up Lines (continued)**

| Field | | Description | Options |
|---|---|---|---|
| Outgoing: | Pri(mary)<br>Sec(ondary)<br>Phone<br>Numbers | Your *Prestige* always calls this remote node using the Primary Phone number first for a dial-up line.<br>If the Primary Phone number is busy or does not answer, your *Prestige* will dial the Secondary Phone number if available.<br>Some areas require dialing the pound sign # before the phone number for local calls. A # symbol may be included at the beginning of the phone numbers as required. | |
| Device Type | | Use the space bar to choose from the following selections: Modem / ISDN TA / X.25 PAD / 56K Modem.<br>The Prestige only selects an idle device of the indicated Device Type to dial out. | [Modem]<br>[ISDN TA]<br>[X25 PAD]<br>[56K Modem] |
| Route | | This fields determines the protocols that your *Prestige* will route. | |
| Bridge | | Bridging is used for protocols that the Prestige doe not support, e.g., SNA, or not turned on in the previous Route field. When bridging is enabled, your *Prestige* will forward any packet that it does not route to this remote node; otherwise, the packets are discarded. . | Press space bar to toggle<br>[Yes/No] |

**Table 4-1. Remote Node Profile Menu Fields for Dial-up Lines (continued)**

| Field | Description | Options |
|---|---|---|
| Edit PPP Options | To edit the PPP options for this remote node, move the cursor to this field, use the space bar to select [Yes] and press [Enter]. This will bring you to Menu 11.2 - Remote Node PPP Options. For more information on configuring PPP options, see the section *Editing PPP Options*. | Press space bar to toggle [Yes] then press [Enter] |
| Rem IP Addr | This is a required field [?] if [Route] is set to [IP]. Enter the IP address of the remote gateway. | |
| Edit IP/IPX/Bridge Options | To edit the parameters, select [Yes] and press [Enter]. This will bring you to Menu 11.3 - Remote Node Network Layer Options. For more information on this screen, refer to the chapter pertaining to your specific protocol. | Press space bar to toggle [Yes] then press [Enter] |
| Edit Script Option | To edit the script, select [Yes] and press [Enter]. This will bring you to Menu 11.4 - Remote Node Script. | [Yes] then press [Enter] |
| Telco Options: | | |
| Allocated Budget (min) | This field sets a ceiling for outgoing call time for this remote node. The default for this field is [0] for no budget control. | Default = 0 |
| Period (hr) | This field sets the time interval to reset the above outgoing call budget control. | |
| Session Option:<br>Input Filter Sets, Output Filter Sets and Call Filter Sets | In these fields, enter the filter set(s) you wish to apply to the incoming and outgoing traffic between this remote node and your Prestige. You can choose from 12 different filter sets. In addition, you can link up to 4 filter sets together for further customization, e.g., 1, 5, 9, 12.<br>Note that spaces are accepted in this field.<br>For more information on customizing your filter sets, *see Chapter 9*. The default is blank, i.e., no filters defined. | Default=Blank |

**Table 4-1. Remote Node Profile Menu Fields for Dial-up Lines (continued)**

| Field | Description | Options |
|---|---|---|
| Session Option:<br>Idle Timeout (sec) | This value specifies the number of idle seconds that elapses before the remote node is automatically disconnected. Idle seconds is the period of time when no data is transmitted from your *Prestige*. Administrative packets such as RIP are not counted as data. The default is 300 seconds (5 minutes). | Default=300sec |
| Once you have completed filling in Menu 11.1.1 – Remote Node Profile, press [Enter] at the message [Press ENTER to Confirm…] to save your configuration, or press [Esc] at any time to cancel. | | |

## 4.1.2 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.

## 4.1.3 PPP Multilink

The *Prestige* uses the PPP Multilink Protocol (PPP/MP) to bundle multiple links in a single connection to boost the effective throughput between two nodes. The bundle works best when the member links are of the same type of call (e.g., POTS vs. ISDN) and at approximately the same speed.

Due to the fragmentation/reconstruction overhead associated with MP, you may not get a linear increase in throughput when a link is added. The overhead becomes more significant as the number of links increases; thus bundling more than 2 links is *not* recommended, because of the rapidly diminishing return for the subsequent links.

The number of links in an MP bundle can be statically configured, or dynamically determined at runtime, as explained in the following section.

### 4.1.4 Bandwidth on Demand

The Bandwidth on Demand (BOD) feature adds or subtracts links dynamically according to traffic demand. After the initial call, the *Prestige* uses BAP (Bandwidth Allocation Protocol) to ask the peer for additional telephone number if BACP (Bandwidth Allocation Control Protocol) is negotiated. Otherwise, the *Prestige* uses the statically configured (primary and secondary) telephone numbers of the remote node.

Bandwidth on demand is controlled by the Minimum and Maximum links of a remote node. BOD is enabled if the (number of) Maximum Ports is greater than the Minimum Ports. Otherwise, BOD is disabled. When BOD is disabled and the number of ports is greater than 1, the *Prestige* will try to bring up as many links as specified, however, the number of links will be independent of traffic demand.

When bandwidth on demand is enabled, a second link will be brought up if traffic on the initial link is higher than the high Target Utility number (for the second port) for longer than the specified Add Persist value. Similarly, the second link will be dropped if the traffic level falls below the low Target Utility number for longer than the Subtract Persist value.

The Target Utility for a second link specifies the line utilization range at which you want your *Prestige* to add or subtract bandwidth. The parameters are separated by a -. For example, 10-20 means the add threshold is 20 kbps and the subtract threshold is 10 kbps.

Your *Prestige* will perform bandwidth on demand only if it initiates the call. Addition and subtraction are based on the selection in the BOD Calculation field. If this field is set to Transmit or Receive, then traffic in either direction will be used to determine if a link should be added or dropped. Transmit will only use outgoing traffic to make this determination, and Receive will only use incoming traffic.

If the second link is not successful in joining the bundle (because the remote device does not recognize the second call as coming from the same device), your *Prestige* will hang up the second link and continue with the first link alone.

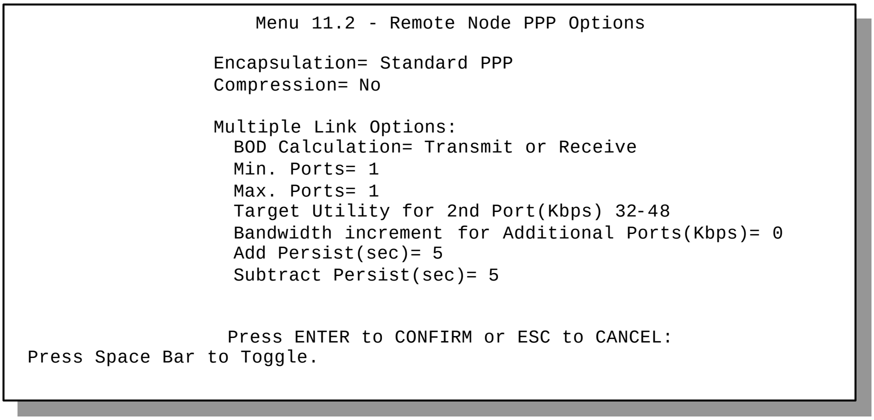
Similarly, a third link will be brought up or dropped based on the target utility for the third link. The target utility for the third link is based on the Target Utility for the second link and Bandwidth Increment for Additional Ports. For example, when Bandwidth Increment for an

Additional Port is 5 (Kbps) and the Target Utility for a second Port is 10-20; then the Target Utility for a third link is 15-25.

The BOD configuration is through Menu 11.2 - Remote Node PPP Options.

### 4.1.5 Editing PPP Options

To edit the remote node PPP Options, move the cursor to the **[Edit PPP Options]** field in Menu 11.1 - Remote Node Profile, and use the space bar to select [Yes].  Press [Enter] to open Menu 11.2, as shown in Figure 4-3.



```
                          Menu 11.2 - Remote Node PPP Options

                   Encapsulation= Standard PPP
                   Compression= No

                   Multiple Link Options:
                     BOD Calculation= Transmit or Receive
                     Min. Ports= 1
                     Max. Ports= 1
                     Target Utility for 2nd Port(Kbps) 32-48
                     Bandwidth increment  for Additional Ports(Kbps)= 0
                     Add Persist(sec)= 5
                     Subtract Persist(sec)= 5


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

**Figure 4-3.	Menu 11.2 - Remote Node PPP Options**

Table 4-2 describes the Remote Node PPP Options Menu, and contains instructions on how to configure the PPP options fields.

**Table 4-2. Remote Node PPP Options Menu Fields**

| Field | Description | Option |
|---|---|---|
| Encapsulation | Select the vendor-specific encapsulation for the link. There are two options in this field. | |
| | ● Standard PPP - Standard PPP encapsulation will be used. | [Standard PPP] |
| | ● CISCO PPP - Cisco PPP encapsulation will be used. | [CISCO PPP] |
| Compression | Turn on/off Stac Compression. The default for this field is Off. | [On/Off]<br>(Default = Off) |
| Multiple Link Options: | | |
| BOD Calculation | Select the direction of the traffic you wish to use in determining when to add or subtract a link. The default for this field is [Transmit or Receive]. | Default = Transmit or Receive |
| Min. Ports | Enter the minimum number of ports for this remote node. | |
| Max. Ports | Enter the maximum number of ports for this remote node. | |
| Target Utility for 2nd Port (kbps) | Enter the two thresholds separated by a [-] for subtracting and adding the second port. | Default=10-20 |
| Bandwidth Increment for Additional Ports (Kbps) | Enter the bandwidth increment to define the two thresholds for subtracting and adding the third port. | |

**Table 4-2. Remote Node PPP Options Menu Fields (continued)**

| Field | Description | Option |
|---|---|---|
| Add Persist | This parameter specifies the number of seconds where traffic is above the adding threshold before the *Prestige* will bring up the second link. | Default = 5 sec |
| Subtract Persist | This parameter specifies the number of seconds where traffic is below the subtraction threshold before your *Prestige* drops the second link. | Default = 5 sec |
| 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. | | |

## 4.1.6 Editing Login Script

For some remote gateways, text login is required before PPP negotiation is started. The *Prestige* provides a script facility for this purpose. The script has six programmable sets; each set is composed of an 'Expect' string and a 'Send' string. After matching a message from the server to the 'Expect' field, the *Prestige* returns the set's 'Send' string to the server.

For instance, a typical login sequence starts with the server printing a banner, a login prompt for you to enter the user name and a password prompt to enter the password:

```
Welcome to Acme, Inc.
Login: myLogin
Password:
```

To handle the first prompt, you specify "`ogin: `" as the 'Expect' string and "`myLogin`" as the 'Send' string in set 1.  The reason for leaving out the leading "`L`" is to avoid having to know exactly whether it is upper or lower case.  Similarly, you specify "`word: `" as the 'Expect' string and your password as the 'Send' string for the second prompt in set 2.

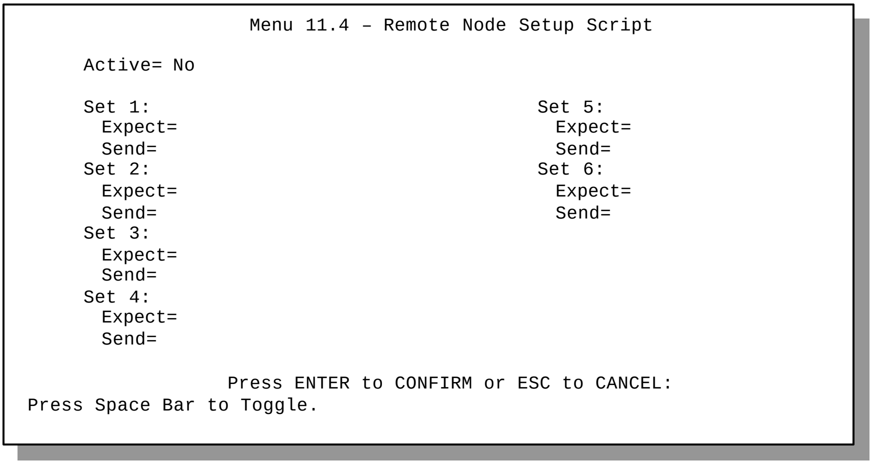
You can use two variables, `$USERNAME` and `$PASSWORD` (all UPPER case), to represent the actual user name and password in the script, so they will not show in the clear.  They are replaced with the outgoing login name and password in the remote node when the *Prestige* sees them in a

‘Send’ string.  Please note that both variables must been entered exactly as shown.  No other characters may appear before or after, either, i.e., they must be used alone in response to login and password prompts.

Please note that the ordering of the sets is significant, i.e., starting from set 1, the *Prestige* will wait until the ‘Expect’ string is matched before it proceeds to set 2, and so on for the rest of the script.  When both the ‘Expect’ and the ‘Send’ fields of the current set are empty, the *Prestige* will terminate the script processing and start PPP negotiation.  This implies two things: first, the sets must be contiguous; the sets after an empty one are ignored.  Second, the last set should match the final message sent by the server.  For instance, if the server prints

```
login successful.
Starting PPP...
```

after you enter the password, then you should create a third set to match the final “`PPP...`” but without a “Send” string.  Otherwise, the *Prestige* will start PPP prematurely right after sending your password to the server.



```
                     Menu 11.4 - Remote Node Setup Script

       Active= No

       Set 1:                                    Set 5:
         Expect=                                   Expect=
         Send=                                     Send=
       Set 2:                                    Set 6:
         Expect=                                   Expect=
         Send=                                     Send=
       Set 3:
         Expect=
         Send=
       Set 4:
         Expect=
         Send=

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

**Figure 4-4.        Menu 11.4 – Remote Node Setup Script**

If there are errors in the script and it gets stuck at a set for longer than the “Dial Timeout” in menu 2 (default 60 seconds), the *Prestige* will timeout and drop the line.  To debug a script, go to Menu 24.4 to initiate a manual call and watch the trace display to see if the sequence of messages and prompts from the server differs from what you expect.

The following Table 4-3 describes each field in Menu 11.4 – Remote Node Setup Script.

**Table 4-3. Remote Node Script Menu Fields**

| **Field** | **Description** | **Option** |
|---|---|---|
| Active | Press the space bar to toggle between [Yes] and [No]. | [Yes/No] |
| Set 1-6: Expect | Enter an Expect string to match.  After matching the Expect string, the *Prestige* returns the string in the [Send] field. | |
| Set 1-6: Send | Enter a string to send out after the Expect string is matched. | |

## 4.2 Leased Line Connection

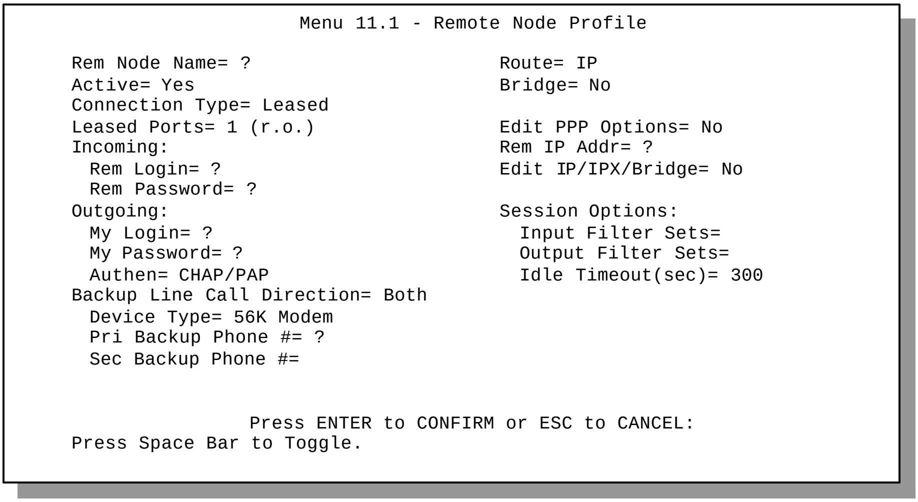
A leased line provides a connection that is always up without dialing and modem negotiation, which can take tens of second. The WAN port on the *Prestige* allows you to connect a leased line modem (async). Obviously, the Connection Type of the WAN port must be selected as [Leased] in Menu 2.1 - Async WAN Port Setup.

### 4.2.1 Dial-up Backup for Leased Line

If you have a dial-up line in addition to the leased line, you can use the dial-up line as a backup for the leased line in the event that the leased line is down. When the leased line connection drops, your *Prestige* will select an available modem to place a phone call to establish a backup connection. When the leased line is up again, your *Prestige* will drop the backup link.

### 4.2.2 Leased Line Remote Node Profile

From Submenu 11.1, select [Leased] in the Connection Type field to go to Submenu 11.1.2 - Remote Node Profile for Leased Line, as shown below in Figure 4-5.



```
                        Menu 11.1 - Remote Node Profile

    Rem Node Name= ?                      Route= IP
    Active= Yes                           Bridge= No
    Connection Type= Leased
    Leased Ports= 1 (r.o.)                Edit PPP Options= No
    Incoming:                             Rem IP Addr= ?
      Rem Login= ?                        Edit IP/IPX/Bridge= No
      Rem Password= ?
    Outgoing:                             Session Options:
      My Login= ?                           Input Filter Sets=
      My Password= ?                        Output Filter Sets=
      Authen= CHAP/PAP                      Idle Timeout(sec)= 300
    Backup Line Call Direction= Both
      Device Type= 56K Modem
      Pri Backup Phone #= ?
      Sec Backup Phone #=


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

**Figure 4-5. Menu 11.1 - Remote Node Profile**

Table 4-4 describes the fields in Menu 11.1.2 - Remote Node Profile for Leased Line that are specific to leased lines.

**Table 4-4. Remote Node Profile Menu Fields for Leased Lines**

| **Field** | **Description** | **Option** |
|---|---|---|
| Connection Type: [Leased] | Use space bar to toggle [Switch/Leased], select [Leased] and press [Enter]**.** | [Leased] |
| Leased Port | If [Leased] is selected in Connection Type, this field displays the WAN port that supports eased line connections.<br>This field is read only (r.o.), since only the WAN port supports leased line.<br>The Connection Type of the WAN port must have been specified as [Leased] in Menu 2.1 - Async WAN Port Setup**.** | [1 (r.o.)] |
| Backup Line Call Direction | This field specifies the call direction for the backup dial-up line.<br>● If this parameter is set to [Both], your *Prestige* can both place and receive backup calls to/from this remote node.<br>● Set this parameter to [None] to disable dial-up backup.<br>● If set to Incoming, your *Prestige* will not place a backup call to this remote node.<br>● If set to Outgoing, your *Prestige* will drop any call from this remote node. | Press space bar to select [Both/None/Outgoing/Incoming]<br>[Both]<br>(default)<br>[None]<br>[Incoming]<br>[Outgoing] |
| Device Type<br>*(*for backup line only)* | This field always shows the only option modem (r.o). | |
| Incoming: Rem Node Login Name | Enter the login name that this remote node uses when it calls your *Prestige*. The login name in this | |

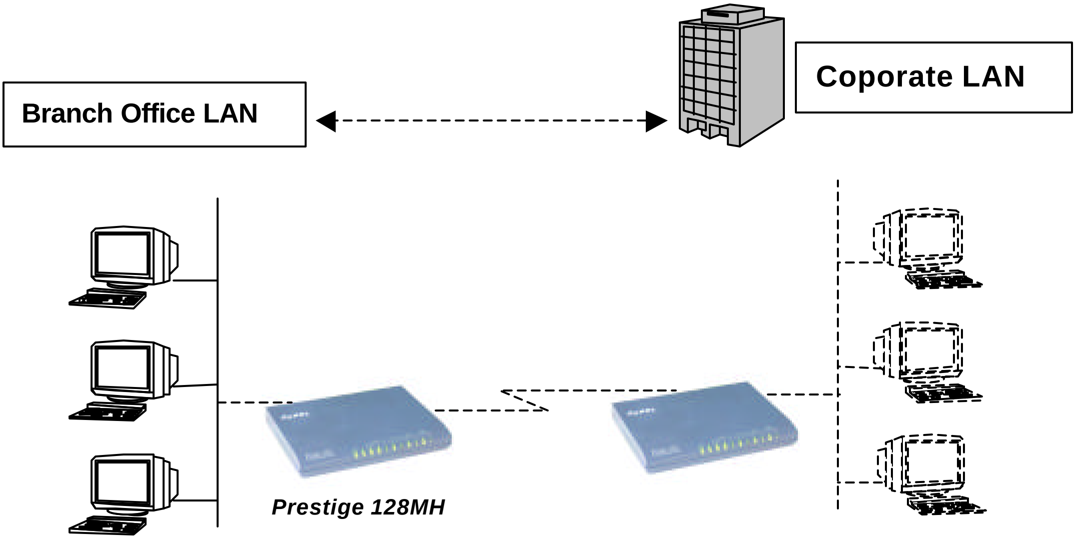
| | | |
|---|---|---|
| Name<br>*(*for backup line only)* | when it calls your *Prestige*. The login name in this field combined with the Rem Node Password will be used to authenticate the incoming calls from this node. | |
| Incoming: Rem Node Password<br>*(*for backup line only)* | Enter the password used when this remote node calls into your *Prestige*. | |
| Outgoing: My Login Name<br>*(*for backup line only)* | This is a required field [?] if [Call Direction] is either [Both] or [Outgoing]. Enter the login name for your *Prestige* when it calls this remote node. | |
| Outgoing: My Password<br>*(*for backup line only)* | This is a required field [?] if [Call Direction] is either [Both] or [Outgoing]. Enter the password for your *Prestige* when it calls this remote node. | |
| Outgoing: Authen<br>*(*for backup line only)* | This field sets the authentication protocol used for outgoing calls.<br>Options for this field are: | |
| | ● CHAP/PAP - Your *Prestige* will accept either CHAP or PAP when calling this remote node. | [CHAP/PAP] |
| | ● CHAP – use CHAP only. | [CHAP] |
| | ● PAP - use PAP only. | [PAP] |
| Primary Phone #<br>*(*for backup line only)* | Enter the primary telephone number that your *Prestige* will dial when the Backup Line function is triggered. | |
| Secondary Phone #<br>*(*for backup line only)* | Enter the secondary telephone number that your *Prestige* will dial when the Backup Line function is triggered. | |

# Chapter 5

# Remote Node TCP/IP Configuration

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

## 5.1 LAN-to-LAN Application



A typical LAN-to-LAN application is to use your *Prestige* to connect a branch office to the headquarters, as depicted in the following Figure 5-1.

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

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

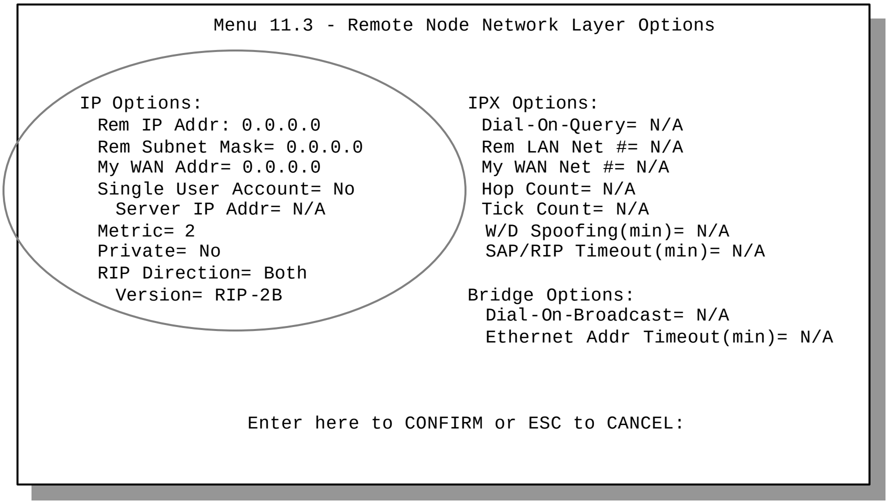
## 5.1.1 Remote Node Setup

Follow the procedure in *Chapter 5 - Remote Node Configuration* to configure the protocol-independent parameters in Menu 11 - Remote Node Profile. For the TCP/IP parameters, follow the instructions below. If you are configuring your *Prestige* to receive incoming calls, you also need to set the default dial-in parameters in Menu 13.

Follow the steps below to edit Menu 11.3 - Remote Node Network Layer Options shown in Figure 5-2.

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

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



```
                  Menu 11.3 - Remote Node Network Layer Options


     IP Options:                           IPX Options:
       Rem IP Addr: 0.0.0.0                  Dial-On-Query= N/A
       Rem Subnet Mask= 0.0.0.0              Rem LAN Net #= N/A
       My WAN Addr= 0.0.0.0                  My WAN Net #= N/A
       Single User Account= No               Hop Count= N/A
         Server IP Addr= N/A                 Tick Count= N/A
       Metric= 2                              W/D Spoofing(min)= N/A
       Private= No                            SAP/RIP Timeout(min)= N/A
       RIP Direction= Both
         Version= RIP-2B                   Bridge Options:
                                              Dial-On-Broadcast= N/A
                                              Ethernet Addr Timeout(min)= N/A



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

**Figure 5-2. Menu 11.3- Remote Node TCP/IP Options**

The following diagram in Figure 5-3 explains the Sample IP Addresses to help you to understand the field of My Wan Address in Menu 11.3.

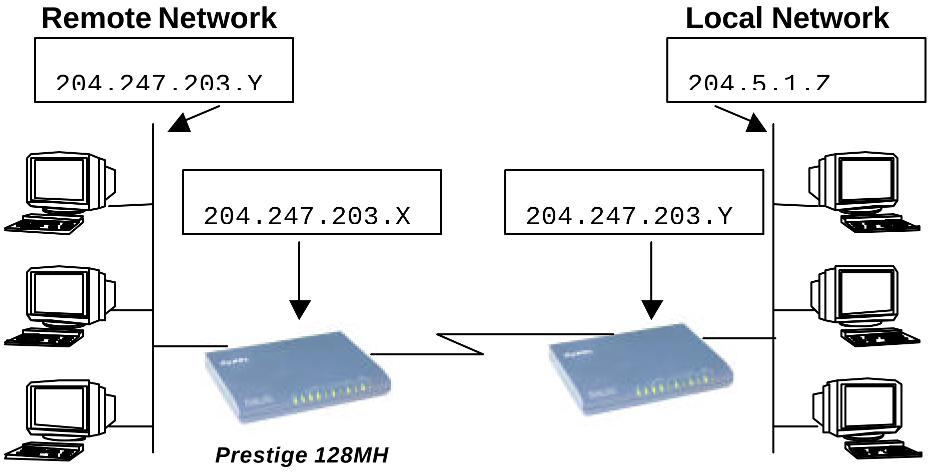


**Figure 5-3. Sample IP Addresses for a TCPI/IP LAN-to-LAN Connection**

To configure the TCP/IP parameters of a remote node, first configure the three fields in Menu 11 – Remote Node Profile, as shown in Table 5-1. For more details on the IP Option fields, refer to *Chapter 3 - Internet Access Application*.

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

| Field | Description | Option |
|---|---|---|
| Route | Make sure [IP] is among the protocols in the Route field in the Remote Node Profile. | [IP] |
| Rem IP Address | Enter the IP address of the remote gateway in Remote Node Profile. | |
| Edit IP/IPX/Bridge | Press the space bar to select [Yes] and press [Enter] to go to Menu 11.3 - Remote Node Network Layer Options Menu. | [Yes]<br>([Yes/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**

| | | |
|---|---|---|
| Rem IP Address | This will show the IP address you entered for this remote node in the previous menu. | |
| Rem IP Subnet Mask | Enter the subnet mask for the remote network. | |
| My WAN Addr | Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your *Prestige*.<br>Note that this is the address assigned to your local *Prestige*, not the remote router.<br>(*See* Figure 5-3 for an explanation of My WAN Addr. With Sample IP Addresses) | |
| Single User Account | Set this field to [Yes] to enable the Single User Account feature for your *Prestige*. Use the space bar to toggle between [Yes] and [No]. *See Chapter 3 - Internet Access Application* for more information on the Single User Account feature. | [Yes/No] |
| Server IP address | If you enable Single User Account and you want to make a server on your LAN accessible to the outside world, enter that server's inside IP address here. | |

**Table 5-2. Remote Node TCP/IP Configuration (continued)**

| Field | Description | Option |
|---|---|---|
| Metric | The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of [1] for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between [1] and [16]. In practice, [2] or [3] is usually a good number. | [1] to [16] |
| Private | This parameter determines if the *Prestige* will include the route to this remote node in its RIP broadcasts. If set to [Yes], this route is kept private and not included in RIP broadcast. If [No], the route to this remote node will be propagated to other hosts through RIP broadcasts. | [Yes/No] |
| RIP | Press the space bar to select the RIP direction from [Both]/[In Only]/[Out Only].. | (Default=Both) |
| Version= | Press the space bar to select the RIP version from [RIP-1]/[RIP-2B]/[RIP-2M]. | [RIP-1] (default) |
| Once you have completed filling in the Network Layer Options Menu, press [Enter] to return to Menu 11. Press [Enter] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] at any time to cancel. | | |

### 5.1.2 Static Route Setup

Static routes tell the *Prestige* routing information that it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN or a remote network is beyond the one that is directly connected to a remote node.

Each remote node specifies only the network to which the gateway is directly connected, and the *Prestige* has no knowledge of the networks beyond. For instance, the *Prestige* knows about network N2 in the following diagram through remote node R. However, the *Prestige* is unable to route a packet to network N3 because it doesn't know that there is a route through remote node R. The static routes are for you to tell the *Prestige* about the networks beyond the remote nodes.

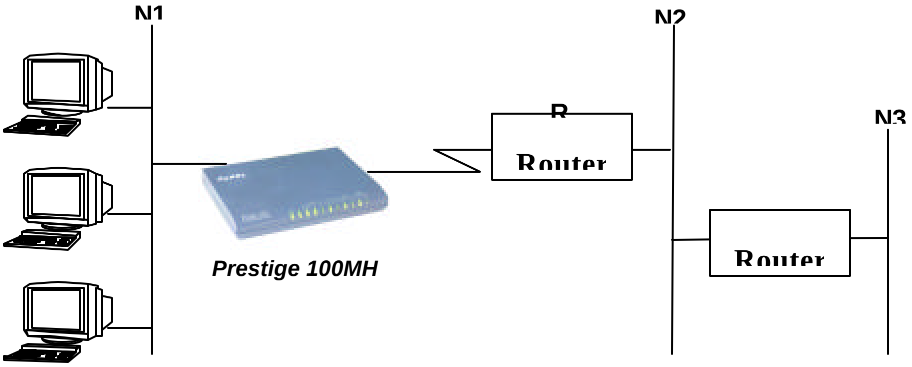
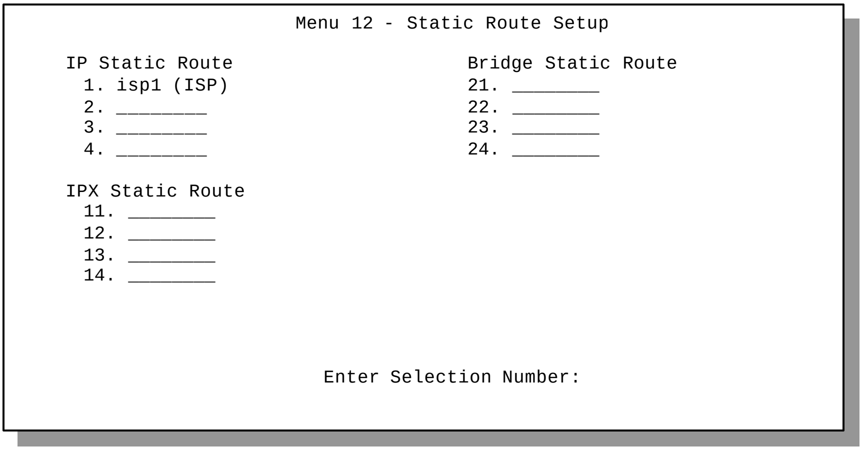


**Figure 5-4. Example of Static Routing Topology**

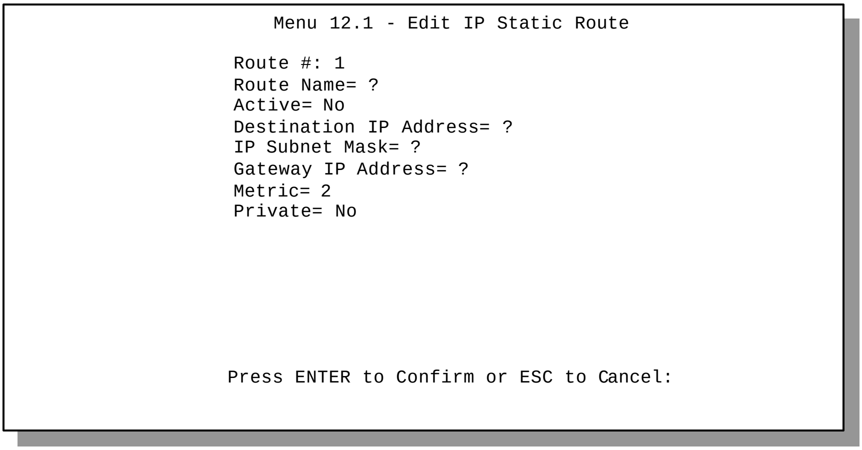
To configure an IP static route, use Menu 12, Static Route Setup, as displayed in Figure 5-5.



```
                       Menu 12 - Static Route Setup

     IP Static Route                     Bridge Static Route
       1. isp1 (ISP)                     21. ________
       2. ________                       22. ________
       3. ________                       23. ________
       4. ________                       24. ________

     IPX Static Route
       11. ________
       12. ________
       13. ________
       14. ________



                         Enter Selection Number:
```

**Figure 5-5. Menu 12 - Static Route Setup**

From Menu 12, select one of the available IP static routes to open Menu 12.2 - Edit IP Static Route, as shown in Figure 5-6.



```
                     Menu 12.1 - Edit IP Static Route

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






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

**Figure 5-6. Menu 12.1 - Edit IP Static Route**

Table 5-3 describes the fields for Menu 12.1 - Edit IP Static Route Setup.

**Table 5-3. Edit IP Static Route Menu Fields**

| **Field** | **Description** |
|---|---|
| Route Name | Enter a descriptive name for this route. This is for identification purpose only. |
| Active | This field allows you to activate/deactivate this static route. |
| Destination IP Address | This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. |
| IP Subnet Mask | Enter the subnet mask for this destination. Follow the discussion on IP subnet mask in this chapter. |
| 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 | Same meaning as those in the Remote Node Setup (*See* Table 6-3). |
| Private | Same meaning as those in the Remote Node Setup (*See* Table 6-3). |

# Chapter 6
# IPX Configuration

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

## 6.1 IPX Network Environment

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

### 6.1.1 Network and Node Number

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

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

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

### 6.1.2 Frame Types

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

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.

### 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* 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.

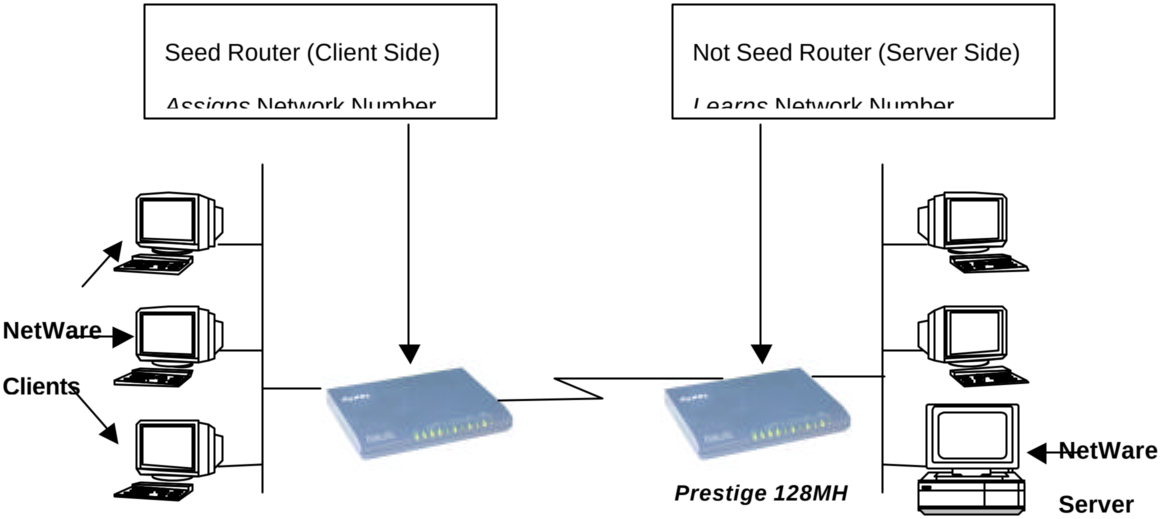


**Figure 6-1. *Prestige* in an IPX Environment**

### 6.2.1 Prestige 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* on LAN without Server

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

## 6.3 IPX Spoofing

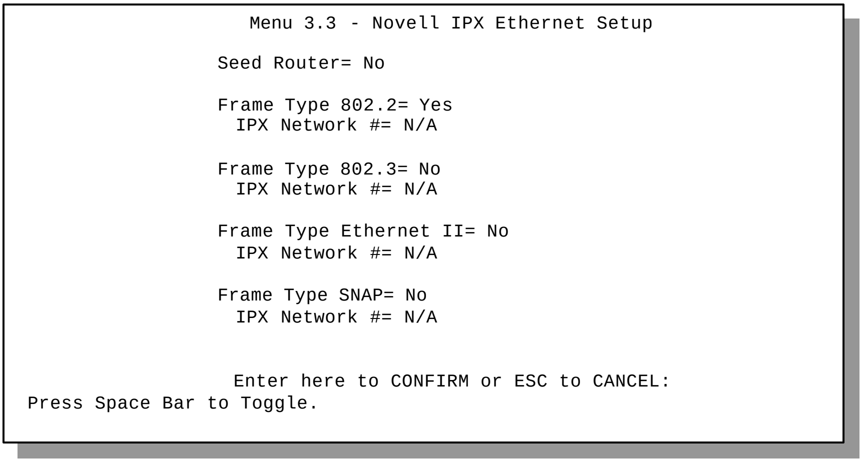
Your *Prestige* comes with several pre-defined call filters designed to prevent certain IPX packets from triggering a call to a remote node.

The built-in call filters are defined as follows:

- Block periodical RIP (Routing Information Protocol) and SAP (Service Advertising Protocol) response messages.
- Block NetWare serialization packets.
- Allow SAP and RIP inquiry packets.

## 6.4 IPX Ethernet Setup

From Menu 3 - Ethernet Setup, select option **[3. Novell IPX Setup]** to go to Menu 3.3 - Novell IPX Ethernet Setup as shown in Figure 6-2.



```
                    Menu 3.3 - Novell IPX Ethernet Setup

                 Seed Router= No

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

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

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

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


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

**Figure 6-2. Menu 3.3 - Novell IPX Ethernet Setup**

The following Table 6-1 describes the Novell IPX Ethernet Setup Menu.

**Table 6-1. Novell IPX Ethernet Setup Fields**

| **Field** | **Description** | **Options** |
|---|---|---|
| Seed Router | Determine if your *Prestige* is to act as a seed router. | [Yes/No] |
| Frame Type | Enable/Disable the individual frame type. Remember to enable only the ones that are actually used on your network. | [802.2]<br>[802.3]<br>[Ethernet II]<br>[SNAP] |
| IPX Network # | If your *Prestige* is a seed router, enter a unique network number for each frame type enabled. | |
| Press [Enter] at the message [Press ENTER to Confirm ...] to save your configuration, or press [Esc] at any time to cancel. | | |

## 6.5 LAN-to-LAN Application with Novell IPX

A typical LAN-to-LAN application is to use your *Prestige* to call from a branch office to the corporate headquarters to enable the stations in the branch office to access the NetWare servers at the headquarters, as depicted in Figure 6-3.

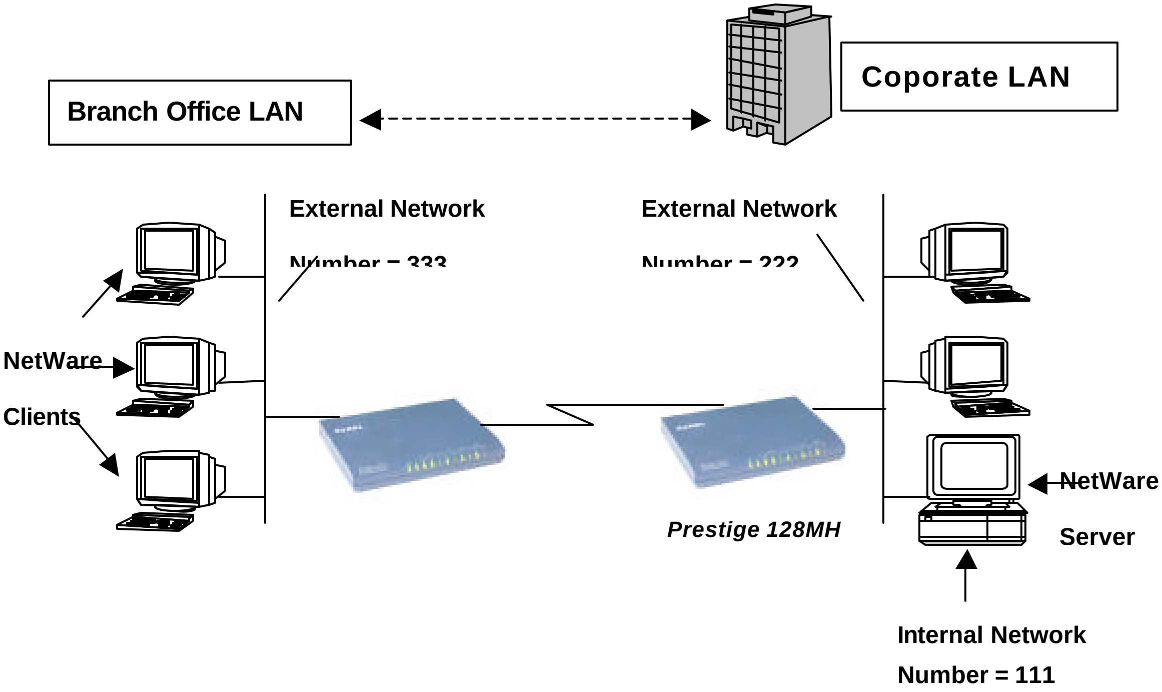


**Figure 6-3. LAN-to-LAN Application with Novell IPX**

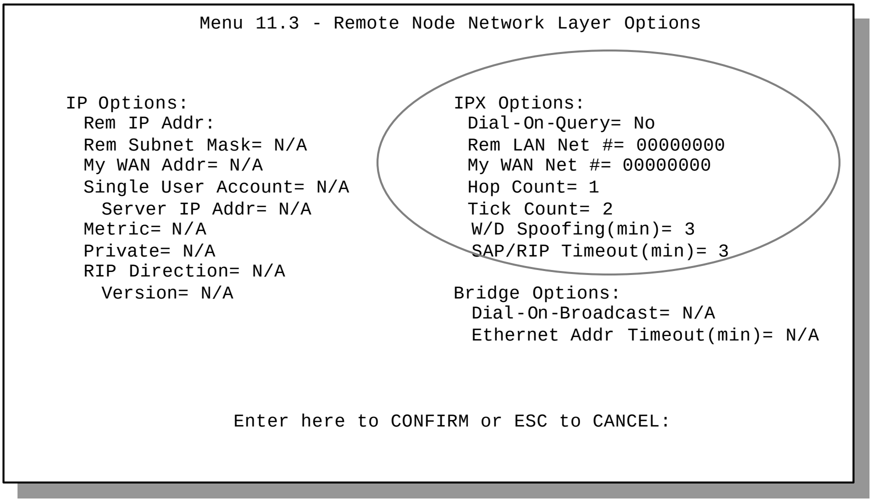
## 6.5.1 IPX Remote Node Setup

Follow the procedure in *Chapter 5* to configure the protocol-independent parameters in Menu 11.1 - Remote Node Profile. For the IPX-specific parameters in Menu 11.3 - Remote Node Network Layer Options, follow the instructions below. If you want the *Prestige* to receive incoming calls, you must also configure the default dial-in parameters in Menu 13.

To edit Menu 11.3 - Remote Node Network Layer Options shown in Figure 6-4, follow these steps:

**Step 3.** In Menu 11.1, make sure **[IPX]** is among the protocols in the Route field. (The Route field should display Route = IPX or Route = IP + IPX.)

**Step 4.** Move the cursor to the [Edit IP/IPX/Bridge] field, then press the space bar to select [Yes] and press [Enter] to open Menu 11.3 - Network Layer Options.



```
                Menu 11.3 - Remote Node Network Layer Options


    IP Options:                           IPX Options:
      Rem IP Addr:                          Dial-On-Query= No
      Rem Subnet Mask= N/A                  Rem LAN Net #= 00000000
      My WAN Addr= N/A                      My WAN Net #= 00000000
      Single User Account= N/A              Hop Count= 1
        Server IP Addr= N/A                 Tick Count= 2
      Metric= N/A                           W/D Spoofing(min)= 3
      Private= N/A                          SAP/RIP Timeout(min)= 3
      RIP Direction= N/A
        Version= N/A                      Bridge Options:
                                            Dial-On-Broadcast= N/A
                                            Ethernet Addr Timeout(min)= N/A



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

**Figure 6-4. Menu 11.3 - Remote Node Novell IPX Options**

Table 6-2 describes the IPX-specific parameters of the remote node setup.

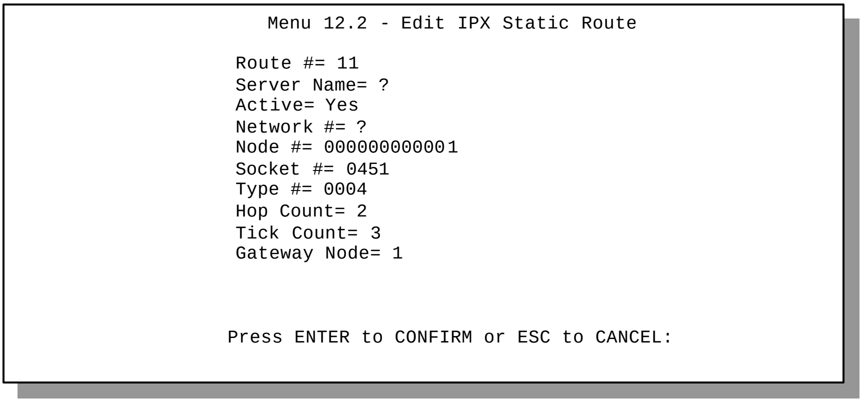
**Table 6-2. Remote Node Novell IPX Options**

| Field | Description | Option |
|---|---|---|
| Dial-On-Query | This field is necessary for your *Prestige* on the client side. When set to [Yes], any Get Service SAP or RIP broadcasts will trigger your *Prestige* to make a call to that remote node. | [Yes/No] |
| Rem LAN Net # | In this field, enter the internal network number of the NetWare server on the remote LAN. | |
| My WAN Net # | In this field, enter the network number of the WAN link. If you leave this field as [00000000], your *Prestige* will determine automatically the network number through negotiation with the PPP peer. | [00000000]<br>(default) |
| Hop Count | This field indicates the number of intermediate networks that must be passed through to reach the remote node. | [1]<br>(default) |
| Tick Count | This field indicates the time-ticks required to reach the remote node. | [2] (default) |
| W/D Spoofing (min) | This field is for the *Prestige* on the server side. Your *Prestige* can spoof a response to a server's WatchDog request after the connection is dropped. In this field, type in the time (number of minutes) that you want your *Prestige* to spoof the WatchDog response. | |
| SAP/RIP Timeout (min) | This field indicates the amount of time that you want your *Prestige* to maintain the SAP and RIP entries learned from this remote node in its internal tables after the connection has been dropped. If this information is retained, then your *Prestige* will not have to get the SAP information when the line is brought back up. Enter the time (number of minutes) in this field. | |
| Once you have completed filling in the Network Layer Options Menu, press [Enter] to return to Menu 11.1. Then press [Enter] at the message [Press ENTER to Confirm] to save your configuration, press [Esc] to cancel. | | |

## 6.5.2 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.

From Menu 12, select one of the IPX Static Routes to open Menu 12.2 - Edit IPX Static Route, as shown in Figure 6-5.



```
                        Menu 12.2 - Edit IPX Static Route

                     Route #= 11
                     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 6-5. Menu 12.2 - Edit IPX Static Route**

Table 6-3 contains the instructions on how to configure the Edit IP Static Route Menu.

**Table 6-3. Edit IPX Static Route Menu Fields**

| **Field** | **Description** |
|---|---|
| Server Name | In this field, enter the name of the server. This must be the *exact* name configured in the NetWare server**.** |
| Network # | This field contains the internal network number of the remote server that you wish to access. [00000000] or [FFFFFFFF] are reserved. |
| Node # | This field contains the address of the node on which the server resides. If you are using a Novell IPX implementation, this value is [000000000001]. |
| Socket # | This field contains the socket number on which the server will receive service requests. The default for this field is hex [0451]. |
| Type # | This field identifies the type of service the server provides. The default for this field is hex [0004]. |
| Gateway Node | In this field, enter the number of the remote node that is the gateway for this static route. |
| Hop Count and Tick Count | These two fields have the same meaning as those in the Ethernet setup. |
| Once you have completed filling in the menu, press [Enter] at the message [Press ENTER to Confirm…] to save your configuration, or press [Esc] to cancel to cancel. | |

# Chapter 7
# Bridging Setup

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

## 7.1 Bridging in General

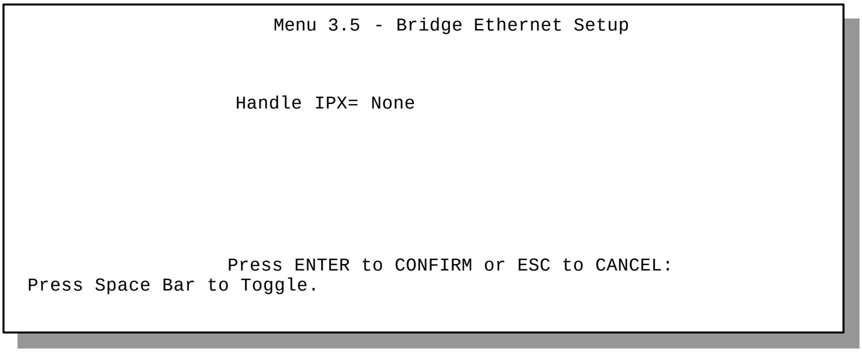
Bridging bases the forwarding decision on the MAC (Media Access Control), or hardware, address, while routing does it on the network layer (IP or IPX) address. Bridging allows the *Prestige* to transport packets of network layer protocols that the *Prestige* does not route, e.g., SNA, from one network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

For efficiency reason, 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.

From Menu 3 - Ethernet Setup, enter option **[4. Bridge Setup]** and Menu 3.5 - Bridge Ethernet Setup displays as shown in Figure 7-1.



```
                         Menu 3.5 - Bridge Ethernet Setup


                     Handle IPX= None








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

**Figure 7-1. Menu 3.5 - Bridge Ethernet Setup**

Table 7-1 describes how to configure the [Handle IPX] field in Menu 3.5.

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

| **Handle IPX Field**<br>**(Menu 3.5)** | **Description** |
|---|---|
| None | When there is no IPX traffic on the LAN or when you do not want to apply any special handling for IPX. |
| Client | When there are only client workstations on the LAN. RIP and SAP (Service Advertising Protocol) response packets will not trigger calls. |
| Server | When there are only IPX servers on the LAN. No RIP or SAP packets will trigger calls. In addition, during the time when the line is down, your *Prestige* 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 aged out, there is no need to maintain its connection to the IPX server. |

If there are both clients and servers on the LAN, and the local clients will access the remote servers, set this field to **Server** but turn on the **Dial-On-Broadcast** parameter in Menu 11.3 to allow the client queries to trigger calls.

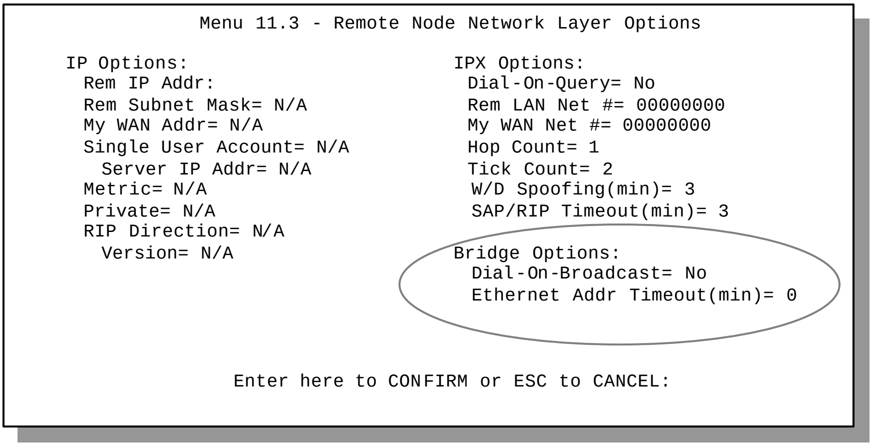
### 7.2.1 Remote Node Bridging Setup

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

To setup Menu 11.3 - Remote Node Network Layer Options shown in Figure 7-2, follow these steps:

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

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



```
                 Menu 11.3 - Remote Node Network Layer Options

     IP Options:                               IPX Options:
       Rem IP Addr:                              Dial-On-Query= No
       Rem Subnet Mask= N/A                      Rem LAN Net #= 00000000
       My WAN Addr= N/A                          My WAN Net #= 00000000
       Single User Account= N/A                  Hop Count= 1
         Server IP Addr= N/A                     Tick Count= 2
       Metric= N/A                                W/D Spoofing(min)= 3
       Private= N/A                               SAP/RIP Timeout(min)= 3
       RIP Direction= N/A
         Version= N/A                          Bridge Options:
                                                  Dial-On-Broadcast= No
                                                  Ethernet Addr Timeout(min)= 0


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

**Figure 7-2. Menu 11.3 - Remote Node Bridging Options**

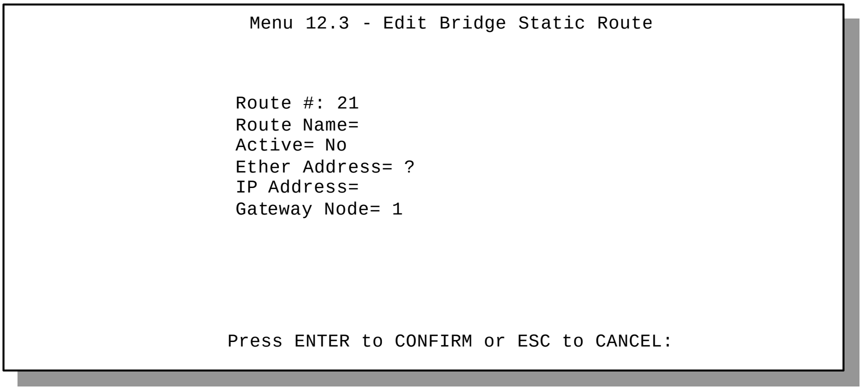
Table 7-2 describes the bridging-specific parameters in the Remote Node Profile and Network Layers menus.

**Table 7-2. Remote Node Network Layers Menu Bridge Options**

| **Field** | **Description** |
|---|---|
| Bridge | Make sure this field is set to [Yes]. |
| Edit IP/IPX/Bridge | Press the space bar to change it to [Yes] and press [Enter] to go to the Network Layer Options Menu. |
| Dial-On-Broadcast | 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) | In this field, enter the time (number of minutes) that you wish your *Prestige* to retain the Ethernet Addr information in its internal tables while the line is down. If this information is retained, your *Prestige* will not have to recompile the tables when the line is brought back up. |
| Once you have completed filling in the 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* about the route to a node before a connection is established. You configure bridge static routes in Menu 12.3, as shown in Figure 7-3.



```
                    Menu 12.3 - Edit Bridge Static Route



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






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

**Figure 7-3. Menu 12.3 - Edit Bridge Static Route**

The following Table 7-3 describes the Bridge Static Route Menu.

**Table 7-3. Bridge Static Route Menu Fields**

| **Field** | **Description** |
|---|---|
| Route Name | Enter a name for the bridge static route for identification purposes. |
| Active | Activate/deactivate the static route. |
| Ether Address | Enter the MAC address of the destination machine that you wish to bridge the packets to. |
| IP Address | If available, enter the IP address of the destination machine that you wish to bridge the packets to. |
| Gateway Node | Enter the number of the remote node that is the gateway of this static route. When a packet’s destination Ethernet (MAC) address matches the value entered above, it will trigger a call to this remote node. |
| 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 8

# Dial-in Server Configuration

You can configure your *Prestige* to receive calls from remote dial-in users, e.g., telecommuters, as well as remote nodes. There are several differences between dial-in users and remote nodes, as summarized in Table 8-1.

**Table 8-1. Remote Dial-in Users/Remote Nodes Comparison Chart**

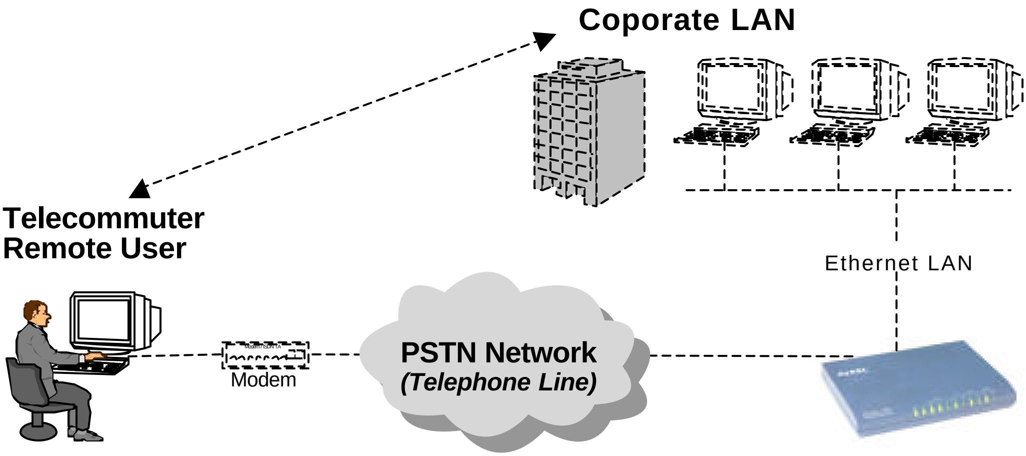
| **Remote Dial-in Users** | **Remote Nodes** |
|---|---|
| Your *Prestige* will only answer calls from remote dial-in users; it will not make call to them. | Your *Prestige* can make calls to and receive calls from the remote node. |
| All remote dial-in users share one common set of parameters, as defined in the Default Dial In Setup (Menu 13). | Each remote node can have its own set of parameters such as Bandwidth On Demand, Protocol, Security, etc. |

This chapter discusses how to setup default dial-in parameters for both remote node and remote dial-in users. The following sections give two examples of how your *Prestige* can be configured as a dial-in server.

Due to memory constraints, your *Prestige* can only store a finite number of users locally. If there are more remote dial-in users than what *Prestige* can support locally, you can use an external RADIUS server to provide authentication service. For details on using a RADIUS server, see the *Using RADIUS Authentication* section in *Chapter 11 - System Security*.

## 8.1 Remote Access Server

Telecommuting enables people to work at remote sites and yet still have access to the resources in the business office. Typically, a telecommuter will use a client workstation with TCP/IP and dial-out capabilities, e.g., a Windows PC or a Macintosh, connected to a modem. For telecommuters to call in to your *Prestige*, you need to configure a dial-in user profile for each telecommuter. Additionally, you need to configure the Default Dial-In Setup to set the operational parameters for all dial-in users.

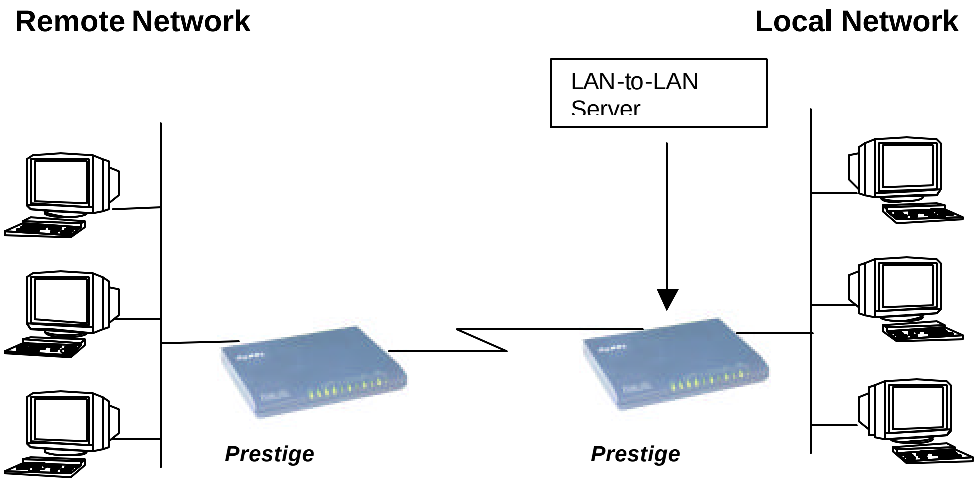


An example of remote access server for telecommuters is shown in Figure 8-1.

**Figure 8-1. Example of Telecommuting**

## 8.2 LAN-to-LAN Server Application

Your *Prestige* can also be used as a dial-in server for LAN-to-LAN application to provide access for the workstations on a remote network. For your *Prestige* to be set up as a LAN-to-LAN server, you need to configure the Default Dial-In Setup to set the operational parameters for incoming calls. Additionally, you must create a remote node for the router on the remote network (*see* *Chapter 5 - Remote Node Configuration*).

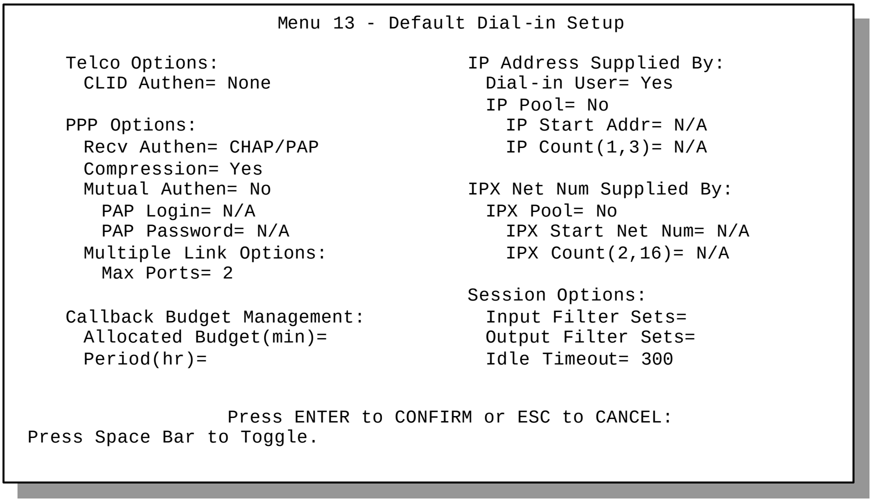


An example of your *Prestige* being used as a LAN-to-LAN server is shown in Figure 8-2.

**Figure 8-2. Example of a LAN-to-LAN Server Application**

## 8.3 Default Dial-In Setup

This section covers the default dial-in parameters. The parameters in Menu 13 affect incoming calls from both remote dial-in users, and remote nodes until authentication is completed. Once authentication is completed and if it matches a remote node, your *Prestige* will use parameters from that particular remote node.



```
                      Menu 13 - Default Dial-in Setup

   Telco Options:                         IP Address Supplied By:
     CLID Authen= None                      Dial-in User= Yes
                                            IP Pool= No
   PPP Options:                               IP Start Addr= N/A
     Recv Authen= CHAP/PAP                    IP Count(1,3)= N/A
     Compression= Yes
     Mutual Authen= No                    IPX Net Num Supplied By:
       PAP Login= N/A                       IPX Pool= No
       PAP Password= N/A                      IPX Start Net Num= N/A
     Multiple Link Options:                   IPX Count(2,16)= N/A
       Max Ports= 2
                                          Session Options:
   Callback Budget Management:              Input Filter Sets=
     Allocated Budget(min)=                 Output Filter Sets=
     Period(hr)=                            Idle Timeout= 300


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

**Figure 8-3. Menu 13 - Default Dial-in Setup**

From the Main Menu, enter 13 to go to Menu 13 - Default Dial-in Setup. This section describes how to configure the protocol-independent fields in this menu. For the protocol-dependent fields, refer to the appropriate chapters.

Table 8-2 describes and contains information on how to configure each parameter in Menu 13 - Default Dial-in Setup.

**Table 8-2. Default Dial-in Setup Fields**

| Field | Description | Option |
|---|---|---|
| Telco Options: CLID Authen | This field sets the CLID authentication parameter for all incoming calls. There are three options for this field:<br>● None - No CLID is required.<br>● Required – CLID must be available, or the Prestige will not answer the call.<br>● Preferred - If the CLID is available then CLID will be used; otherwise, authentication is performed in PPP negotiation. | [None]<br>[Required]<br>[Preferred] |
| PPP Options: Recv. Authen | This field sets the authentication protocol for incoming calls. For security reason, setting authentication to none is strongly discouraged. Options for this field are:<br>● CHAP/PAP - Your *Prestige* will try CHAP first, but PAP will be used if CHAP is not available.<br>● CHAP – Use CHAP only.<br>● PAP – Use PAP only.<br>● None – Your *Prestige* tries to acquire CHAP/PAP first, but no authentication is required if CHAP/PAP is not available. | [CHAP/PAP]<br>[CHAP]<br>[PAP]<br>[None] |
| PPP Options: Mutual Authen | Some vendors, e.g., Cisco, require mutual authentication, i.e., the node that initiates the call will request a user name and password from the far end that it is dialing to. If the remote node requires mutual authentication, set this field to Yes. | [Yes/No] |
| PAP Login | This field is applicable only if the Mutual Authen. Field is set to [Yes]. Enter in the login name to be used to respond to the far end's PAP authentication request. This field does not apply to CHAP authentication. | |
| PAP Password | This field is applicable only if the Mutual Authen. Field is set to [Yes]. Enter in the PAP password to be used to respond to the far end's authentication request. This field does not apply to CHAP authentication. | |

**Table 8-2. Default Dial-in Setup Fields (continued)**

| Field | Description | Option |
|---|---|---|
| Multiple Link Options: Max Port | Enter the maximum number of ports in an MP bundle between your *Prestige* and a remote dial-in user. | Default = 1 |
| Callback Budget Management: Allocated Budget (min) | This field sets the budget callback time for all the remote dial-in users. The default for this field is [0] for no budget control. | Default = 0 |
| Callback Budget Management: Period (hr) | This field sets the time interval to reset the above callback budget control. | |
| Dial-In IP Address Supplied By: Dial-in User | If set to [Yes], the *Prestige* will allow a remote host to specify its own IP address.<br>If set to [No], the remote host must use the IP address assigned by your *Prestige* from the IP pool, configured below. This is to prevent the remote host from using an invalid IP address and potentially disrupting the whole network. | (Default = Yes)<br>[Yes/No] |
| Dial-In IP Address Supplied By: IP Pool | This field tells your *Prestige* to provide the remote host with an IP address from the pool. This field is required if Dial-In IP Address Supplied By: Dial-in User is set to [No]. You can configure this field even if Dial-in User is set to [Yes], in which case your *Prestige* will accept the IP address if the remote peer specifies one; otherwise, an IP address is assigned from the pool. | [Yes/No]<br>(Default = No) |
| IP Pool: IP Start Addr | This field is applicable only if you selected [Yes] in the Dial-In IP Address Supplied By: IP Pool field.<br>The IP pool contains contiguous IP addresses and this field specifies the first one in the pool. | |
| IP Count (1-3) | In this field, enter the number ([1], [2], or [3]) of addresses in the IP Pool. For example, if the starting address is 192.168.135.5 and the count is [2], then the pool will have 192.68.135.5 and 192.68.135.6 | [1], [2], [3] |

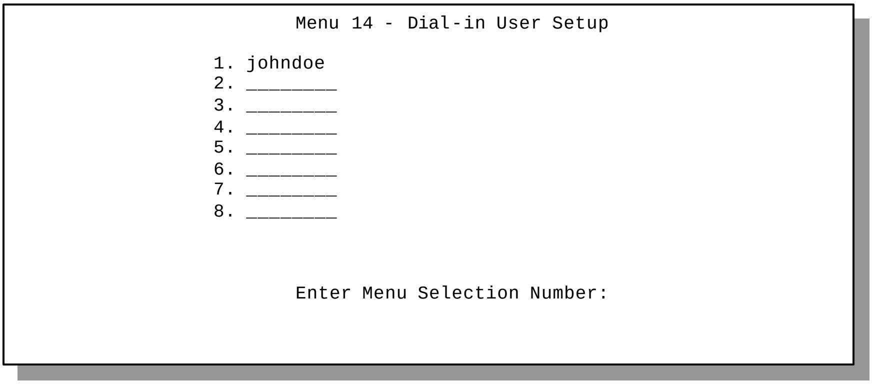
**Table 8-2. Default Dial-in Setup Fields (continued)**

| Field | Description | Option |
|---|---|---|
| Dial-In IPX Net. Num. Supplied By: IPX Pool | This field tells your *Prestige* to provide the remote host with an IPX network number from the pool. Otherwise, your *Prestige* will generate a random IPX network number. | [Yes/No]<br>(Default = No) |
| IPX Start Net. Num. | This field is applicable only if you selected [Yes] in the Dial-In IPX Net. Num. Supplied By: IPX Pool field. The IPX pool contains contiguous IPX network numbers and this field specifies the first one in the pool. | |
| IPX Count (1,16) | Enter the number ([1] - [16]) of network numbers in the IPX Pool. For example, if the starting number is 12345678, and the count is [2], then the IPX pool will have 12345678 and 12345679. | [1] to [16] |
| Session Options:<br>Input Filter Sets<br>Output Filter Sets | Enter the filter set(s) to apply to the incoming and outgoing traffic between your *Prestige* and the remote dial-in user. Keep in mind that the filter set(s) will only apply to remote dial-in users but not the remote nodes.<br>You can choose from 12 different filter sets. In addition, you can link up to 4 filter sets together for further customization (for example, 1, 5, 9, 12).<br>Note that spaces and [-] symbol, are accepted in this field. For more information on customizing your filter sets, *see Chapter 9 - Filter Configuration*. The default is blank, i.e., no filters. | Default = blank |
| Session Options:<br>Idle Timeout | This value is the number of idle seconds that elapses before the dial-in user is automatically disconnected when the *Prestige* is calling back. Idle The idle timer is reset whenever there is traffic from the *Prestige*.<br>This field will only be used when calling back; otherwise, the idle timeout is governed by the caller. | |
| Once you have completed filling in Menu 13 - Default Dial-in Setup, press [Enter] at the message [Press ENTER to Confirm…] to save your configuration, or press [Esc] at any time to cancel. | | |

## 8.4 Dial-In Users Setup

The following steps describe the setup procedure for setting up a remote dial-in user.

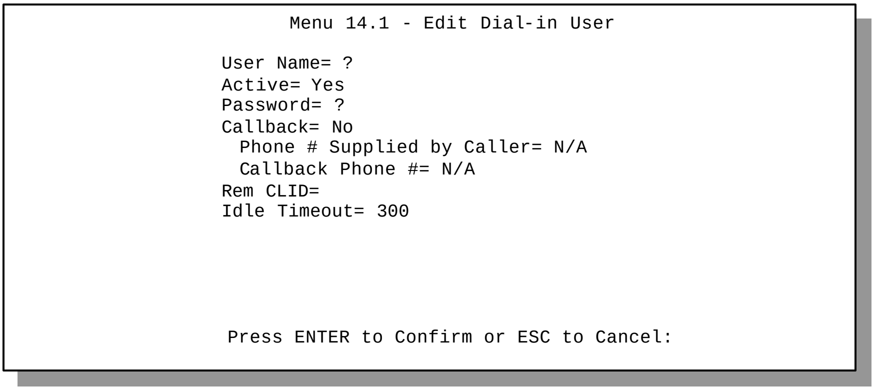
**Step 1.** From the Main Menu, enter option 14 to go to Menu 14 - Dial-in User Setup, as shown in Figure 8-4.



```
                    Menu 14 - Dial-in User Setup

              1. johndoe
              2. ________
              3. ________
              4. ________
              5. ________
              6. ________
              7. ________
              8. ________



                    Enter Menu Selection Number:
```

**Figure 8-4. Menu 14 - Dial-in User Setup**

**Step 2.** Select one of users by number, this will bring you to Menu 14.1 - Edit Dial-in User, as shown in Figure 8-5.



```
                    Menu 14.1 - Edit Dial-in User

              User Name= ?
              Active= Yes
              Password= ?
              Callback= No
                Phone # Supplied by Caller= N/A
                Callback Phone #= N/A
              Rem CLID=
              Idle Timeout= 300




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

**Figure 8-5. Menu 14.1 - Edit Dial-in User**

Table 8-3 provides instructions on how to fill in the Edit Dial-In User fields.

**Table 8-3. Edit Dial-in User Menu Fields**

| **Field** | **Description** | **Option** |
|---|---|---|
| User Name | This is a required field. This will be used as the login name for authentication. Choose a descriptive word for login, for example, [johndoe]. | |
| Active | You can disallow dial-in access to this user by setting this field to [Inactive]. Inactive users are displayed with a [-] (minus sign) at the beginning of the name in Menu 14. | [Active]<br>[Inactive] |
| Password | Enter the password for the remote dial-in user. | |
| Callback | This field determines if your *Prestige* will allow call back to this user upon dial-in. If this option is enabled, your *Prestige* will call back to the user if requested. In such a case, your *Prestige* will disconnect the initial call from this user and dial back to the specified callback number (see below).<br>● [No] - The default is [no callback].<br>● [Optional] - The user can choose to disable callback.<br>● [Mandatory] - The user can not disable callback. | Default=No<br>[No]<br>[Optional]<br>[Mandatory] |
| Phone # Supplied by Caller | This option allows the user to specify the call back telephone number on a call-by-call basis. This is useful when your *Prestige* returns a call back to a mobile user at different numbers, e.g., a sales rep. In a hotel.<br>● If the setting is [Yes], the user can specify and send to the *Prestige* the callback number of his/her choice.<br>● The default is [No], i.e., your *Prestige* always calls back to the fixed callback number. | Default=No<br>[Yes]<br>[No] |
| Callback Phone # | If [Phone # Supplied by Caller] is [Yes], then this is a required field. Otherwise, a [N/A] will appear in the field. Enter the telephone number to which your *Prestige* will call back. | |

**Table 8-3. Edit Dial-in User Menu Fields (continued)**

| Field | Description | Option |
|---|---|---|
| Rem CLID | If you enable CLID Authen field in Menu 13, then you need to specify the telephone number from which this user calls. Your *Prestige* wil check the CLID in the incoming call against the CLIDs in the database. If they do not match and CLID Authen is Required, your *Prestige* will not answer the call. | |
| Idle Time-out | Enter the idle time (in seconds). This time-out determines how long the dial-in user can be idle before your *Prestige* disconnects the call when the *Prestige* is calling back.<br>Idle time is defined as the period of time where there is no data traffic between the dial-in user and your *Prestige*. The default is 300 seconds (5 minutes). | Default=300 seconds |
| Once you have completed filling in Menu 14.1 - Edit Dial-in User, press [Enter] at the message [Press ENTER to Confirm…] to save your configuration, or press [Esc] at any time to cancel. | | |

## 8.5 CLID Authentication

CLID (Calling Line IDentification) authentication affords you the security of limiting a user to only initiate connections from a fixed location. The *Prestige* uses the caller ID sent by the switch to match against the CLIDs in the database. Please note that for CLID authentication to work on the *Prestige*, your telephone company must support caller ID. You must also include the AT command in the [initAT] string in Menu 2 to enable caller ID detection on the modem.

## 8.6 Callback

Callback serves two purposes. One is security. When set to callback to a fixed number, an intruder will not gain access to your network even if he/she stole the password from your user, because the *Prestige* always calls back to the pre-configured number.

The other is ease of accounting. For instance, your company pays for the connection charges for telecommuting employees and you use your *Prestige* as the dial in server. When you turn on the callback option for the dial-in users, all usage are charged to the company instead of the employees, and your accounting department can avoid the hassles of accountability and reimbursement.

# Chapter 9
# Filter Configuration

## 9.1 About Filtering

Your *Prestige* uses filters to decide whether or not to allow passage of a data packet and/or to make a call. There are two types of filters: data filters and call filters.

Data filters screen the data to determine if the packet should be allowed to pass. Data filters are further divided into incoming and outgoing filters, depending on the direction of the packet direction relative to a port. Call filters are used to determine if a packet should be allowed to trigger a call.

Outgoing packets must pass through the data filters before they encounter the call filters. Call filters are divided into two groups, the built-in call filters and user-defined call filters. Your *Prestige* has built-in call filters that prevent administrative, e.g., RIP and SAP (Service Advertising Protocol), packets from triggering calls. These filters are always enabled and not accessible to you. Your *Prestige* applies the built-in filters first and then the user-defined call filters, if applicable, as illustrated in Figure 9-1, *Outgoing Packet Filtering Process*.

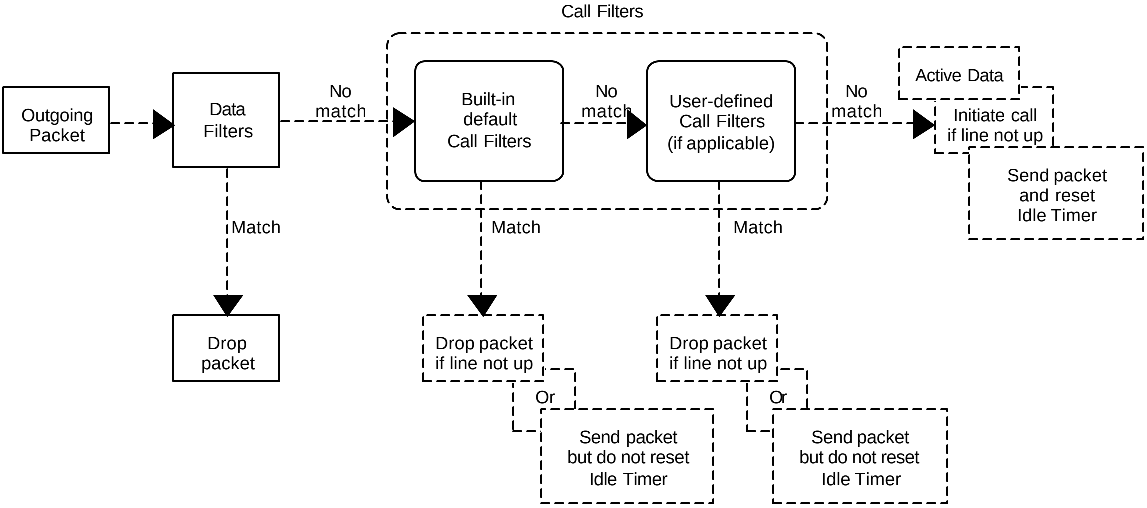

Call Filters
Outgoing Packet
Data Filters
No match
Built-in default Call Filters
No match
User-defined Call Filters (if applicable)
No match
Active Data
Initiate call if line not up
Send packet and reset Idle Timer
Match
Match
Match
Drop packet
Drop packet if line not up
Or
Send packet but do not reset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

**Figure 9-1. Outgoing Packet Filtering Process**

For incoming packets, your *Prestige* applies data filters only. Packets are processed depending upon whether a match is found. The following sections describe how to configure filter sets.

## The Filter Structure of the *Prestige*

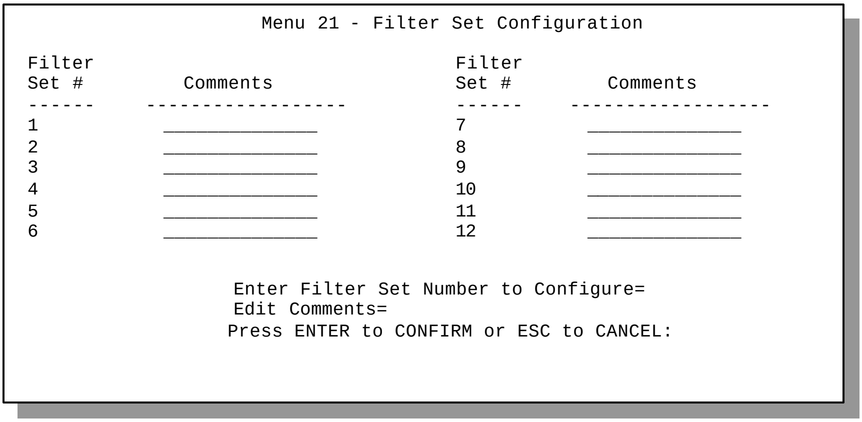
A filter set consists of one or more filter rules. Usually, you would group related rules, e.g., all the rules for NetBIOS, into a single set and give it a descriptive name. The *Prestige* allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system.

You 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.

## 9.2 Configuring a Filter Set

To configure a filter sets, follow the procedure below:

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



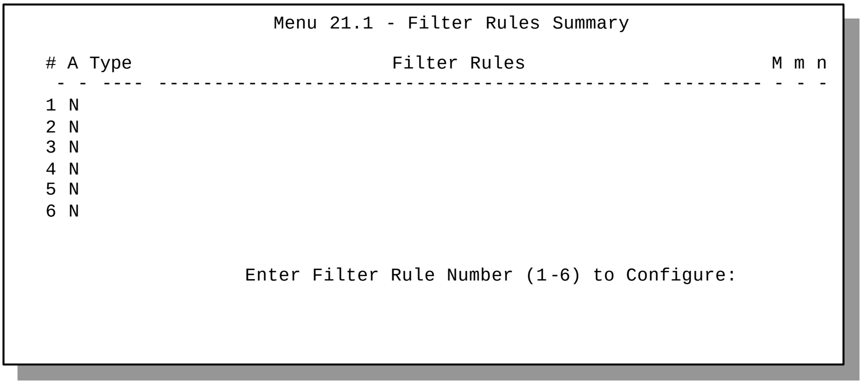
```
                     Menu 21 - Filter Set Configuration

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


                   Enter Filter Set Number to Configure=
                   Edit Comments=
                  Press ENTER to CONFIRM or ESC to CANCEL:
```

**Figure 9-2. Menu 21 - Filter Set Configuration**

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

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

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



```
                    Menu 21.1 - Filter Rules Summary

   # A Type                     Filter Rules                      M m n
    - - ---- ------------------------------------------- --------- - - -
   1 N
   2 N
   3 N
   4 N
   5 N
   6 N


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

**Figure 9-3.  Menu 21.1 - Filter Rules Summary**

## 9.2.1 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 Menu 21.1.

**Table 9-1.  Abbreviations Used in the Filter Rules Summary Menu**

| Abbreviations | Description | Display |
|---|---|---|
| # | Refers to the filter rule number (1-6). | |
| A | Refers to Active. | [Y] means the filter rule is active.<br>[N] means the filter rule is inactive. |
| Type | Refers to the type of filter rule.<br>This shows GEN for generic, IP for TCP/IP and IPX for Novell IPX. | [GEN] for Generic<br>[IP] for TCP/IP<br>[IPX] for Novell IPX |

**Table 9-1. Abbreviations Used in the Filter Rules Summary Menu (continued)**

| Abbreviations | Description | Display |
|---|---|---|
| Filter Rules | The filter rule parameters will be displayed here (see below). | |
| M | Refers to More. | [Y] means there are more rules to check.<br>[N] means there are no more rules to check. |
| m | Refers to Action Matched. | [F] means to forward the packet.<br>[D] means to drop the packet.<br>[N] means check the next rule. |
| n | Refers to Action Not Matched | [F] means to forward the packet.<br>[D] means to drop the packet.<br>[N] means check the next rule. |

The protocol dependent filter rules abbreviation are listed as follows:

- If the filter type is IP, the following abbreviations listed in Table 9-2 will be used.

**Table 9-2. Abbreviations Used If Filter Type Is IP**

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

- If the filter type is IPX, the following abbreviations listed in Table 9-3 will be used.

**Table 9-3.        Abbreviations Used If Filter Type Is IPX**

| **Abbreviation** | **Description** |
|---|---|
| PT | IPX Packet Type |
| SS | Source Socket |
| DS | Destination Socket |

- If the filter type is GEN (generic), the following abbreviations listed in Table 9-4 will be used.

**Table 9-4.        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.

## 9.3 Configuring a Filter Rule

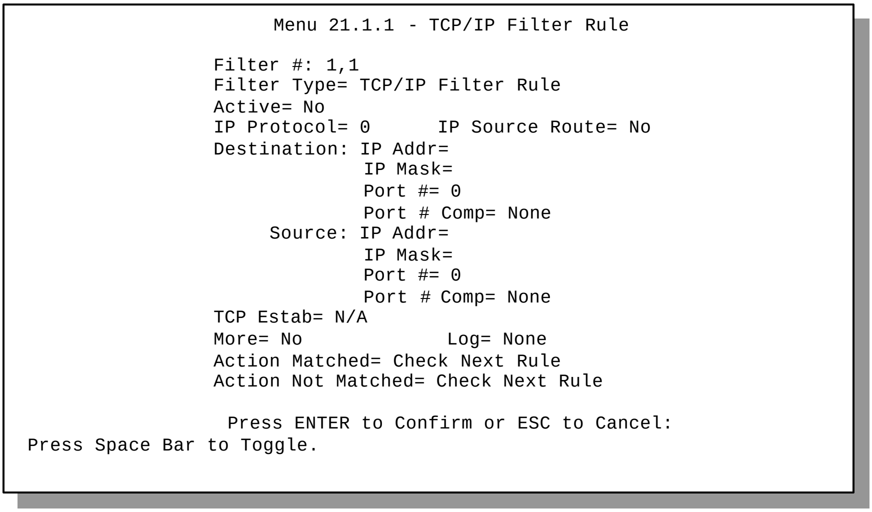
To configure a filter rule, enter its number in Menu 21.1 - Filter Rules Summary and press Enter to open Menu 21.1.1 for the rule.

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

### 9.3.1 TCP/IP Filter Rule

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

To configure a TCP/IP 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 in Figure 9-4.



```
                      Menu 21.1.1 - TCP/IP Filter Rule

                 Filter #: 1,1
                 Filter Type= TCP/IP Filter Rule
                 Active= No
                 IP Protocol= 0      IP Source Route= No
                 Destination: IP Addr=
                              IP Mask=
                              Port #= 0
                              Port # Comp= None
                      Source: IP Addr=
                              IP Mask=
                              Port #= 0
                              Port # Comp= None
                 TCP Estab= N/A
                 More= No             Log= None
                 Action Matched= Check Next Rule
                 Action Not Matched= Check Next Rule

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

**Figure 9-4. Menu 21.1.1 - TCP/IP Filter Rule**

The following Table 9-5 describes how to configure your TCP/IP filter rule.

**Table 9-5.   TCP/IP Filter Rule Menu Fields**

| **Field** | **Description** | **Option** |
|---|---|---|
| Active | This field activates/deactivates the filter rule. | [Yes/No] |
| IP Protocol | Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. This value must be between 0 and 255 | [0-255] |
| IP Source Route | If Yes, the rule applies to packet with IP source route option; else the packet must not have source route option. The majority of IP packets do not have source route. | [Yes/No] |
| Destination: IP Addr | Enter the destination IP Address of the packet you wish to filter. This field is a don't-care if it is 0.0.0.0. | IP address |
| Destination: IP Mask | Enter the IP subnet mask to apply to the Destination: IP Addr. | Subnet mask |
| Destination: Port # | Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is a don't-care if it is 0. | [0-65535] |
| Destination: Port # Comp | Select the comparison to apply to the destination port in the packet against the value given in Destination: Port #. | [None/Less/Greater/Equal/Not Equal] |
| Source: IP Addr | Enter the source IP Address of the packet you wish to filter. This field is a don't-care if it is 0.0.0.0. | IP Address |
| Source: IP Mask | Enter the IP subnet mask to apply to the Source: IP Addr. | IP Mask |
| Source: Port # | Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is a don't-care if it is 0. | [0-65535] |
| Source: Port # Comp | Select the comparison to apply to the source port in the packet against the value given in Source: Port #. | [Yes/No] |
| TCP Estab | This field is applicable only when IP Protocol field is 6, TCP. If yes, the rule matches only established TCP | [Yes/No] |

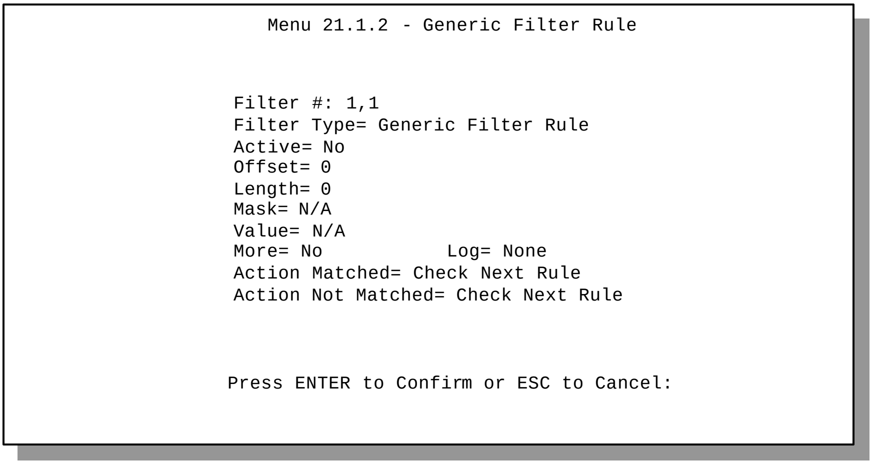
| Field | Description | Option |
|---|---|---|
| | connections; else the rule matches all TCP packets. | |
| More | If yes, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according the action fields.<br>If More is [Yes], then Action Matched and Action Not Matched will be N/A. | [Yes / N/A] |
| Log | Select the logging option from the following:<br>● None – No packets will be logged.<br>● Action Matched - Only packets that match the rule parameters will be logged.<br>● Action Not Matched - Only packets that do not match the rule parameters will be logged.<br>● Both – All packets will be logged. | [None]<br>[Action Matched]<br>[Action Not Matched]<br>[Both] |
| Action Matched | Select the action for a matching packet. | [Check Next Rule]<br>[Forward]<br>[Drop] |
| Action Not Matched | Select the action for a packet not matching the rule. | [Check Next Rule]<br>[Forward]<br>[Drop] |
| Once you have completed filling in Menu 21.1.1 - TCP/IP Filter Rule, press [Enter] at the message [Press Enter to Confirm] to save your configuration, or press [Esc] to cancel. This data will now be displayed on Menu 21.1 - Filter Rules Summary. | | |

### 9.3.2 Generic Filter Rule

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

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

To configure a generic rule, select Generic Filter Rule in the Filter Type field and press Enter to open Menu 21.1.2 - Generic Filter Rule, as shown in Figure 9-5.



```
       Menu 21.1.2 - Generic Filter Rule



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



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

**Figure 9-5. Menu 21.1.2 - Generic Filter Rule**

Table 9-6 describes the fields in the Generic Filter Rule Menu.

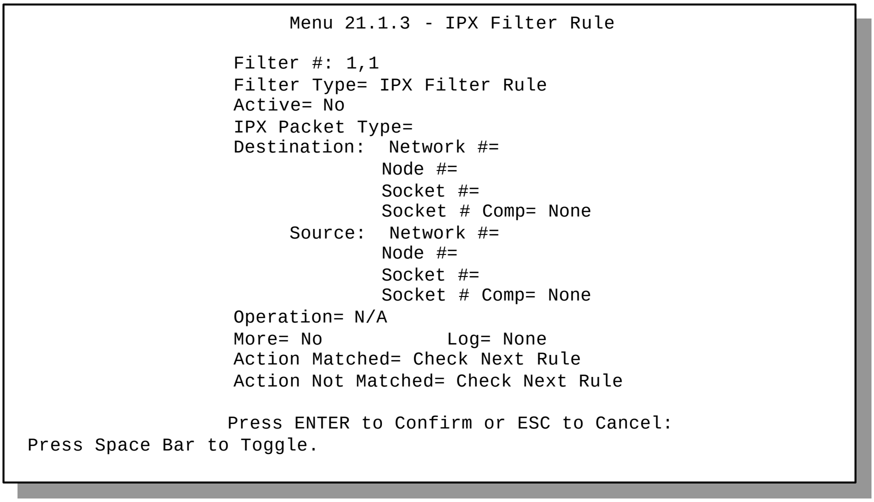
**Table 9-6. Generic Filter Rule Menu Fields**

| **Field** | **Description** | **Default** |
|---|---|---|
| Offset | Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255. | Default = 0 |
| Length | Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8. | Default = 0 |
| Mask | Enter the mask (in Hexadecimal) to apply to the data portion before comparison. | |
| Value | Enter the value (in Hexadecimal) to compare with the data portion. | |
| Once you have completed filling in Menu 21.1.2 - generic Filter Rule, press [Enter] at the message [Press Enter to Confirm] to save your configuration, or press [Esc] to cancel. This data will now be displayed on Menu 21.1 - Filter Rules Summary. | | |

### 9.3.3 Novell IPX Filter Rule

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

To configure an IPX rules, select IPX Filter Rule from the Filter Type field and press Enter to open Menu 21.1.3 IPX Filter Rule, as shown in Figure 9-6.



```
                       Menu 21.1.3 - IPX Filter Rule

                  Filter #: 1,1
                  Filter Type= IPX Filter Rule
                  Active= No
                  IPX Packet Type=
                  Destination:  Network #=
                               Node #=
                               Socket #=
                               Socket # Comp= None
                       Source:  Network #=
                               Node #=
                               Socket #=
                               Socket # Comp= None
                  Operation= N/A
                  More= No           Log= None
                  Action Matched= Check Next Rule
                  Action Not Matched= Check Next Rule

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

**Figure 9-6.      Menu 21.1.3 - IPX Filter Rule**

Table 9-7 describes the IPX Filter Rule.

**Table 9-7. IPX Filter Rule Menu Fields**

| **Field** | **Description** |
|---|---|
| IPX Packet Type | Enter the IPX packet type (1-byte in hexadecimal) you wish to filter.<br>The popular types are (in hexdecimal):<br>01 - RIP<br>04 - SAP<br>05 - SPX (Sequenced Packet eXchange)<br>11 - NCP (Netware Core Protocol)<br>14 - Novell NetBIOS |
| Destination/Source Network # | Enter the destination/source network numbers (4-byte in hexadecimal) of the packet that you wish to filter. |
| Destination/Source Node # | Enter in the destination/source node number (6-byte in hexadecimal) of the packet you wish to filter. |
| Destination/Source Socket # | Enter the destination/source socket number (2-byte in hexadecimal) of the packets that you wish to filter. |
| Destination/Source Socket # Comp | Select the comparison you wish to apply to the destination/source socket in the packet against that specified above. |
| Operation | This field is applicable only if one of the Socket # fields is 0452 or 0453 indicating SAP and RIP packets. There are seven options for this field that specify the type of the packet.<br>● None.<br>● RIP Request.<br>● RIP Response.<br>● SAP Request.<br>● SAP Response.<br>● SAP Get Nearest Server Request.<br>● SAP Get Nearest Server Response |
| Once you have completed filling in Menu 21.1.3 - IPX Filter Rule, press [Enter] at the message [Press Enter to Confirm] to save your configuration, or press [Esc] to cancel. This data will now be displayed on Menu 21.1 - Filter Rules Summary. | |

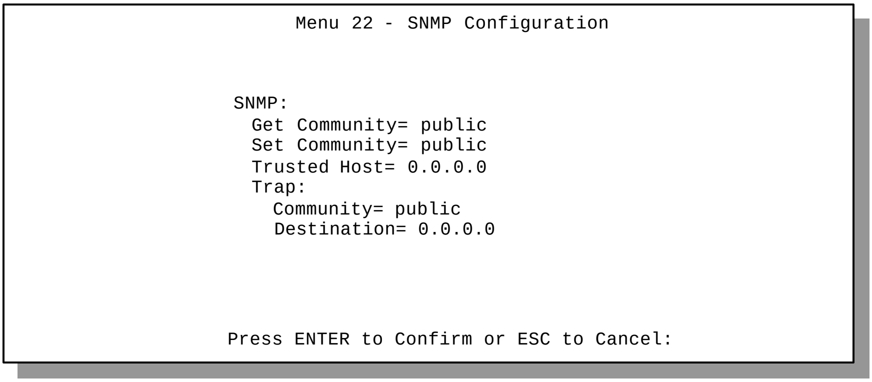
# Chapter 10
# SNMP Configuration

## 10.1 About SNMP

SNMP (Simple Network Management Protocol) is a protocol for network management and monitoring. Your *Prestige* supports SNMP agent functionality, which allows a manager station to manage and monitor the *Prestige* through the network. Keep in mind that SNMP is only available if TCP/IP is configured on your *Prestige*.

## 10.2 Configuring SNMP

To configure SNMP, select option **[22. SNMP Configuration]** from the Main Menu to open Menu 22 - SNMP Configuration, as shown in Figure 10-1. 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 10-1. Menu 22 - SNMP Configuration**

The following table describes the SNMP configuration parameters.

**Table 10-1. SNMP Configuration Menu Fields**

<table>
<tr><th>Field</th><th>Description</th><th>Default</th></tr>
<tr><td>Get Community</td><td>Enter the get community, which is the password for the incoming Get- and GetNext- requests from the management station.</td><td>public</td></tr>
<tr><td>Set Community</td><td>Enter the set community, which is the password for incoming Set-requests from the management station.</td><td>public</td></tr>
<tr><td>Trusted Host</td><td>If you enter a trusted host, your <i>Prestige</i> will only respond to SNMP messages from this address. If you leave the field blank (default), your <i>Prestige</i> will respond to all SNMP messages it receives, regardless of source.</td><td>blank</td></tr>
<tr><td>Trap:<br>Community</td><td>Enter the trap community, which is the password sent with each trap to the SNMP manager.</td><td>public</td></tr>
<tr><td>Trap:<br>Destination</td><td>Enter the IP address of the station to send your SNMP traps to.</td><td>blank</td></tr>
<tr><td colspan="3">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.</td></tr>
</table>

# Chapter 11

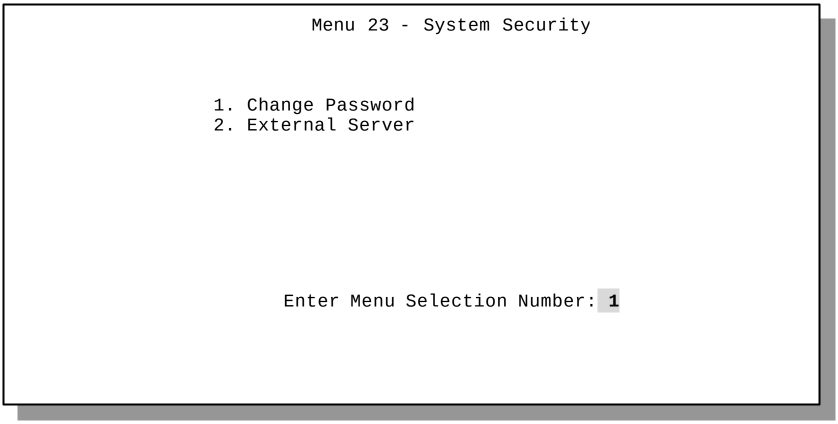
# System Security

This chapter covers Menu 23, which is for you to change the system password and to configure an external authentication server.

## 11.1 Changing the System Password

To change the system password, following steps below:

**Step 1.** Select option **[23. System Security]** in the Main Menu to open Menu 23 - System Security as shown in Figure 11-1.

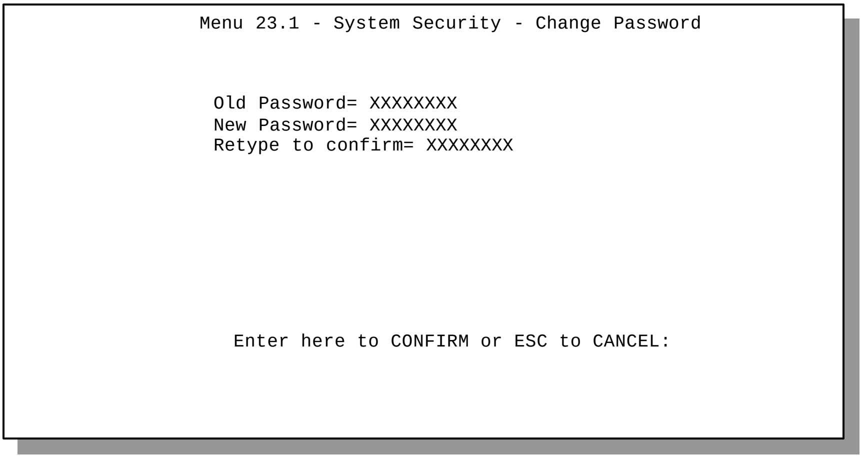


```
                         Menu 23 - System Security



                 1. Change Password
                 2. External Server








                        Enter Menu Selection Number: 1
```

**Figure 11-1. Menu 23 - System Security**

**Step 2.** From the System Security Menu, select option **[1. Change Password]** to open Menu 23.1 - System Security - Change Password.

**Step 3.** Enter your existing system password and press [Enter].



```
                 Menu 23.1 - System Security - Change Password



                  Old Password= XXXXXXXX
                  New Password= XXXXXXXX
                  Retype to confirm= XXXXXXXX









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

**Figure 11-2. Menu 23.1 - System Security - Change Password**

**Step 4.** Enter your new system password and press [Enter].

**Step 5.** Re-type your new system password for confirmation and press [Enter].

As you enter the password, the screen displays an (X) for each character you type.

## 11.2 Using RADIUS Authentication

Your *Prestige* has a built-in dial-up user list; however, the number of users that can be stored locally is limited due to memory constraints. If you have more users than what the *Prestige* can store locally, use an external RADIUS (Remote Authentication Dial-In User Service) server that provides authentication service for unlimited number of users.

### 11.2.1 Installing a RADIUS Server

To use RADIUS authentication, you need to have a UNIX or Windows NT machine on your network as the RADIUS server, as well as the RADIUS software itself.

You can obtain the RADIUS server software, along with documentation, at

**`http://www.livingston.com/Tech/FTP/pub-le-radius.shtml`** or
**`ftp://ftp.livingston.com/pub/le/radius`**/

Follow the included instructions to install the software on your server.

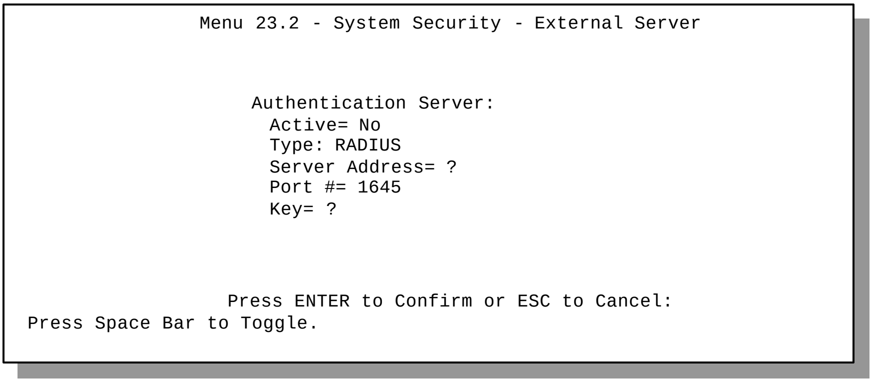
After you install the server software, you will need to edit the `dictionary` file in the RADIUS configuration directory (usually `/etc/raddb`). Using any text editor, add the following lines to the `dictionary` file:

```
# Zyxel proprietary attributes
ATTRIBUTE  Zyxel-Callback-Option  192  integer
VALUE      Zyxel-Callback-Option  None       0
VALUE      Zyxel-Callback-Option  Optional   1
VALUE      Zyxel-Callback-Option  Mandatory  2

# Callback phone number source
ATTRIBUTE  Zyxel-Callback-Phone-Source  193  integer
VALUE      Zyxel-Callback-Phone-Source  Preconfigured  0
VALUE      Zyxel-Callback-Phone-Source  User           1
```

These changes add the support for CLID authentication, as described in the section below.

## 11.2.2 RADIUS Server Configuration

To configure the RADIUS server, select option 23, System Security, from the Main Menu to open Menu 23 - System Security.  Select option 2, External Server from this menu to open Menu 23.2 - System Security - External Server, shown in Figure 11-3.



```
                  Menu 23.2 - System Security - External Server



                       Authentication Server:
                         Active= No
                         Type: RADIUS
                         Server Address= ?
                         Port #= 1645
                         Key= ?




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

**Figure 11-3.      Menu 23.2 - System Security - External Server**

The fields in the System Security - External Server Menu are listed in Table 11-1.

**Table 11-1. System Security - External Server Menu Fields**

| Field | Description | Default |
|---|---|---|
| Active | Determines whether the external security facility is enabled.<br>If No, only the built-in dial-up user list will be used.<br>If Yes, the built-in dial-up user list will be searched first, then the external authentication server. | |
| Type | Determines the type of the external authentication server. At present only RADIUS is supported. | |
| Server Address | The IP address of the RADIUS server. | |
| Port # | The IP port number used by the authentication server. The default is port 1645. | [1645] |
| Key | A "password" used to authenticate your *Prestige* to the RADIUS service. Please note that this is between the *Prestige* and the server; it has nothing to do with the dial-in users. | |

### The Key Field

The “key”, or password, must match that in the `client` file in the RADIUS server’s `/etc/raddb` directory, as shown in the following example:

```
# Client Name        Key
#-------------------------
192.168.1.1          1234
```

After you configure a RADIUS server, your *Prestige* will use it to authenticate all users that it can not find in its internal dial-up user list (*see* Menu 14)

## 11.2.3 Adding Users to the RADIUS Database

To add a user to the RADIUS database, edit the `users` file in the RADIUS server’s `/etc/raddb` directory, and add a line similar to the following:

```
Joeuser  Password = “joepassword”
```

## 11.2.4 Using RADIUS Authentication for CLID

To use RADIUS for CLID authentication, create a user record in the `users` file where the user name (the first field) is the telephone number, and the password (the second field) is always `Zyxel-CLID` (case-sensitive). The regular user name is put in a User-Name field.  The following is an example of a CLID user record:

```
5551212    Password = “Zyxel-CLID”
User-Name = ”joeuser”
Zyxel-Callback-Option = Mandatory
Zyxel-Callback-Phone-Source = Preconfigured
Dialback-No = “5551212”
```

Note that if CLID is turned off in your *Prestige*, you need to have a separate user record for `joeuser` so the regular user name/password mechanism still works.

# Chapter 12

# Telnet Configuration and Capabilities

## 12.1 About Telnet Configuration

Before the *Prestige* is properly setup for TCP/IP, the only option for configuring it is through the console port. Once your *Prestige* is configured, you can use telnet to configure it remotely as shown in Figure 12-1.

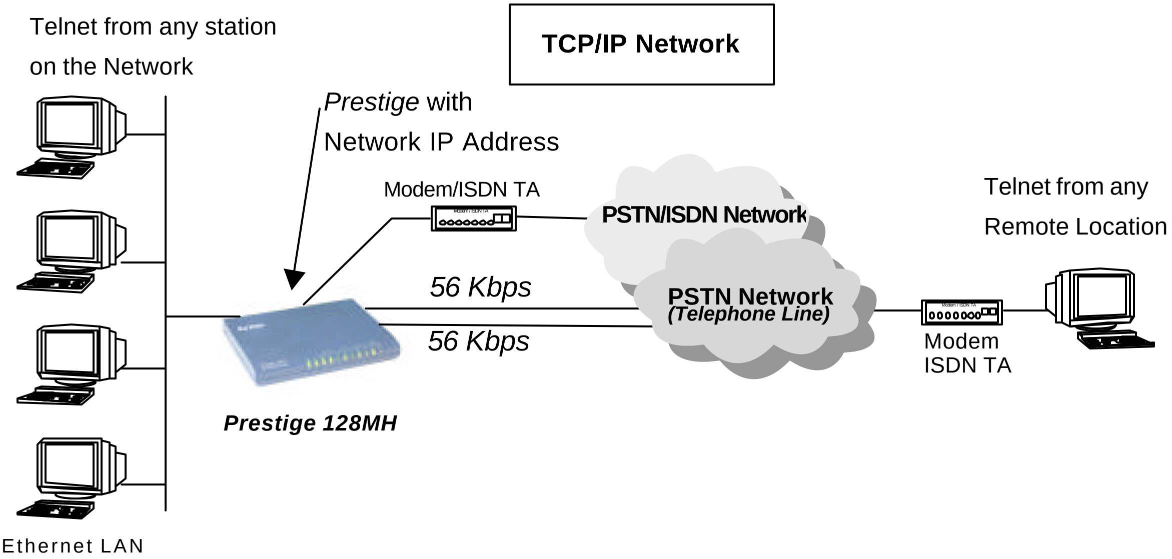


**Figure 12-1. Telnet Configuration on a TCP/IP Network**

If your *Prestige* is configured for IPX but not IP routing in Menu 1, telnet is still available provided you assign the *Prestige* a correct IP address and subnet mask. When IP routing is disabled, the *Prestige* can still function as a host.

## 12.2 Telnet Under SUA

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

## 12.3 Telnet Capabilities

### 12.3.1 Single Administrator

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

### 12.3.2 System Timeout

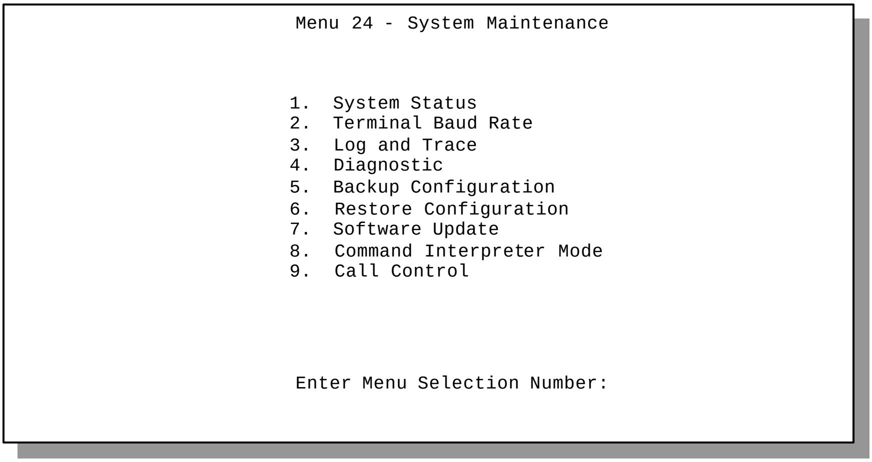
There is a system timeout of 5 minutes (300 seconds) for either the console port or telnet. Your *Prestige* will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in Menu 24.1.

# Chapter 13

# System Maintenance

This chapter covers the diagnostic tools that help you to maintain your Prestige. These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Select menu 24 in the main menu to open Menu 24 - System Maintenance, as shown in Figure 13-1.

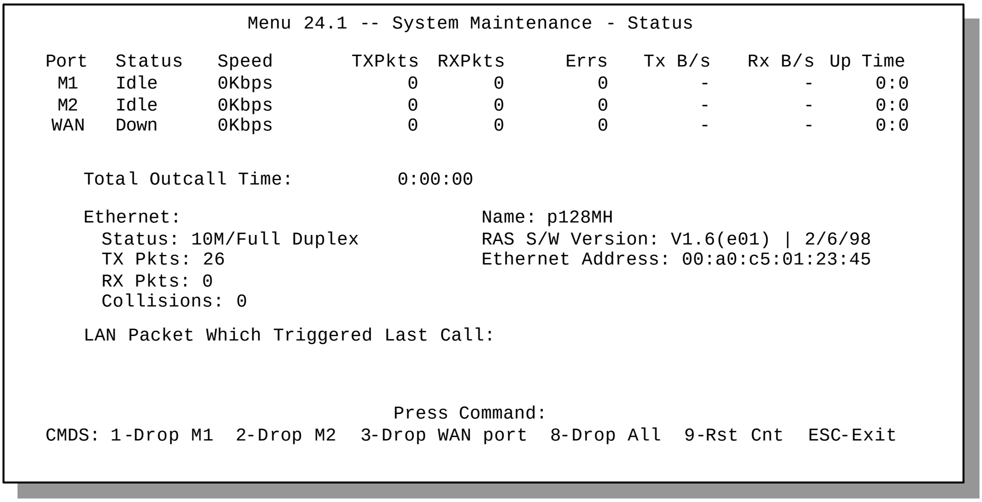


```
                        Menu 24 - System Maintenance



                       1.  System Status
                       2.  Terminal Baud Rate
                       3.  Log and Trace
                       4.  Diagnostic
                       5.  Backup Configuration
                       6.  Restore Configuration
                       7.  Software Update
                       8.  Command Interpreter Mode
                       9.  Call Control





                        Enter Menu Selection Number:
```

**Figure 13-1. Menu 24 - System Maintenance**

## 13.1 System Status

The first selection, System Status, gives you information on the version of your system firmware and the status and statistics of the ports, as shown in Figure 13-2.



```
                  Menu 24.1 -- System Maintenance - Status

Port  Status   Speed       TXPkts  RXPkts      Errs   Tx B/s   Rx B/s Up Time
 M1   Idle     0Kbps             0       0        0        -        -     0:0
 M2   Idle     0Kbps             0       0        0        -        -     0:0
WAN   Down     0Kbps             0       0        0        -        -     0:0


   Total Outcall Time:          0:00:00

   Ethernet:                           Name: p128MH
     Status: 10M/Full Duplex           RAS S/W Version: V1.6(e01) | 2/6/98
     TX Pkts: 26                       Ethernet Address: 00:a0:c5:01:23:45
     RX Pkts: 0
     Collisions: 0

   LAN Packet Which Triggered Last Call:



                               Press Command:
CMDS: 1-Drop M1  2-Drop M2  3-Drop WAN port  8-Drop All  9-Rst Cnt  ESC-Exit
```

**Figure 13-2. Menu 24.1 - System Maintenance - Status**

Follow the procedure below to go to the System Status Menu.

**Step 1.** Select option 24 from the Main Menu to access Menu 24 - System Maintenance.

**Step 2.** From Menu 24, select option **[1. System Status]**.

**Step 3.** There are five possible commands in Menu 24.1 - System Maintenance - Status.

- Entering 1 or 2 or 3 to disconnect the call on the specified WAN port;
- Entering 8 to disconnect the calls on all WAN ports,
- Entering 9 to reset the counters, and [Esc] to exit this screen.

Please note that entering 9 will reset all counters except the Total Outcall Time.

The following Table 13-1 describes the fields present in Menu 24.1 - System Maintenance - Status.

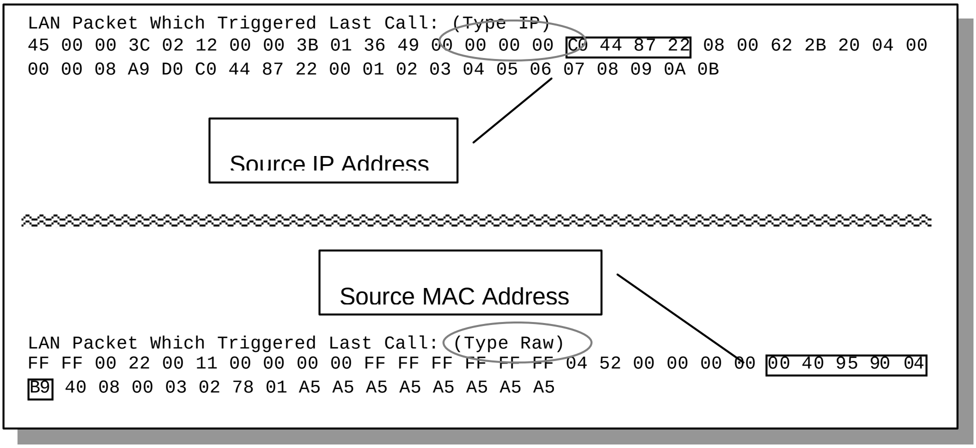
**Table 13-1. System Maintenance - Status Menu Fields**

| Field | Description |
|---|---|
| 1. Port | Shows statistics for the modems and WAN port, respectively. |
| 2. Status | Shows the status of the port ([Idle], [Calling], or [Answering]). When the connection is up, it shows the name of the remote node or the dial-in user currently connected. |
| 3. Speed | The connection speed of the current call. |
| 4. TXPkts | The number of transmitted packets on this port. |
| 5. RXPkts | The number of received packets on this port. |
| 6. Errs | The number of packets (both in and out) with errors and discarded on this port. |
| 7. Tx B/s | The running display of the number bytes transmitted in the last second. |
| 8. Rx B/s | The running display of the number bytes received in the last second. |
| 9. Up Time | The elapsed time of the current call. |
| 10. Total Outgoing call Time | The grand total outgoing call time for all WAN ports since the system was last powered on. |
| 11. Ethernet | The following 4 fields show the status of the Ethernet port. |
| 12. Status | Shows the current status (speed and half/full duplex) of the LAN. |
| 13. TX Pkts | The number of transmitted packets to LAN. |
| 14. RX Pkts | The number of received packets from LAN |
| 15. Collision | The number of collisions (more than 1 station trying to transmit at the same time). |

**Table 13-1. System Maintenance - Status Menu Fields (continued)**

| Field | Description |
|---|---|
| 16. Name | Displays the system name of your *Prestige*. This information can be modified in Menu 1 – General Setup. |
| 17. RAS S/W Version | Shows to the version of the current RAS firmware. |
| 18. Ethernet Address | Shows to the Ethernet MAC address assigned to your *Prestige*. |
| 19. LAN Packet Which Triggered Last Call | Shows the first 48 octets of the LAN packet that triggered the last outgoing call. There are three different types of packets: IP, IPX, and RAW. By viewing the packet information, you can determine which station sends a packet to trigger an outgoing call. |

Figure 13-3 shows two examples of triggering packets from the LAN: the first of an ICMP ping packet (Type: IP) and the second a SAP broadcast packet (Type: Raw). With this information, you can determine the workstation from the source IP address or the source MAC address of the packet.



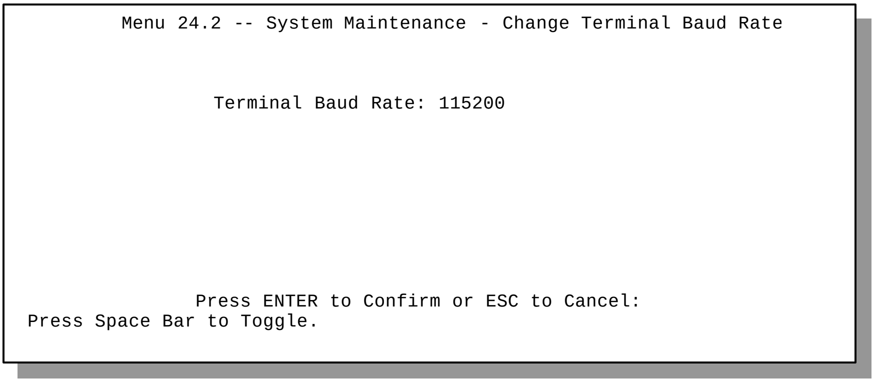
```
LAN Packet Which Triggered Last Call: (Type IP)
45 00 00 3C 02 12 00 00 3B 01 36 49 00 00 00 00 C0 44 87 22 08 00 62 2B 20 04 00
00 00 08 A9 D0 C0 44 87 22 00 01 02 03 04 05 06 07 08 09 0A 0B
```

```
LAN Packet Which Triggered Last Call: (Type Raw)
FF FF 00 22 00 11 00 00 00 00 FF FF FF FF FF FF 04 52 00 00 00 00 00 40 95 90 04
B9 40 08 00 03 02 78 01 A5 A5 A5 A5 A5 A5 A5 A5
```

**Figure 13-3. LAN Packet That Triggered Last Call**

## 13.2 Terminal Baud Rate

You can set up different baud rates for the console port through Menu 24.2 - Terminal Baud Rate. Your *Prestige* supports 9600 (default), 19200, 38400, 57600, and 115200bps for the console port. Use the space bar to select the desired baud rate in Menu 24.2, as shown in Figure 13-4.



```
        Menu 24.2 -- System Maintenance - Change Terminal Baud Rate



                 Terminal Baud Rate: 115200









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

**Figure 13-4. Menu 24.2 - System Maintenance - Change Terminal Baud Rate**

## 13.3 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.

### 13.3.1 Viewing Error Log

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

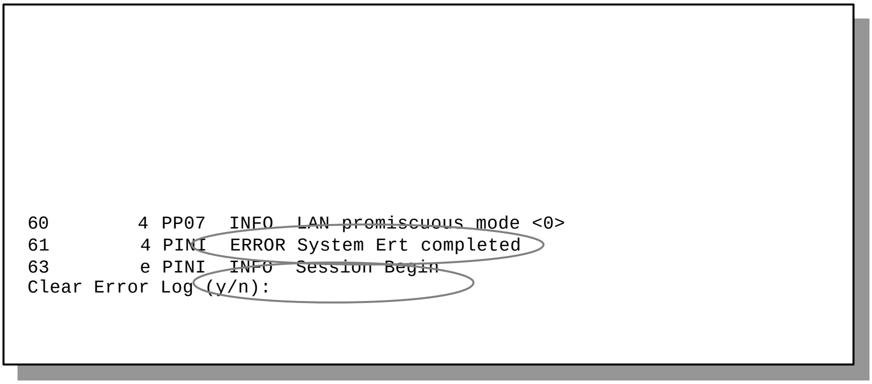
**Step 1.** Select option 24 from the Main Menu to open Menu 24 - System Maintenance.

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

**Step 3.** Select the first option from Menu 24.3 - System Maintenance - Log and Trace to display the error log in the system.

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

Examples of typical error and information messages are presented in Figure 13-5.

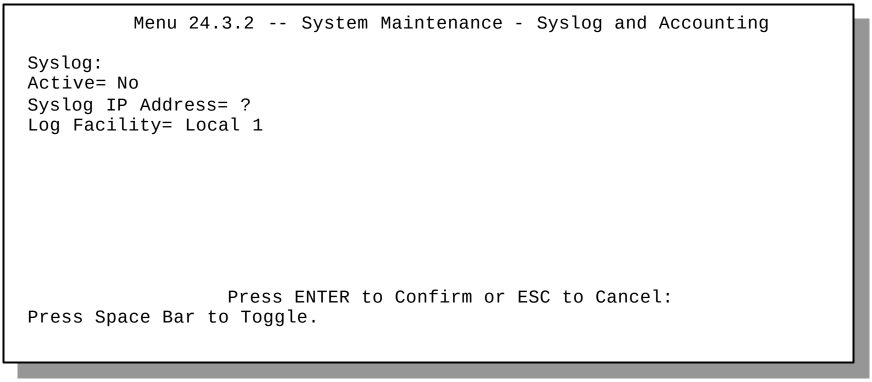


```
60         4 PP07  INFO  LAN promiscuous mode <0>
61         4 PINI  ERROR System Ert completed
63         e PINI  INFO  Session Begin
Clear Error Log (y/n):
```

**Figure 13-5.  Examples of Error and Information Messages**

## 13.3.2 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 in Figure 13-6.



```
          Menu 24.3.2 -- System Maintenance - Syslog and Accounting

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









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

**Figure 13-6. Menu 24.3.2 - System Maintenance - Syslog and Accounting**

You need to configure the following 3 parameters described in Table 13-2 to activate syslog.

**Table 13-2. System Maintenance Menu Syslog Parameters**

| **Parameter** | **Description** |
|---|---|
| Active | Use the space bar to turn on or off syslog. |
| Syslog IP Address | Enter the IP Address of your syslog server. |
| Log Facility | Use the space bar to toggle between the 7 different Local options. The log facility allows you to log the message in different files in the server. Please refer to your UNIX manual for more detail. |

Your *Prestige* sends three types of syslog messages: call information messages (i.e. CDR), error information messages and session information messages. Some examples of these syslog messages are shown below:

Call Information Messages:

```
line 1 channel 1, call 41, C01, Incoming Call, 40001
line 1 channel 1, call 41, C01, ANSWER Connected, 49K 40001
line 1 channel 1, call 41, C01, Incoming Call, Call Terminated
```

Error Information Messages:

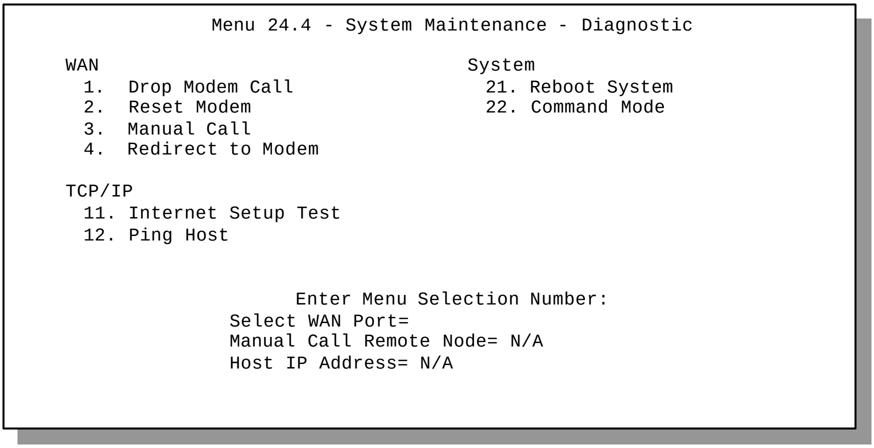
```
line 1, channel 1, call 44, E01, CLID call refuse
line 1, channel 1, call 45, E02, IP address mismatch
```

Session Information Messages:

```
line 1, channel 1, call 41, I01, IPCP up, myPrestige
line 1, channel 1, call 41, I01, IPCP down, myPrestige
```

# 13.4 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 in Figure 13-7.



```
                  Menu 24.4 - System Maintenance - Diagnostic

     WAN                                   System
       1.  Drop Modem Call                   21. Reboot System
       2.  Reset Modem                       22. Command Mode
       3.  Manual Call
       4.  Redirect to Modem

     TCP/IP
       11. Internet Setup Test
       12. Ping Host


                          Enter Menu Selection Number:
                    Select WAN Port=
                    Manual Call Remote Node= N/A
                    Host IP Address= N/A
```

**Figure 13-7. Menu 24.4 - System Maintenance - Diagnostic**

Follow the procedure below to get to Diagnostic

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

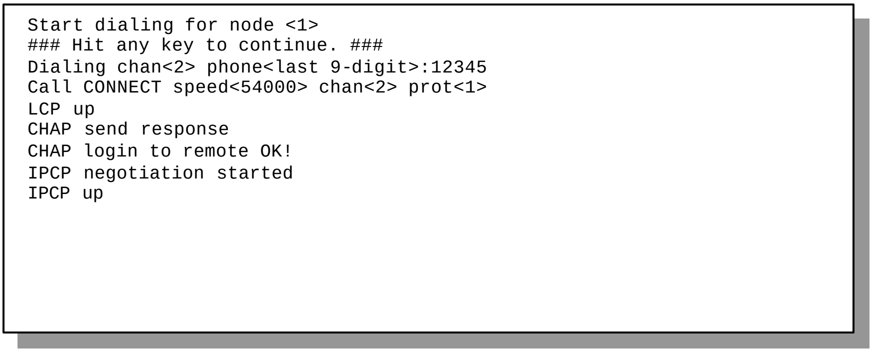
**Step 2.** From this menu, select option 4. Diagnostic. This will open Menu 24.4 - System Maintenance - Diagnostic.

The following Table 13-3 describes the diagnostic tests available in Menu 24.4 for your *Prestige* and the connections.

**Table 13-3. System Maintenance Menu Diagnostic**

| **Fields** | **Description** |
|---|---|
| Drop WAN Port | This command drops the call on a WAN port. Selecting this option brings you to the Select WAN Port field to specify the port. |
| Reset WAN Port | This command resets the specified WAN port. Selecting this option brings you to the Select WAN Port field to specify the port. |
| Manual Call | This option allows you to manually place a call to a remote node. The *Prestige* will show you the trace of what is happening during the call setup and PPP negotiation. |
| Redirect to WAN Port | This command redirects the keyboard to the WAN port. Anything you type will be sent to the WAN device and the device's response will be shown on your screen. Selecting this option brings you to the Select WAN Port field to specify the port |
| Internet Setup Test | This test checks to see if your Internet access configuration is correct. When this option is chosen, your *Prestige* will call the ISP and perform the PPP negotiations. If everything is working properly, you will see an appropriate response. Otherwise, note the error message and take the appropriate troubleshooting steps. |
| Ping Host | This diagnostic sends an ICMP echo packet to the remote host and shows you the round-trip time when the *Prestige* gets a response. This is to test if the host is reachable via TCP/IP. |
| Reboot System | This option reboots the system. |
| 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. |

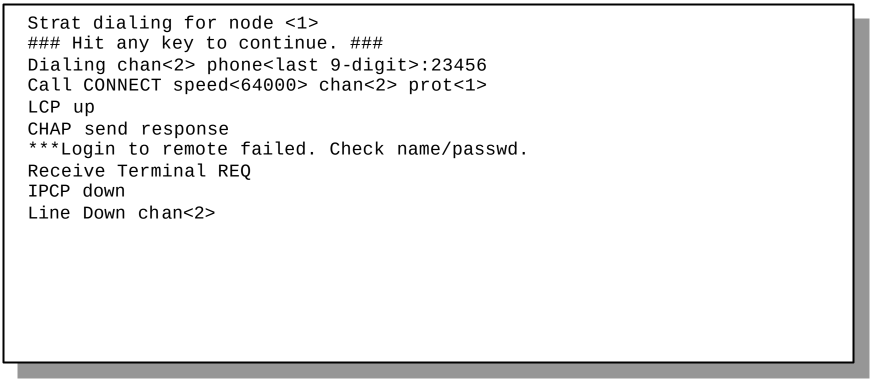
Figure 13-8 shows an example of a successful connection after selecting option **[3. Manual Call]** in Menu 24.4.



```
Start dialing for node <1>
### Hit any key to continue. ###
Dialing chan<2> phone<last 9-digit>:12345
Call CONNECT speed<54000> chan<2> prot<1>
LCP up
CHAP send response
CHAP login to remote OK!
IPCP negotiation started
IPCP up
```

**Figure 13-8. Trace Display for a Successful Manual Call**

Figure 13-9 shows a trace example where authentication failed.



```
Strat dialing for node <1>
### Hit any key to continue. ###
Dialing chan<2> phone<last 9-digit>:23456
Call CONNECT speed<64000> chan<2> prot<1>
LCP up
CHAP send response
***Login to remote failed. Check name/passwd.
Receive Terminal REQ
IPCP down
Line Down chan<2>
```

**Figure 13-9. Trace Display for a Failed Authentication**

## 13.5 Backup Configuration

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

You must perform the backup and restore through the console port. Any serial communications program should work fine; however, you must use XMODEM protocol to perform the download/upload.

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

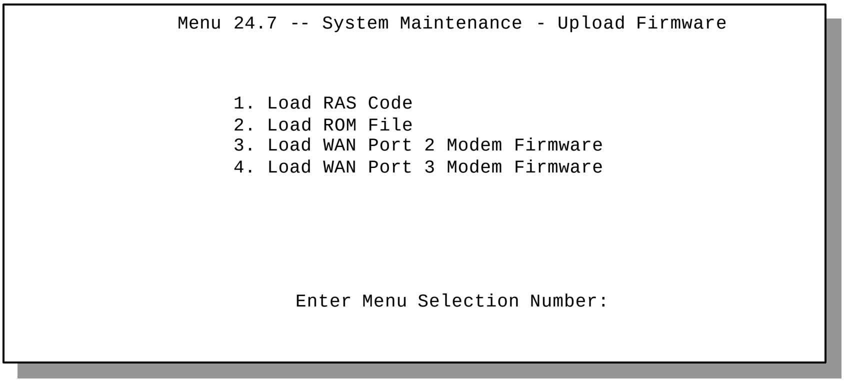
## 13.6 Restore Configuration

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

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.

## 13.7 Firmware Update

Menu 24.7 -- System Maintenance - Upload Firmware allows you to upgrade the firmware for the various modules and the ROM file system. Uploading is only possible through the console port. Note that this function erases the old data before installing the new one. Do not attempt to update unless you have the new firmware at hand. There are 4 components in the system: RAS code (program code) and ROM File system and firmware for the modem modules, as shown Figure 13-10.



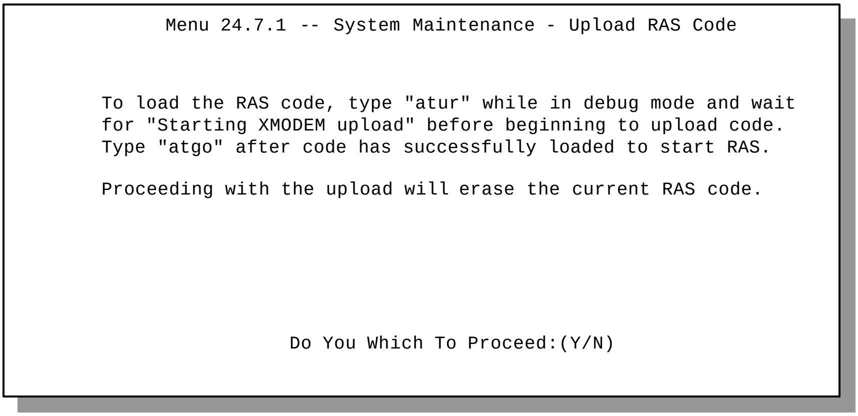
```
             Menu 24.7 -- System Maintenance - Upload Firmware



                  1. Load RAS Code
                  2. Load ROM File
                  3. Load WAN Port 2 Modem Firmware
                  4. Load WAN Port 3 Modem Firmware






                          Enter Menu Selection Number:
```

**Figure 13-10. Menu 24.7 - System Maintenance - Upload Firmware**

### 13.7.1 Upload RAS code

RAS (Remote Access Service) code refers to the firmware that controls the main function of the *Prestige*. Menu 24.7.1 shows you the instructions for uploading RAS code. If you answer yes to the prompt, the *Prestige* will reboot automatically. Press any key when you see the message “Press Any key to enter Debug Mode within 3 seconds.” to enter debug mode.

Once in debug mode, type `atur` and wait for your *Prestige* to respond with “Starting XMODEM upload” to begin uploading the new firmware (upload procedure varies depending on the software used to access your *Prestige*). After successfully uploading the new firmware, type `atgo` to restart your *Prestige.*



```
              Menu 24.7.1 -- System Maintenance - Upload RAS Code


        To load the RAS code, type "atur" while in debug mode and wait
        for "Starting XMODEM upload" before beginning to upload code.
        Type "atgo" after code has successfully loaded to start RAS.

        Proceeding with the upload will erase the current RAS code.






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

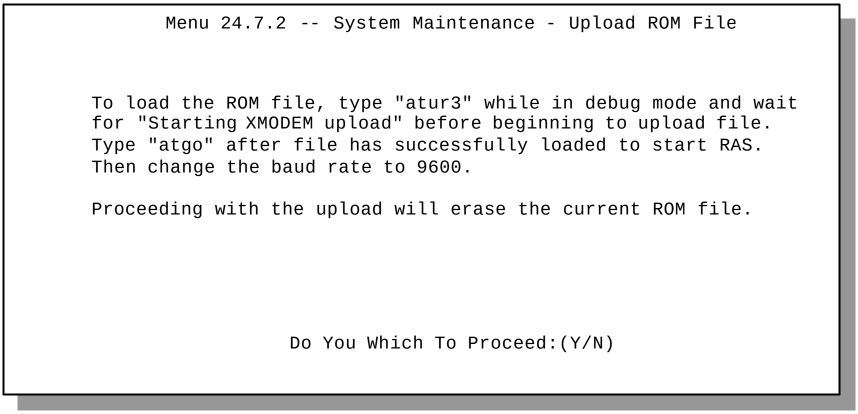
**Figure 13-11. Menu 24.7.1 - Uploading RAS Code**

### 13.7.2 Uploading ROM File

The configuration, system-related data, the error log and the trace log are all stored in the ROM file system. Menu 24.7.2 shows you the instructions for uploading ROM file. Please be aware that uploading the ROM file replaces everything contained within. If you answer yes to the prompt, the *Prestige* will reboot automatically. Press any key when you see the message “Press Any key to enter Debug Mode within 3 seconds.” to enter debug mode.

Once in debug mode, type [atur3] and wait for your *Prestige* to respond with “Starting XMODEM upload” to begin uploading the ROM file (uploading procedure varies depending on the software used). After successfully uploading the ROM file, type `atgo` to restart your *Prestige*.

If you upload the default ROM file, you will lose all configuration that you had before and the console port will be set to the default of 9600 baud. You will need to change the baud rate of your serial communications software to 9600 before you can connect to the *Prestige* again.



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



       To load the ROM file, type "atur3" while in debug mode and wait
       for "Starting XMODEM upload" before beginning to upload file.
       Type "atgo" after file has successfully loaded to start RAS.
       Then change the baud rate to 9600.

       Proceeding with the upload will erase the current ROM file.






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

**Figure 13-12. Menu 24.7.2 - System Maintenance - Upload ROM File**

### 13.7.3 Updating Modem Firmware

Commands 3 and 4 allow you to update the firmware for the built-in modems. The uploading method will be different depending on the particular modem module in your *Prestige*. Please visit ZyXEL’s web site at *www.zyxel.com* for the instructions and modem firmware.

## 13.8 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.

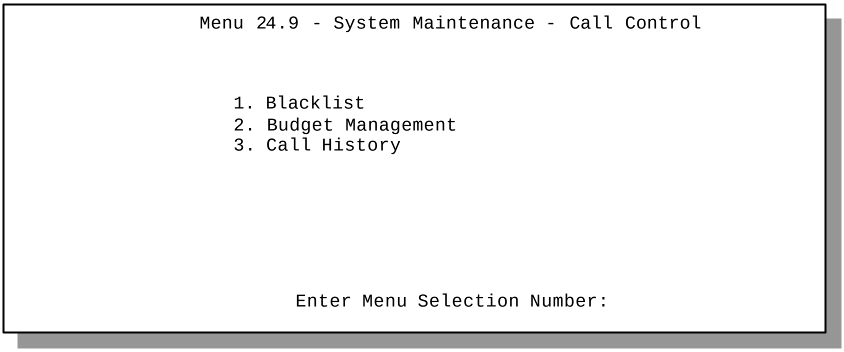
## 13.9 Call Control

The *Prestige* provides two call control functions: budget management and blacklist.

The budget management function allows you to set a limit on the total outgoing call time of the *Prestige* over a period of time. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

The blacklist function prevents the *Prestige* from re-dialing to an unreachable phone number. It is a list of phone numbers, up to a maximum of 14, to which the *Prestige* will not make an outgoing call. If the *Prestige* tries to dial to a phone number and fails a certain number of times (configurable in Menu 24.9.1), then the phone number is put in the blacklist. You will have to enable the number manually before the *Prestige* will dial that number again.

To enter the call control menu, select option [9. Call Control] in Menu 24 to go to Menu 24.9 - System Maintenance - Call Control, as shown in Figure 13-13.



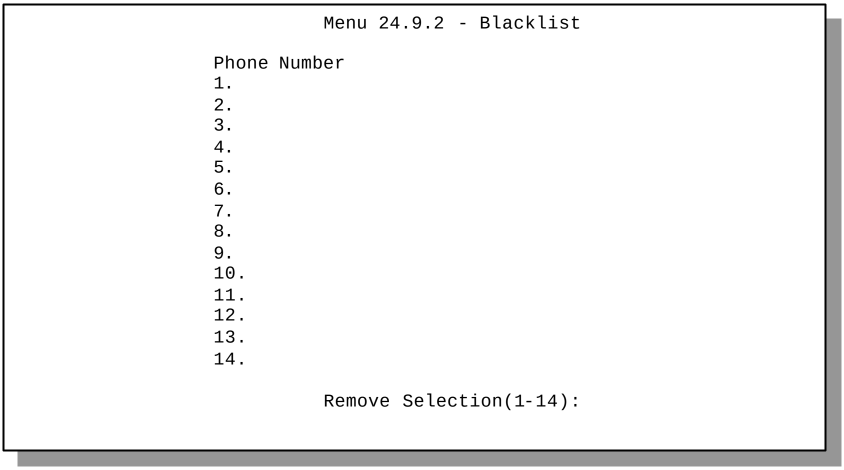
```
                   Menu 24.9 - System Maintenance - Call Control



                      1. Blacklist
                      2. Budget Management
                      3. Call History






                            Enter Menu Selection Number:
```

**Figure 13-13.    Menu 24.9 - System Maintenance - Call Control**

### 13.9.1 Blacklist

The phone numbers on the blacklist are numbers that the *Prestige* had problems connecting in the past. The only operation allowed is for you to take a number off the list by entering its index number.

Menu 24.9.2 shows the list of telephone numbers that have been blacklisted.

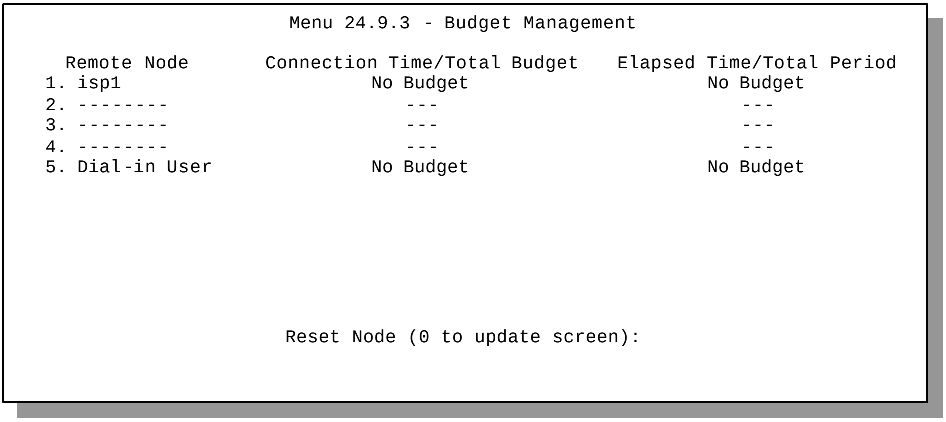


```
                          Menu 24.9.2 - Blacklist

                 Phone Number
                 1.
                 2.
                 3.
                 4.
                 5.
                 6.
                 7.
                 8.
                 9.
                 10.
                 11.
                 12.
                 13.
                 14.

                          Remove Selection(1-14):
```

**Figure 13-14. Menu 24.9.2 - Blacklist**

## 13.9.2 Budget Management

Menu 24.9.3 shows the budget management statistics for outgoing calls.



```
                      Menu 24.9.3 - Budget Management

  Remote Node       Connection Time/Total Budget   Elapsed Time/Total Period
1. isp1                      No Budget                      No Budget
2. --------                     ---                            ---
3. --------                     ---                            ---
4. --------                     ---                            ---
5. Dial-in User              No Budget                      No Budget







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

**Figure 13-15.   Menu 24.9.3 - Budget Management**

The total budget is the time limit on the accumulated time for outgoing call to a remote node or for calling back to the dial-in users collectively. When this limit is reached, the call will be dropped and further outgoing calls to that remote node or dial-in user (callback) will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node or the dial-in users. The budget and the reset period can be configured in the Menu 11 and 13 for a remote node and for the dial-in user, respectively.

# Chapter 14

# Troubleshooting

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

## 14.1 Problems Starting Up the *Prestige*

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

| **Problem** | **Corrective Action** | |
|---|---|---|
| None of the LEDs are on when you power on the *Prestige* | Check the connection between the AC adapter and the *Prestige*.<br>If the error persists, you may have a hardware problem. In this case you should contact 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 Baud |
| | | No parity, 8 Data bits, 1 Stop bit. |

## 14.2 Problems With the WAN Ports

**Table 14-2. Troubleshooting a WAN Port Connection**

| **Problem** | **Corrective Action** |
|---|---|
| RDY LED of a WAN port is off | Check if the WAN port is connected to an external modem/ISDN TA.<br>Check if LINE 1 or LINE 2 is connected to a telephone line. |
| | Check if the power of the external modem/ISDN TA is turned on. |

## 14.3 Problems with the LAN Interface

**Table 14-3. Troubleshooting the LAN Interface**

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

## 14.4 Problems Connecting to a Remote Node or ISP

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

| Problem | Corrective Action |
|---|---|
| Can’t connect to a remote node or ISP | Check Menu 24.1 to verify the line status. If it indicates [down], then refer to the section on the line problems. |
| | In Menu 24.4.5, do a manual call to that remote node. Observe the messages and take appropriate actions. |

## 14.5 Problems for Remote User to Dial-in

**Table 14-5. Troubleshooting for Remote Users to Dial-in**

| Problem | Corrective Action |
|---|---|
| A remote user cannot dial-in | First verify that you have configured the authentication parameters in Menu 13. These would be CLID Authen and Recv. Authen. |
| | In Menu 14, verify the user name and password for the remote dial-in user. |
| | If the remote dial-in user is negotiating IP, verify that the IP address is supplied correctly in Menu 13. Check that either the remote dial-in user is supplying a valid IP address, or that the *Prestige* is assigning a valid address from the IP pool. |
| | If the remote dial-in user is negotiating IPX, verify that the IPX network number is valid from the IPX pool (if it is being used). |

# Chapter 15

# Acronyms and Abbreviations

| | |
|---|---|
| BAP/BACP | Bandwidth Allocation Protocol/Bandwidth Allocation Control protocol |
| BOD | Bandwidth on Demand |
| CDR | Call Detail Record |
| CHAP | Challenge Handshake Authentication Protocol |
| CLID | Calling Line IDentification |
| CSU/DSU | Channel Service Unit/Data Service Unit |
| DCE | Data Communications Equipment |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| DTE | Data Terminal Equipment |
| IANA | Internet Assigned Number Authority |
| IP | Internet protocol |
| IPCP | IP Control Protocol |
| IPX | Internetwork Packet eXchange |
| ISDN | Integrated Service Digital Network |
| ISP | Internet Service Provider |
| LAN | Local Area Network |
| MAC | Media Access Control |
| MP | (PPP) Multilink Protocol |
| NAT | Network Address Translation |
| PAP | Password Authentication Protocol |
| POTS | Plain Old Telephone Service |

| | |
|---|---|
| PPP | Point to Point Protocol |
| PSTN | Public Switched Telephone Network |
| RADIUS | Remote Authentication Dial-In User Service |
| RIP | Routing Information Protocol |
| SAP | (IPX) Service Advertising Protocol |
| SNAP | Sub-Network Access Protocol |
| SNMP | Simple Network Management Protocol |
| SUA | Single User Account |
| TA | (ISDN) Terminal Adapter |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| UTP | Unshielded Twisted Pair (cable) |
| WAN | Wide Area Network |

# Index