Prestige 100IH

ISDN Router

User's Guide

Version 2.41

Feb 2000

ZyXEL

TOTAL INTERNET ACCESS SOLUTION

Copyright

Disclaimer

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

The declarations of CE marking:

The Prestige 100 and 100IH has been approved for connection to the Public Switched Telecommunication Network using interfaces compatible with ITU-TSS recommendation I.420 (Basic Rate ISDN user access). The Prestige 100 and 100IH comply with the following directives:

The Council Directive 89/336/EEC of 3 May 1992 on the approximation of the laws of the member states relation to Electro Magnetic Compatibility. (EMC Directive).

Council Directive 91/263/EEC of 29 April 1991 on the approximation of the laws of the Member States concerning telecommunication terminal equipment. (The Telecom Terminal Equipment Directive).

93/68/EEC of 22 July 1993 amending the Directives 89/336/EEC, 91/263 /EEC and 92/31/EEC. (Marking Directive).

The Council Directive 92/31/EEC of 28 April 1992 amending directive on the approximation of the laws of the member states relating to Electro Magnetic Compatibility.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two (2) years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-

manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

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

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

Customer Support

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

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

Table of Contents

List of Figures

List of Tables

Preface

About Your Prestige

Congratulations on your purchase of the Prestige ISDN Router. Don't forget to register your Prestige (fast, easy online registration at www.zyxel.com) for free future product updates and information.

The Prestige 100IH is a high-performance routers that offer complete solutions for your WAN (Wide Area Network) applications such as Internet access, LAN-to-LAN connections, telecommuting and remote access over ISDN (Integrated Service Digital Network).

You do not need to set any switches to configure the Prestige. The user-friendly Prestige Web Configurator (PWC) is a JAVA based utility that allows you to manage the Prestige via a Worldwide Web browser. You can also manage the Prestige via the SMT (System Management Terminal), a menu-driven interface that you can access from either a terminal emulator or telnet.

Setup Information

ISDN Line

1. Contact your local telephone company's ISDN Ordering Center to find out what type of ISDN service is available and the switch type.
2. When the telephone company installs your ISDN line, please be sure to obtain and write down the following information for future use:
   a. ISDN switch type
   b. ISDN telephone number(s)

Supplemental services such as Call Forwarding are supported by the Prestige but must be subscribed to separately from the telephone company.

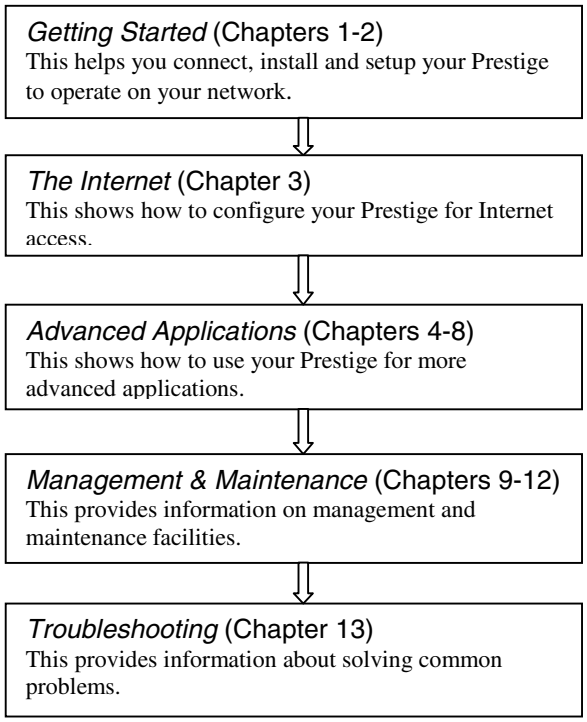
Ethernet Setup Information

IP Address - The IP Address is the unique 32-bit number assigned to your Prestige. This address is written in dotted decimal notation (four 8-bit numbers, between 0 and 255, separated by periods), e.g., 192.168.1.1.

Please note that every machine on a network must have a unique IP address - do not assign an arbitrary address to any machine. If you are not sure as to which IP address to assign to the Prestige, contact your Internet Service Provider (ISP) or refer to Chapter 3 of this guide for more details.

IP Subnet Mask - An IP address consists of two parts, the network ID and the host ID. The IP Subnet Mask is used to specify the network ID portion of the address, expressed in dotted decimal notation. The Prestige automatically calculates this mask based on the IP address that you assign. Unless you have a special need for subnetting, use the default mask as calculated by the Prestige.

Structure of this Manual



Chapter 1: Getting to Know Your ISDN Router

1.1 Features of the Prestige

Time and Date Setting

This all new feature allows the Prestige to connect to a time server to synchronize its system clock when it is booting.

Call Scheduling

The call scheduling feature allows the Prestige to manage a remote node and dictate when a remote node should be called and for how long

NAT(Network Address Translation)

ZyXEL's SUA (Single User Account) has now been replaced by the all new NAT support. NAT (Network Address Translation - NAT, RFC 1631) is the translation of an Internet Protocol address used within one network to a different IP address known within another network. NAT supports five types of IP/port mapping. They are:

1. One to One: In One-to-One mode, the Prestige maps one local IP address to one global IP address.
2. Many to One: In Many-to-One mode, the Prestige maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the SUA Only option in today's routers).
3. Many to Many Overload: In Many-to-Many Overload mode, the Prestige maps the multiple local IP addresses to shared global IP addresses.
4. Many to Many No Overload: In Many-to-Many No Overload mode, the Prestige maps the each local IP addresses to unique global IP addresses.
5. Server: This type allows us to specify multiple inside servers of different types behind the NAT.

ZyXEL is also proud to announce that NetMeeting is supported for both incoming and outgoing calls. For outgoing calls, there is no special configuration needed but for incoming calls, set the NetMeeting server to ports 1503 and 1720.

ISDN Basic Rate Interface (BRI) Support

The Prestige supports a single BRI. A BRI offers two 64 Kbps channels, which can be used independently for two destinations or be bundled to speed up data transfer.

Extensive Analog Phone Support

The Prestige is equipped with two standard phone jacks for you to connect analog devices such as telephones and FAX machines. It also supports supplementary services such as call waiting and 3-way calling.

Incoming Call Support

In addition to making outgoing calls, the Prestige allows you to configure it as a remote access server for telecommuting employees.

Outgoing Data Call Bumping Support

Call bumping is a feature that allows the Prestige to manage an MP bundle dynamically, dropping or reconnecting a channel in a bundle when necessary. Previously, the Prestige did this for voice calls only, but now with this new feature, the Prestige can drop a channel in an MP bundle if there is a data packet to another remote node. No SMT Menu changes are necessary for this new feature.

CLID Callback Support For Dial-In Users

CLID is an authentication method to identify a dial-in user. CLID callback is used as an ISDN toll saving feature because the call can be disconnected immediately without picking up the phone.

TCP/IP and PPP Support

- TCP/IP (Transmission Control Protocol/Internet Protocol) network layer protocol.
- PPP/MP (Point-to-Point Protocol/Multilink Protocol) link layer protocol.

Integrated 4-Port Ethernet Hub

The Prestige 100IH is equipped with a built-in 4-port Ethernet 10Base-T hub. The built-in hub eliminates the need to purchase a separate hub when building a one to four-port network. For a larger number of workstations, additional hubs can be daisy-chained to the Prestige.

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

- Accessing SMT (System Management Terminal) through telnet connection.
- Windows-based PNC (Prestige Network Commander).

Logging and Tracing

- CDR (Call Detail Record) to help to analyze and manage the telephone bill.
- Built-in message logging and packet tracing.
- Unix syslog facility support.

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

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.

Prestige Network Commander (PNC)

The PNC is a Windows based utility designed to allow users to access the Prestige's management settings via a Worldwide Web browser.

Upgrade P100IH Firmware via LAN

The PCT allows upgrading of the Prestige 100IH firmware over the local LAN.

Supplementary Voice Features

The Prestige supports the following Supplementary Voice Features on both of its analog, or POTS (Plain Old Telephone Service), phone ports:

- Call Waiting
- Three Way Calling (conference)
- Call Transfer
- Call Forwarding

1.2 Applications for Prestige 100IH

1.2.1 Internet Access

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

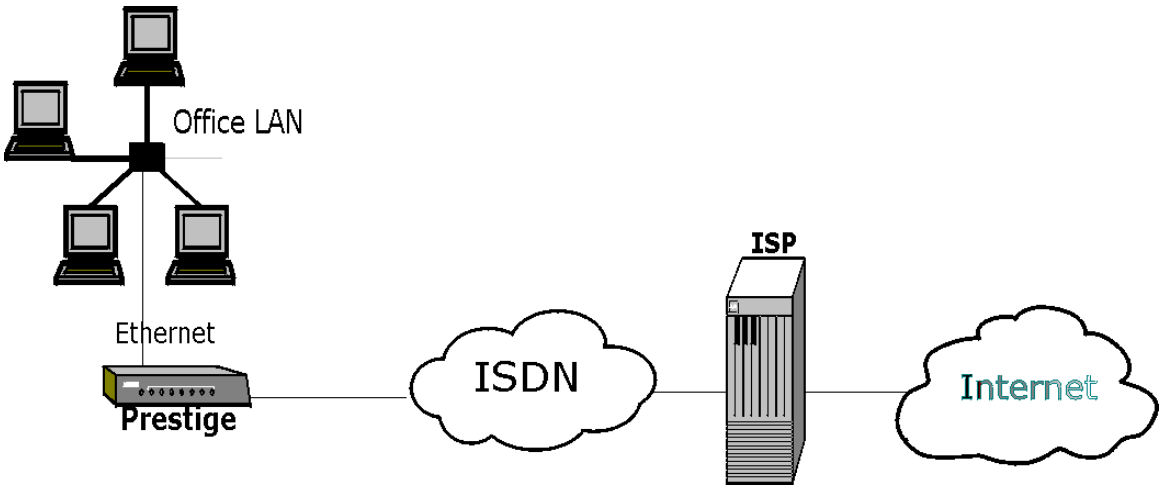


Figure 1-1 Internet Access Application

Internet Single User Account

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

1.2.2 LAN-to-LAN Connection

You can use the Prestige to connect two geographically dispersed networks over the ISDN line. A typical LAN-to-LAN application for your Prestige is shown next.

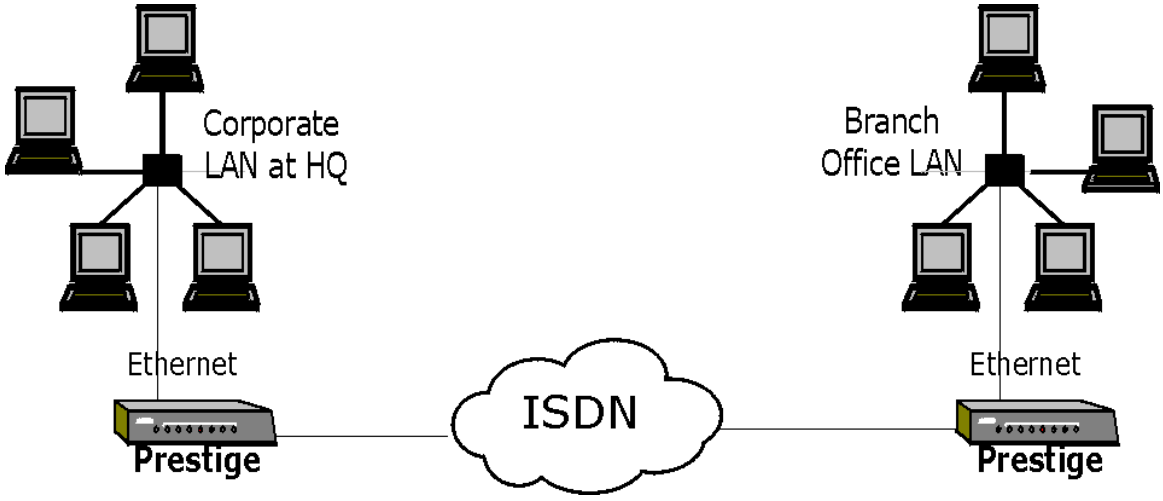


Figure 1-2 LAN-to-LAN Connection Application

1.2.3 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.

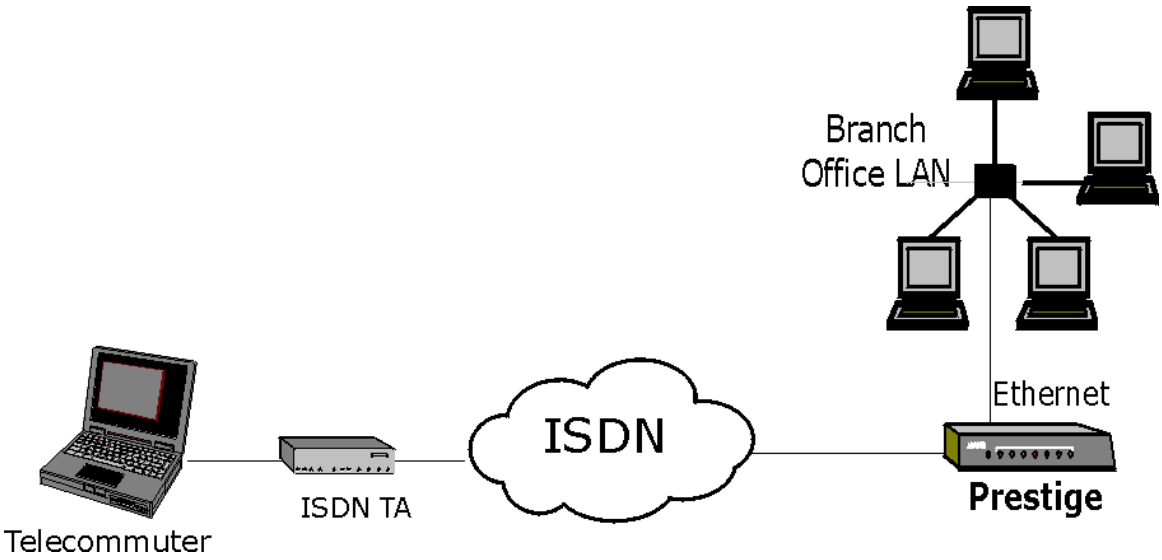


Figure 1-3 Telecommuting/Remote Access Server Application

Chapter 2: Hardware Installation & Initial Setup

2.1.1 Front Panel LEDs OF P100IH

The LED indicators on the front panel indicate the operational status of the Prestige 100IH. The following table describes the LED functions:

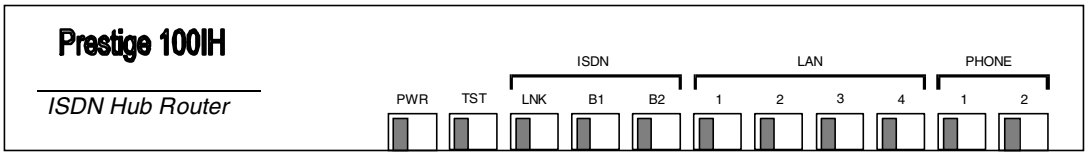


Figure 2-1 Front Panel Of P100IH

Table 2-1 LED functions

PWR	The PWR (power) LED is on when power is applied to the Prestige.
TST	A blinking TST (test) LED indicates the Prestige is functioning properly. A steady or an off TST indicates malfunction.
ISDN: LNK	The LNK (Link) LED is on when the Prestige is connected to an ISDN switch and the line has been successfully initialized.
ISDN: B1/B2	The B1/B2 LED is on when the corresponding B channel is in use.
LAN: 1 to 4	A steady LED indicates an active station is connected to the corresponding port. The LED blinks when the connected station is transmitting.
PHONE: 1/2	The LED is on when the device on the corresponding phone port is in use.

2.2 Prestige 100IH Rear Panel and Connections

The figure below shows the rear panel of your Prestige 100IH and the connection diagram.

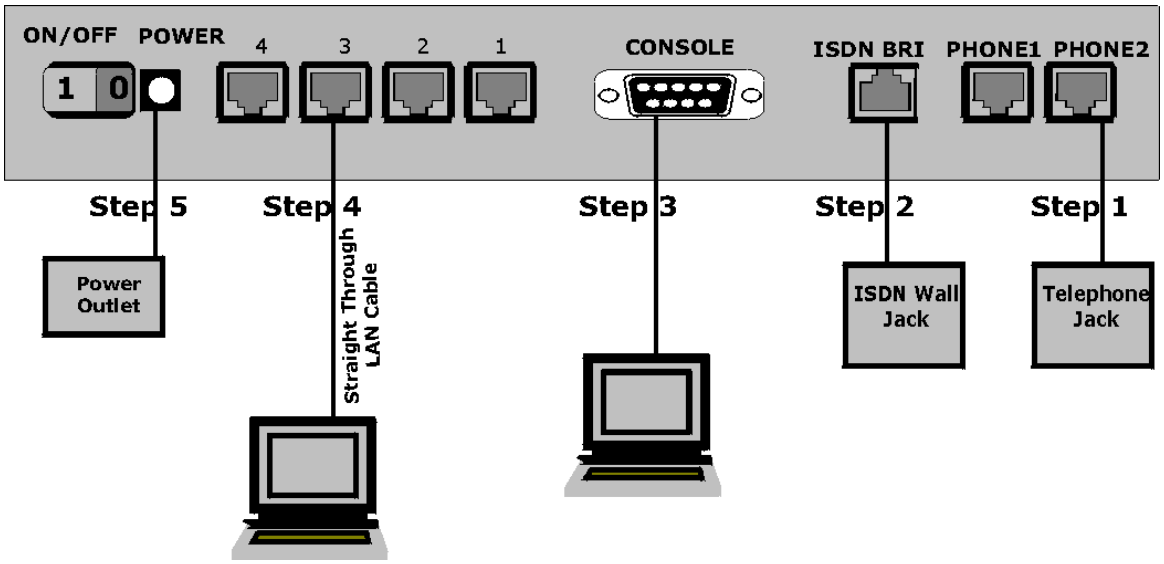


Figure 2-2 Prestige 100IH Rear Panel and Connections

Step 1. *Connecting a Telephone/Fax to the Prestige*

You can connect regular telephones, fax machines or other analog devices to the Prestige. To connect an analog device, plug the end of the telephone cord from the device to either port **PHONE1** or **PHONE2** on the rear panel of the Prestige.

Step 2. *Connecting the ISDN Line*

Connect the Prestige to the ISDN network using the included ISDN (black) cable. Plug one end of the cable into the port labeled **ISDN BRI** and the other to the ISDN wall jack.

Step 2. *Connecting the Console Port*

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

After the initial setup, you can modify the configuration remotely through telnet connections. See the Telnet Chapter for detailed instructions on using telnet to configure your Prestige.

Step 4. *Connecting a Workstation to the Prestige*

Ethernet 10Base-T networks use Unshielded Twisted Pair (UTP) cable with RJ-45 connectors that look like a bigger telephone plug with 8 pins. Connect a workstation to the built-in hub on the Prestige 100IH to create an Ethernet network. Connect one end of a straight through Ethernet cable (white tag) to the NIC on the workstation and the other end to one of the built-in 4 Ethernet ports on the Prestige 100IH (Figure 2-2).

Step 5. *Connecting the Power Adapter to your Prestige*

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

2.3 Additional Installation Requirements

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

1. A computer with Ethernet 10Base-T NIC (Network Interface Card).
2. A computer equipped with communications software configured to the following parameters:

- VT100 terminal emulation.
- 9600 bps (bits per second).
- No parity, 8 Data bits, 1 Stop bit.

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

2.4 Power On Your Prestige

At this point, you should have connected the console port, the ISDN BRI port, the Ethernet port and the power port to the appropriate devices or lines. You can now apply power to the Prestige by flipping the power switch to on (**I** is ON, **O** is OFF).

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.

```
Copyright (c) 1994 - 2000 ZyXEL Communications Corp.
ethernet address: 00:a0:c5:77:03:42
Resetting ISDN firmware.(2) ISDN Firmware DSS1: V 09D
.............................Press ENTER to continue...
.................
```

Figure 2-3 Power-On Display

Step 2. Entering Password

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

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

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

```
Enter Password : XXXX
```

Figure 2-4 Login Screen

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 the table below.

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

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

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

                          Prestige 100IH Main Menu

Getting Started                     Advanced Management
  1. General Setup                      21. Filter Set Configuration
  2. ISDN Setup
  3. Ethernet Setup                     23. System Password
  4. Internet Access Setup              24. System Maintenance

Advanced Applications                   26. Schedule Setup
  11. Remote Node Setup
  12. Static Routing Setup
  13. Default Dial-in Setup
  14. Dial-in User Setup
  15. NAT Setup                         99. Exit

                      Enter Menu Selection Number:
```

Figure 2-5 SMT Main Menu

2.5.1 System Management Terminal Interface Summary

Table 2-3 Main Menu Summary

#	Menu Title	Description
1	General Setup	Use this menu to set up general information and to enable routing for specific protocols and bridging.
2	ISDN Setup	Use this menu to set up the ISDN.
3	Ethernet Setup	Use this menu to set up Ethernet.
4	Internet Access Setup	A quick and easy way to set up Internet connection.
11	Remote Node Setup	Use this menu to set up the Remote Node for LAN-to-LAN connection, including Internet connection.
12	Static Routing Setup	Use this menu to set up static route for different protocols.
13	Default Dial-in Setup	Use this menu to set up 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 set up dial-in users.
15	NAT Setup	Use this menu to configure NAT.
21	Filter Set Configuration	Use this menu to setup filters to provide security, call control, etc.

23	System Security	Use this menu to setup security related parameters.
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
26	Schedule Setup	This menu allows the Prestige 100IH to manage a remote node and dictate when a remote node should be called and for how long.
99	Exit	To exit from SMT and return to the blank screen.

2.6 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. Enter 23 in the Main Menu to open **Menu 23 - System Password** as shown below.

When the Submenu 23 System Password appears, type in your existing system password, i.e., 1234, and press [Enter].

```
                    Menu 23.1 - System Password


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




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

Figure 2-6 Menu 23.1 - System Password

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

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

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

2.7 Filename conventions

The configuration file (sometimes called the romfile or romfile-0) contains the settings in the menus such as password, DHCP Setup defaults, TCP/IP Setup defaults etc. The external (i.e., not on the Prestige) configuration filename is usually the router model name with a *.rom extension, e.g., P100IH.rom. The

ZyNOS firmware file (sometimes referred to as the “ras” file) is the file that contains the ZyXEL Network Operating System firmware and the external firmware file is usually called the router model name with a *.bin extension, e.g., P100IH.bin. Rename the configuration filename to “rom-0” and the firmware filename to “ras” when transferring files to the Prestige (i.e., the internal filenames on the Prestige). Renaming the files is not necessary when you transfer files to the Prestige using the X-Modem protocol.

2.7.1 Resetting the Prestige

If you have forgotten your password or for some reason cannot access the SMT menu you will need to reinstall the configuration file. Uploading the configuration file replaces the current configuration file with the default configuration file, you will lose all configurations that you had before and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity and 1 stop bit (8n1). The password will be reset to the default of 1234, also.

Turn off the Prestige and begin a Telnet session with the default console port settings. Turn on the Prestige again. When you see the message "Press Any key to enter Debug Mode within 3 seconds", press any key to enter debug mode. You should already have downloaded the correct file from your nearest ZyXEL FTP site.

2.8 General Setup

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

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

Step 1. Enter 1 in the Main Menu to open **Menu 1 – General Setup**.

Step 2. The Menu 1 - General Setup screen appears, as shown below. Fill in the required fields marked [?] as shown in the following table.

```
                        Menu 1 - General Setup

        System Name= p100ih
        Location= branch
        Contact Person's Name= JohnDoe




             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 30 alphanumeric characters long. Spaces are not allowed, but dashes “-” and underscores "_" are accepted.	100IH
Location (optional)	Enter the geographic location (up to 31 characters) of your Prestige.	MyHouse
Contact Person's Name (optional)	Enter the name (up to 30 characters) of the person in charge of this Prestige.	JohnDoe

2.9 ISDN Setup Menus

Menu 2 is for you to enter the information about your ISDN line. Different telephone companies deploy different types of switches for ISDN service. Depending on the switch for your particular installation, you will have a different number of telephone numbers You need to pass the ISDN setup before your system can make an outgoing call or answer an incoming call.

2.9.1 Supplementary Voice Services

To take full advantage of the Supplementary Voice Services available though the Prestige’s phone ports, you will need to subscribe to your phone company for them. The Supplementary Voice Services available on the Prestige series include:

- Call Waiting
- Three Way Calling (conference)
- Call Transfer
- Call Forwarding.

The Advanced Phone Services chapter in this manual describes these services in more detail. There may be an additional charge for each of these services, so just choose the services you need. The phone company representative will ask you for the Feature Keys (buttons) for any Voice Features that you have chosen to activate. The Default Feature Keys for the Prestige series are as follows:

2.9.2 Setup Menus

Switch Type

The only switch type supported in Europe is DSS-1.

MSN and Subaddress

Depending on your location, you may have Multiple Subscriber Number (MSN) where the telephone company gives you more than one number for your ISDN line. You can assign each number to a different port, e.g., the first number to data calls, the second to A/B adapter 1 and so on. Or (DSS1) the telephone company may give you only one number, but allow you to assign your own subaddresses to different ports, e.g., subaddress 1 to data calls and 2 to A/B adapter 1.

Incoming Call Routing

The **Incoming Phone Number Matching** setting governs how incoming calls are routed. If you select **Multiple Subscriber Number (MSN)** or **Called Party Subaddress**, a call (either ISDN data or analog) is routed to the port that matches the dialed number; if no match is found, the call is dropped.

If you select **Don't Care**, then all data calls are routed to the Prestige itself. Analog calls, however, are routed to either A/B adapter 1 or 2, or simply ignored, depending on the **Analog Call Routing** field.

Global Calls

A global call is an incoming analog call where the switch did not send the dialed number. This happens most often when the call originates from an analog telephone line.

If you specify explicit matching, i.e., **Incoming Phone Number Matching** is either MSN or Called Party Subaddress, then global calls are always ignored. If it is **Don't Care** and **Analog Call Routing** is either A/B Adapter 1 or 2, then the Prestige uses **Global Analog Call** to decide how to handle global calls. If you set **Global Analog Call** to **Accept**, then global calls are routed to the port according to the **Analog Call Routing** setting; if you set **Global Analog Call** to **Ignore**, then the Prestige ignores all global calls. If **Analog Call Routing** is **Ignore** to begin with, then all analog calls, including global calls, are ignored.

PABX Outside Line Prefix

A PABX (Private Automatic Branch eXchange) generally requires you to dial a number (a single digit in most cases) when you need an outside line. If your Prestige is connected to a PABX, enter this number in **PABX Outside Line Prefix**, otherwise, leave it blank.

Please note that the PABX prefix is for calls initiated by the Prestige only. If you place a call from a device on either A/B adapter, you must dial the prefix by hand.

Outgoing Calling Party Number

If this field is not blank, the Prestige will use its value as the *calling party number* for "ISDN Data", "A/B Adapter 1" and "A/B Adapter 2" outgoing calls. Otherwise, the individual entries for "ISDNData", "A/B Adapter 1" and "A/B Adapter 2" will be used as the calling party number. You only need to fill in this field if your switch or PABX requires a specific calling party number for outgoing calls, otherwise, leave it blank. If you need to override the individual calling party number, enter Command Interpreter mode and issue the command:

```
isdn initstring set AT&ZOx=number
```

where x is 'I' for ISDN data calls, 'A' for A/B Adapter 1 and 'B' for A/B Adapter 2. For instance,

```
isdn initstring set AT&ZOI=100&ZOA=101&ZOB=102
```

sets the calling party number to 100 for ISDN data calls, 101 for A/B adapter 1 and 102 for A/B adapter 2.

```
                          Menu 2 - ISDN Setup

        Switch Type: DSS-1(Taiwan)
        B Channel Usage= Switch/Switch


        ISDN Data     =                                      Subaddress=
        A/B Adapter 1 =                                      Subaddress=
        A/B Adapter 2 =                                      Subaddress=
        A/B Adapter 2 Accepts Modem Call= Disable

        PABX Outside Line Prefix =
        Outgoing Calling party Number =
        Incoming Phone Number Matching= Multiple Subscriber Number (MSN)
          Analog Call Routing= N/A
          Global Analog Call= N/A
      Edit Advanced Setup = No

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

Figure 2-8 Menu 2 – ISDN Setup for DSS1

Table 2-5 Menu 2 – ISDN Setup

Switch Type	**This field is fixed as DSS1or 1TR6.**
B Channel Usage	In general, this is **Switch/Switch**. If you are only using one B channel (e.g., your Prestige is sharing the ISDN BRI line with another device on the S/T bus), then select **Switch/Unused**. The default is **Switch/Switch.** The options for this field are: ♦ **Switch/Switch** ♦ **Leased/Unused** ♦ **Switch/Unused** ♦ **Switch/Lease** ♦ **Unused/Leased** ♦ **Leased/Switch** ♦ **Leased/Leased**
ISDN Data & Subaddress	Enter the telephone number and the subaddress assigned to ISDN data calls for the Prestige. The maximum number of digits is 25 for the telephone number and 5 for the subaddress.
A/B Adapter 1 & Subaddress	Enter the telephone number and the subaddress assigned to A/B Adapter 1 (PHONE1).
A/B Adapter 2 & Subaddress	Same as above for A/B Adapter 2 (PHONE2).

PABX Outside Line Prefix	Enter the number for outside line access if the Prestige is connected to a PABX; otherwise, leave it blank. The maximum number of digits is 4.
Outgoing Calling Party Number	You only need to fill in this field if your switch requires a specific **Outgoing Calling Party Number**; otherwise, leave it blank.
Incoming Phone Number Matching	Determines how incoming calls are routed. The choices for this field are **Multiple Subscriber Number (MSN)**, **Called Party Subaddress** and **Don't Care**.
Analog Call Routing	Select the destination for analog calls. The choices are **A/B Adapter 1**, **A/B Adapter 2** and **Ignore**. This field is only applicable when **Incoming Phone Number Matching** is **Don't Care**.
Global Analog Call	Select how to handle global analog calls. The choices are **Accept** and **Ignore**. This field is not applicable when the **Analog Call Routing** is **Ignore**.
Edit Advanced Setup	Select **Yes** and press **Enter** to go to the advanced setup submenu (DSS1 only).

2.9.3 Advanced Setup

Select **Yes** in the **Edit Advanced Setup** field of **Menu 2 – ISDN Setup** to display menu 2.1 below.

ISDN Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number. By default call waiting is enabled on both telephone ports (except for France), but can be disabled on either port from **Menu 2.1**

How to use call waiting

The **Call Waiting** feature on your ISDN line works in exactly the same way as it does on a regular analog line. After hearing a call waiting indicator tone, press and immediately release the flash button on your telephone. This puts your current call on hold and answers the incoming call.

Calling Line Indication

The **Calling Line Indication**, or Caller ID, governs whether the other party can see your number when you call. If set to **Enable**, the Prestige sends the caller ID and the party you call can see your number; if it is set to **Disable**, the caller ID is blocked.

```
Menu 2.1 - ISDN Advanced Setup

Phone 1 Call Waiting= Enable
Phone 2 Call Waiting= Enable
Calling Line Indication= Enable
```

Figure 2-9 ISDN Advanced Setup

When you are finished, press **ENTER** at the message: 'Press ENTER to confirm', the Prestige uses the information that you entered to initialize the ISDN line. It should be noted that whenever the switch type is changed, the ISDN initialization takes slightly longer.

At this point, the Prestige asks if you wish to test your ISDN. If you select **Yes**, the Prestige will perform a loop-back test to check the ISDN line. If the loop-back test fails, please note the error message that you receive and take the appropriate troubleshooting action.

```
Setup LoopBack Test...
Dialing to 40000// ...
Sending and Receiving Data ...
Disconnecting...
LoopBack Test OK
### Hit any key to continue. ###
```

Figure 2-10 Loopback test

2.10 Ethernet Setup

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

```
Menu 3 - Ethernet Setup


1. General Setup
2. TCP/IP and DHCP Setup




Enter Menu Selection Number:
```

Figure 2-11 Menu 3 - Ethernet Setup

2.10.1 General Ethernet Setup

This menu allows you to select your **Ethernet interface**, either **10BaseT** or **AUI** for the Prestige 100 (only **10BaseT** for the Prestige 100IH, so this field does not appear) and 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:
                      protocol filters= 2
                        device filters=
                    Output Filter Sets:
                      protocol filters=
                        device filters=

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

Figure 2-12 Menu 3.1 - General Ethernet Setup

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

Chapter 3: Internet Access

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

3.1 Factory Ethernet Defaults

The Ethernet parameters of the Prestige are preset in the factory with the following values:

1. IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits).
2. DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If the parameters are satisfactory, you can skip to section 3.3 **TCP/IP Ethernet Setup and DHCP** to enter the DNS server address(es) if your ISP gives you explicit DNS server address(es). If you wish to change the factory defaults or to learn more about TCP/IP, please read on.

3.2 TCP/IP Parameters

3.2.1 IP Address and Subnet Mask

Similar to the 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 Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, e.g., only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

```
10.0.0.0      -  10.255.255.255

172.16.0.0    -  172.31.255.255

192.168.0.0   -  192.168.255.255
```

For this reason, it is recommended that you choose your network number from the above list.

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

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

3.2.3 RIP Setup

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

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

3.2.4 DHCP Configuration

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (workstations) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The Prestige has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. The Prestige 100IH can now also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients. DHCP relay is a middle role between the server and the client. Whenever a DHCP client requests an IP address, the "DHCP relay" relays requests and responses between the DHCP server and DHCP client, so it looks to the client that the Prestige is the actual DHCP server.

IP Pool Setup

The Prestige is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64 for the client machines. This leaves 31 IP addresses, 192.168.1.2 to 192.168.1.32 (excluding the Prestige itself which has a default IP of 192.168.1.1) for other server machines, e.g., server for mail, FTP, telnet, web, etc., that you may have.

DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, e.g., the IP address of *www.zyxel.com* is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The DNS server addresses that you enter in the DHCP setup are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP does give you the DNS server addresses, enter them in the **DNS Server** fields in **DHCP Setup**.

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

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

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

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

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

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

      TCP/IP Setup:
        IP Address= 192.68.1.1
        IP Subnet Mask= 255.255.255.0
        RIP Direction= Both
          Version= RIP-1


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

Figure 3-1 Menu 3.2 – TCP/IP and DHCP Ethernet Setup

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

Table 3-1 DHCP Ethernet Setup Menu Fields

Field	Description	Example
DHCP Setup		
DHCP=	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. If the Prestige 100IH is set to **Relay**, it will act as a surrogate DHCP server where it relays IP address assignment from the actual real DHCP server to the clients. When DHCP is used, the following four items need to be set:	**None** **Server** (default) **Relay**
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size, or count, of the IP address pool.	32
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	
Relay Server Address=	If you chose **Relay** in the DHCP= field above, then enter the IP of the actual DHCP server from which the Prestige will relay requests and responses here.	

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

Table 3-2 TCP/IP Ethernet Setup Menu Fields

Field	Description	Example
TCP/IP Setup		
IP Address	Enter the IP address of your Prestige in dotted decimal notation	192.168.1.1 (default)
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige	255.255.255.0
RIP Direction	Press the space bar to select the RIP direction from **Both/In Only/Out Only.**	**Both** (default)
Version	Press the space bar to select the RIP version from **RIP-1/RIP-2B/RIP-2M.**	**RIP-1** (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 the table below 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 **Internet Access Setup** to go to Menu 4 - Internet Access Setup, as displayed below. The following table contains instructions on how to configure your Prestige for Internet access.

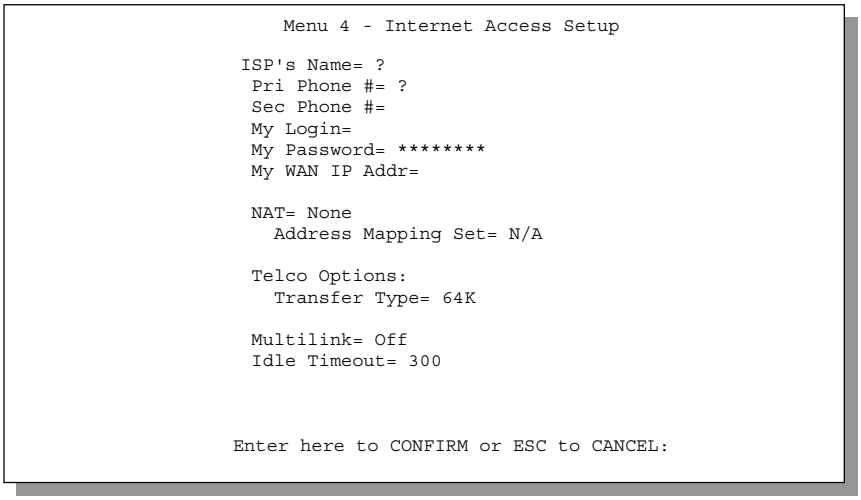


Figure 3-2 Menu 4 – Internet Access Setup

Table 3-4 Internet Access Setup Menu Fields

Field	Description
ISP's Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.
ISP IP Addr	Enter the IP Address of the remote gateway at the ISP's site. If you don't have this data, just leave it blank.
Pri Phone and Sec Phone Number	Both the Primary and the Secondary Phone number refer to the number that the Prestige dials to connect to the ISP.
My Login Name	Enter the login name given to you by your ISP.
My Password	Enter the password associated with the login name above.
My WAN IP Addr=	
NAT Address Mapping Set=	Choose from None, Full Feature or SUA Only. *See Chapter 4:* for a full discussion of this new feature. A NAT Server Set is a list of LAN side servers mapped to external ports (similar to the old SUA menu 15.1 before). You

Field	Description
	may enter any server set number up to 10, but the first one is used foe SUA only.
Telco options: Transfer Type	This field specifies the type of connection between the Prestige and this remote node. Select **64K,** or **Leased**.
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. This option is only available if the transfer type is **64K.** See menu 11.2 for more details.
Idle Timeout	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. *This option only applies when the Prestige initiates the call.*

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.

Chapter 4: NAT

4.1 Introduction

NAT (Network Address Translation - NAT, RFC 1631) is the translation of an Internet Protocol address used within one network to a different IP address known within another network. One network is designated the *inside* network and the other is the *outside*. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and "unmaps" the global IP addresses on incoming packets back into local IP addresses. The IP addresses for the NAT can be either fixed or dynamically assigned by the ISP. In addition, you can designate servers, e.g., a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see below), NAT offers the additional benefit of firewall protection. If no server is defined in these cases, all incoming inquiries will be filtered out by your Prestige, thus preventing intruders from probing your network. For more information on IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT).*

4.1.1 Advantages of NAT

- NAT is a cost-effective solution to access the Internet or other remote TCP/IP networks as NAT conserves on the number of global IP addresses that a company needs in its communication with the outside world.
- NAT supports popular Internet applications such as MS traceroute, CuSeeMe, IRC, RealAudio, VDOLive, Quake and PPTP with no extra configuration needed.
- NAT supports servers, including multiple servers of the same type, to be accessible to the outside world.
- NAT can provide firewall protection if you do not specify a server (for Many-to-One and Many-to-Many Overload mapping) and all incoming inquiries will be filtered out by your Prestige.
- UDP and TCP packets can be routed. In addition, partial ICMP, including echo and traceroute, is supported.

4.1.2 How NAT works

Each packet consists of two addresses – a source address and a destination address. For outgoing packets, the ILA is the source address on the LAN, and the IGA is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. The term "Inside" refers to the set of networks that are subject to translation. Network Address Translation operates by mapping private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One

and Many-to-Many Overload NAT mapping) and then forwards each packet to the Internet ISP, thus making them appear as if they had come from the NAT system itself (e.g., the Prestige). The Prestige keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following diagram illustrates this.

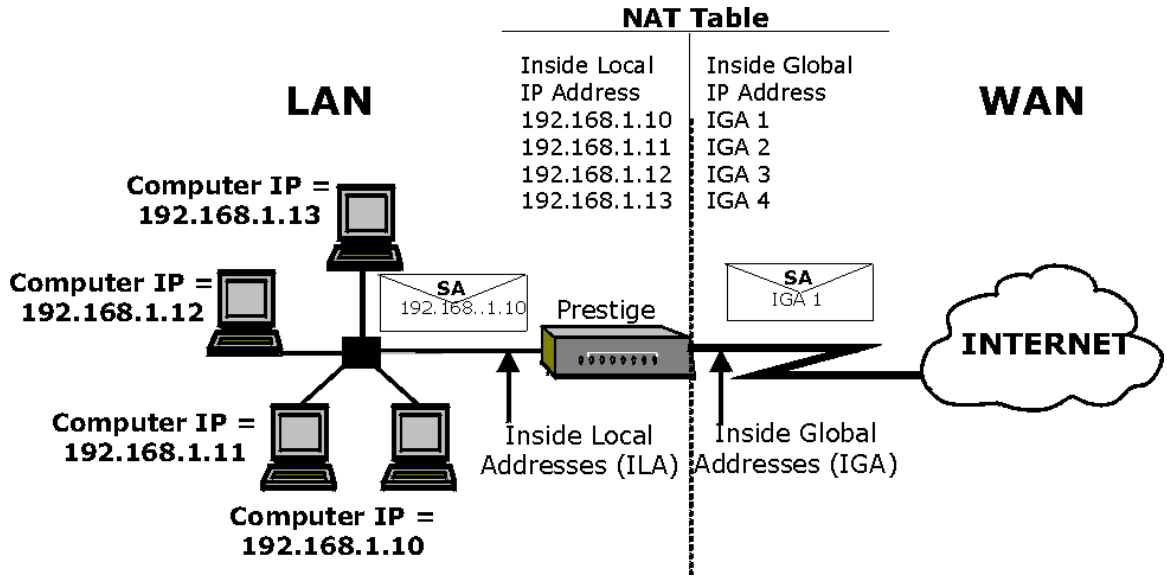


Figure 4-1 How NAT Works

4.1.3 NAT Mapping Types

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

1. One to One: In One-to-One mode, the Prestige maps one local IP address to one global IP address.
2. Many to One: In Many-to-One mode, the Prestige maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the SUA Only option in today's routers).
3. Many to Many Overload: In Many-to-Many Overload mode, the Prestige maps the multiple local IP addresses to shared global IP addresses.
4. Many to Many No Overload: In Many-to-Many No Overload mode, the Prestige maps the each local IP addresses to unique global IP addresses.
5. Server: This type allows us to specify multiple inside servers of different types behind the NAT.

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

The following table summarizes these types.

Table 4-1 NAT Mapping Types

Type	IP Mapping
One-to-One	ILA1←→ IGA1
Many-to-One (SUA/PAT)	ILA1←→ IGA1 ILA2←→ IGA1 …
Many-to-Many Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA1 ILA4←→ IGA2 …
Many-to-Many No Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA3 …
Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1

4.2 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs behind the Prestige can "talk" to three distinct Internet destinations. More examples follow at the end of this chapter.

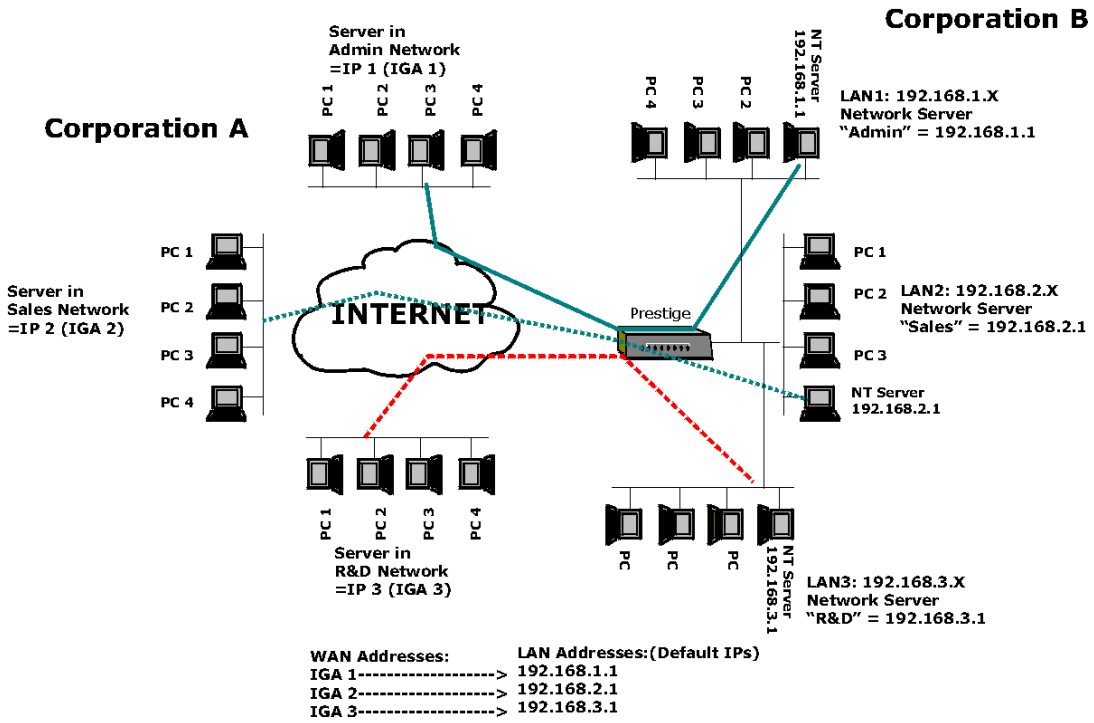


Figure 4-2 NAT Application

4.3 SUA (Single User Account) Versus NAT

SUA (Single User Account) in previous ZyNOS versions is a NAT set with 2 rules, Many-to-One and Server. See *section 4.5.1* for a detailed description of the NAT set for SUA. The Prestige now has **Full Feature** NAT support to map global IP addresses to local IP addresses of clients or servers using all mapping types as outlined in *Table 4-1 NAT Mapping Types*. The Prestige supports NAT sets on a remote node basis. They are reusable, but only one set is allowed for each remote node. The last set (**SUA Only** option in Menu 15.1) is a convenient, pre-configured, read only Many-to-1 port mapping set, sufficient for most purposes (*see section 4.6* for some examples) and helpful to people already familiar with SUA in previous ZyNOS versions.

Please upload the latest configuration file (romfile) for NAT and SUA to work properly.

4.4 SMT Menus

NAT Setup In The Main Menu

Enter 15 from the main menu to configure NAT (this was SUA in previous versions).

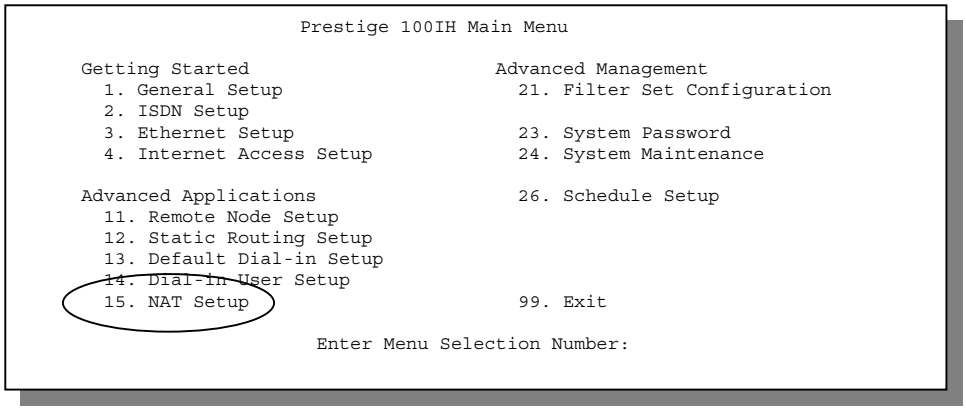


Figure 4-3 NAT in the Main Menu

4.4.1 Applying NAT in the SMT Menus

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

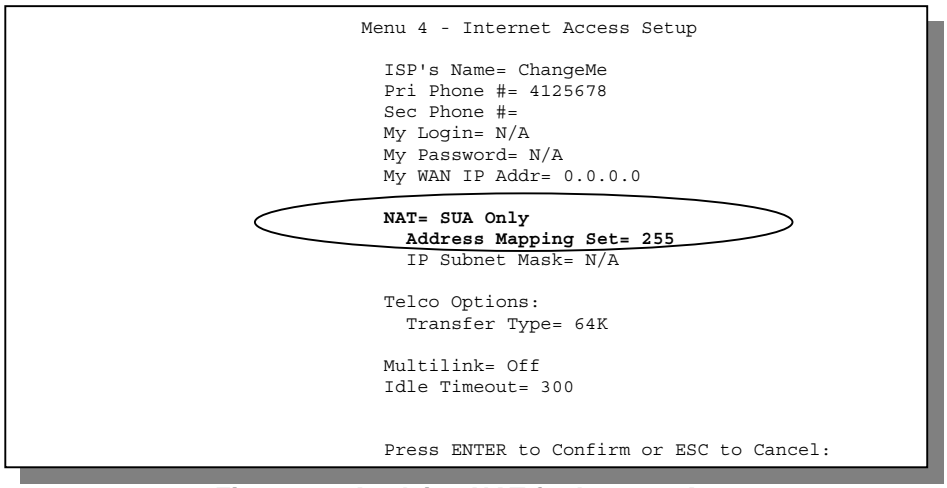


Figure 4-4 Applying NAT for Internet Access

This figure shows how you apply NAT to the remote node in Menu 11.1.

Step 1. Enter 11 from the Main Menu.

Step 2. Move the cursor to the **Edit IP** field, press the [SPACEBAR] to toggle the default **No** to **Yes**, then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options.**

```
            Menu 11.3 - Remote Node Network Layer Options

        Rem IP Address= 172.16.1.20
        IP Subnet Mask= 255.255.0.0
        My WAN Addr = 192.168.1.10

        NAT= Full Feature
          Address Mapping Set= 4

        Metric= N/A
        Private= N/A
        RIP Direction= Both
          Version= RIP-2B




        Enter here to CONFIRM or ESC to CANCEL:

        Press Space Bar to Toggle.
```

Figure 4-5 Applying NAT to the Remote Node

The following table describes the options for Network Address Translation.

Table 4-2 Applying NAT in Menus 4 & 11.3

Field	Options	Description
Network Address Translation	**Full Feature**	When you select this option the SMT will use Address Mapping Set 1 (Menu 15.1 – *see section 4.5.1* for further discussion). You can configure any of the 5 mapping types described in *Table 4-1 NAT Mapping Types*.
	None	NAT is disabled when you select this option.
	SUA Only	When you select this option the SMT will use Address Mapping Set 255 (Menu 15.1 – *see section 4.5.1*). It is a convenient, pre-configured, read only Many-to-1 port mapping set, sufficient for most purposes and helpful to people already familiar with SUA in previous ZyNOS versions. Note that there is also a **Server** type whose IGA is **0.0.0.0** in this set.

Address Mapping Set=	A NAT Server Set is a list of LAN side servers mapped to external ports (similar to the old SUA menu 15.1 before). You may enter any server set number up to 10, but the first one is used foe SUA only.

4.5 Configuring NAT

To configure NAT, enter 15 from the Main Menu to bring up the following screen.

```
                    Menu 15 - NAT Setup

              1.    Address Mapping Sets
              2.    NAT Server Sets


              Enter Menu Selection Number:
```

Figure 4-6 Menu 15 NAT Setup

4.5.1 Address Mapping Sets and NAT Server Sets:

Use the Address Mapping Sets menus and submenus to create the mapping table used to assign global addresses to machines on the LAN. Each remote node must specify which NAT Address Mapping Set to use. You can see the NAT Address Mapping sets in Menu 15.1. Set 255 is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use Set 1, which supports all mapping types as outlined in *Table 4-3*. When you select **SUA Only**, the SMT will use the pre-configured Set 255 (read only) – *see section 4.2*.

The NAT Server set is a list of LAN side servers mapped to external ports. To use this set (one set for the P312), a server rule must be set up inside the NAT Address Mapping set. Please *see section 4.5.2* for further information on these menus.

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

```
                    Menu 15.1 - Address Mapping Sets

                         1. Marc
                         2.
                         3.
                         4.
                         5.
                         6.
                         7.
                         8.
                         255. SUA (read only)


                             Enter Menu Selection Number:
```

Figure 4-7 Menu 15.1 - Address Mapping Sets

Let's look first at Option 255. Option 255 is equivalent to SUA in previous ZyXEL routers (*see section 4.2).* The fields in this menu cannot be changed. Entering 255 brings up this screen.

```
                    Menu 15.1.255 - Address Mapping Rules

 Set Name= SUA

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


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

Figure 4-8 SUA Address Mapping Rules

The following table explains the fields in this screen.

Please note that the fields in this menu are read-only. The Type, Local and Global Start/End IPs are normally (not for this read-only menu) configured in Menu 15.1.1.1 (described later) and the values are displayed here.

Table 4-3 SUA Address Mapping Rules

Field	Description	Options/Example
Set Name	This is the name of the set you selected in Menu 15.1 or enter the name of a new set you want to create.	**SUA**
Idx	This is the index or rule number.	**1**
Local Start IP	This is the starting local IP address (ILA).	**0.0.0.0**
Local End IP	This is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.	**255.255.255.255**
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the Global Start IP.	**0.0.0.0**
Global End IP	This is the ending global IP address (IGA).	**N/A**
Type	These are the mapping types discussed above (*see Table 4-1*). Type **Server** allows us to specify multiple servers of different types behind NAT to this machine. *See section 4.6* for some examples.	**Server**
Server Set	This refers to the NAT Server Sets in menu 15.1	**255**

Note: For all Local and Global IPs, the End IP address must begin after the IP Start address.

Now let's look at Option 1 in Menu 15.1. Enter 1 to bring up this menu. We'll just look at the differences from the previous menu. Note that, this screen is not read only, so we have extra **Action** and **Select Rule** fields. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.

Please note that if the Set Name field is left blank, the entire set will be deleted.

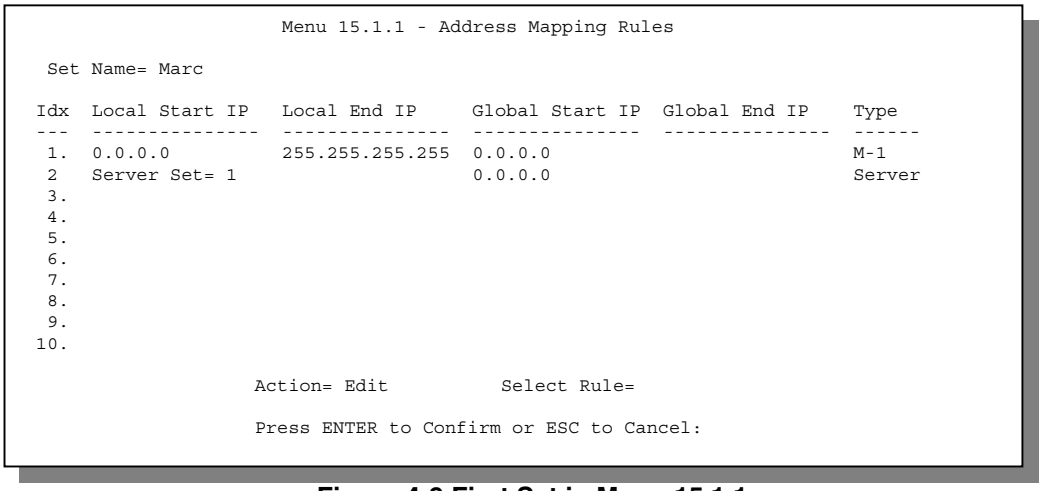


Figure 4-9 First Set in Menu 15.1.1

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

Ordering Your Rules

If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9.

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

The description of the other fields is as described above. The Type, Local and Global Start/End IPs are configured in Menu 15.1.1.1 (described later) and the values are displayed here.

Table 4-4 Menu 15.1.1

Field	Description	Option
Set Name	Enter a name for this set of rules. This is a required field. Please note that if this field is left blank, the entire set will be deleted.	**Marc**
Action	There are 4 actions. The default is **Edit**. **Edit** means you want to edit a selected rule (see following field). **Insert Before** means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. **Delete** means to delete the selected rule and then all the rules after the selected	**Edit** **Insert Before** **Delete** and **Save Set**

Field	Description	Option
	one will be advanced one rule. **Save Set** means to save the whole set (note when you choose this action, the **Select Rule** item will be disabled).	
Select Rule	When you choose **Edit**, **Insert Before** or **Delete** in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.	**1**

N.B.: Save Set in the Action field means to save the whole set. You must do this if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.

Be careful when ordering your rules as each rule is executed in turn beginning from rule 1.

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the Type, Local and Global Start/End IPs displayed in Menu 15.1.1.

```
                    Menu 15.1.1.1 - Marc - Rule 1

          Type= Many-to-One

          Local IP:
            Start= 0.0.0.0
            End  = 255.255.255.255

          Global IP:
            Start= 0.0.0.0
            End  = N/A

          Server Mapping Set= N/A


                        Press ENTER to Confirm or ESC to Cancel:

      Press Space Bar to Toggle.
```

Figure 4-10 Editing The First Rule in a Set

```
                    Menu 15.1.1.1 - Marc - Rule 2

            Type= Server

            Local IP:
              Start= N/A
              End  = N/A

            Global IP:
              Start= 0.0.0.0
              End  = N/A

            Server Mapping Set= 1


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

Figure 4-11 Editing The Second Rule in a Set

The following table describes the fields in these screens.

Table 4-5 Menu 15.1.1.1 – configuring an individual rule

Field	Description	Option/Example
Type	Press the [SPACEBAR] to toggle through a total of 5 types. These are the mapping types discussed above (*see Table 4-1*). Type **Server** allows us to specify multiple servers of different types behind NAT to this machine. *See section 4.6* for some examples.	**One-to-One** **Many-to-One** **Many-to-Many Overload** **Many-to-Many No Overload and Server**
Local IP	Local and Global IP fields are **N/A** for the **Server Type.**	
Start	This is the starting local IP address (ILA).	**0.0.0.0**
End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for **One-to-One** and **Server** types**.**	**255.255.255.255**
Global IP		
Start	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to **0.0.0.0** only if the types are **Many-to-One** or **Server**.	**0.0.0.0**
End	This is the ending global IP address (IGA).	**172.16.23.55**

Field	Description	Option/Example
	This field is **N/A** for **One-to-One, Many-to-One** and **Server** types.	

Note: For all Local and Global IPs, the End IP address must begin after the IP Start address, i.e., you cannot have an End IP address beginning before the Start IP address.

4.5.2 NAT Server Sets

A NAT Server Set is a list of LAN side servers mapped to external ports (similar to the old SUA menu 15.1 before).

Multiple Servers Behind NAT

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

As an example (see the following figure), if you have a web server at 192.168.1.36 and an FTP server 192.168.1.33, then you need to specify for port 80 (web) the server at IP address 192.168.1.36 and for port 21 (FTP) another at IP address 192.168.1.33.

Please note that a server can support more than one service, e.g., a server can provide both FTP and DNS service, while another provides only web service.

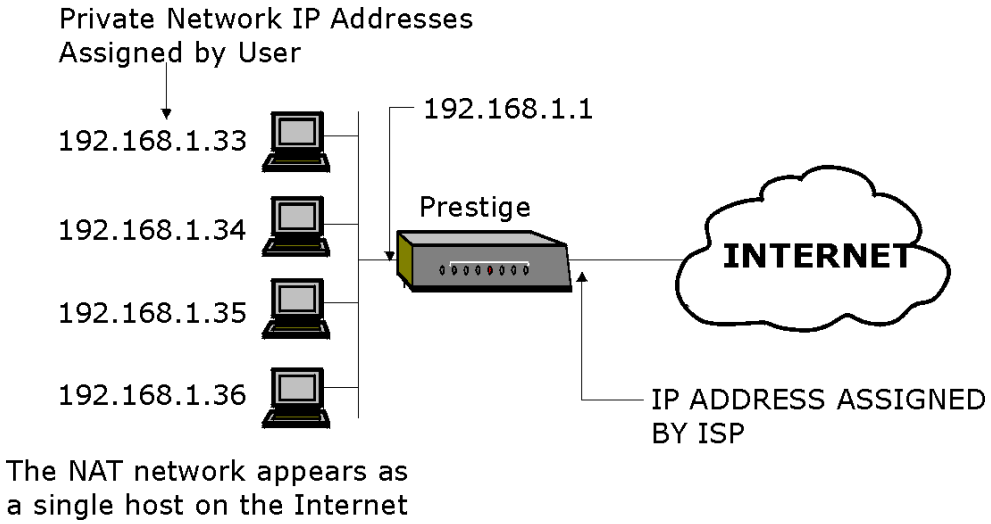


Figure 4-12 Multiple Servers Behind NAT

Configuring a Server behind NAT

Follow the steps below to configure a server behind NAT:

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

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

```
                Menu 15.2 - NAT Server Sets

                  1. Server Set 1 (Used for SUA Only)
                  2. Server Set 2
                  3. Server Set 3
                  4. Server Set 4
                  5. Server Set 5
                  6. Server Set 6
                  7. Server Set 7
                  8. Server Set 8
                  9. Server Set 9
                 10. Server Set 10

                         Enter Set Number to Edit:
```

Figure 4-13 Menu 15.2 – NAT Server Sets

Step 3. Enter the index number of the set you want to configure. This brings up menu 15.2.X where X is the index number.

Step 4. Enter the service port number in the **Port #** field and the inside IP address of the server in the IP Address field.

```
          Menu 15.2.2 - Multiple Server Configuration
                Port #           IP  Address
                ----            ---------------
                1.Default       0.0.0.0
                2.21            192.168.1.33
                3.23            192.168.1.34
                4.25            192.168.1.35
                5.80            192.168.1.36
                6. 0            0.0.0.0
                7. 0            0.0.0.0
                8. 0            0.0.0.0
                9. 0            0.0.0.0
                10. 0           0.0.0.0
                11. 0           0.0.0.0
                12. 0           0.0.0.0

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

Figure 4-14 Menu 15.2.1 –Multiple Server Configuration

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

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

Table 4-6 Services & Port numbers

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

4.6 Examples

4.6.1 Example 1 - Internet Access Only

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

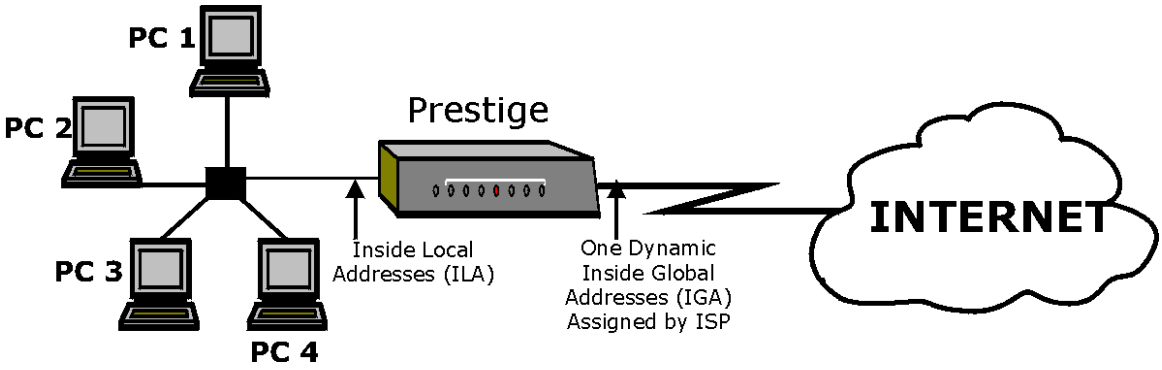


Figure 4-15 NAT Example 1

```
                Menu 4 - Internet Access Setup

                  ISP's Name= ChangeMe
                  Pri Phone #= 4125678
                  Sec Phone #=
                  My Login= N/A
                  My Password= N/A
                  My WAN IP Addr= 0.0.0.0

                  NAT= SUA Only
                    Address Mapping Set= 255
                    IP Subnet Mask= N/A

                  Telco Options:
                    Transfer Type= 64K

                  Multilink= Off
                  Idle Timeout= 300


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

Figure 4-16 Internet Access & NAT Example

From Menu 4 shown above, simply choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section 4.1.3.* The **SUA Only** read only option from the **Network Address Translation** field in Menus 4 and 11.3 is specifically pre-configured to handle this case.

4.6.2 Example 2 – Internet Access with an Inside Server

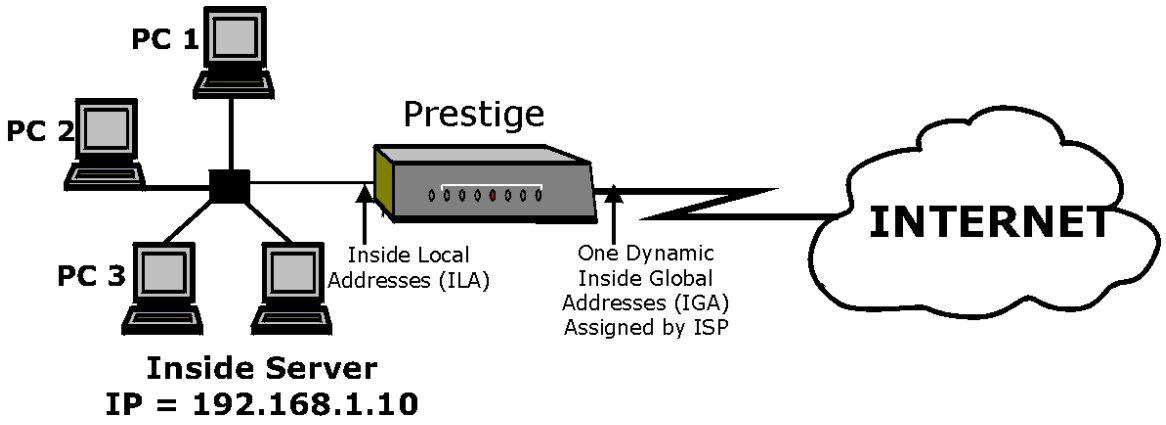


Figure 4-17 NAT Example 2

In this case, we do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to Menu 15.2.1 to specify the Inside Server behind the NAT as shown in the next figure.

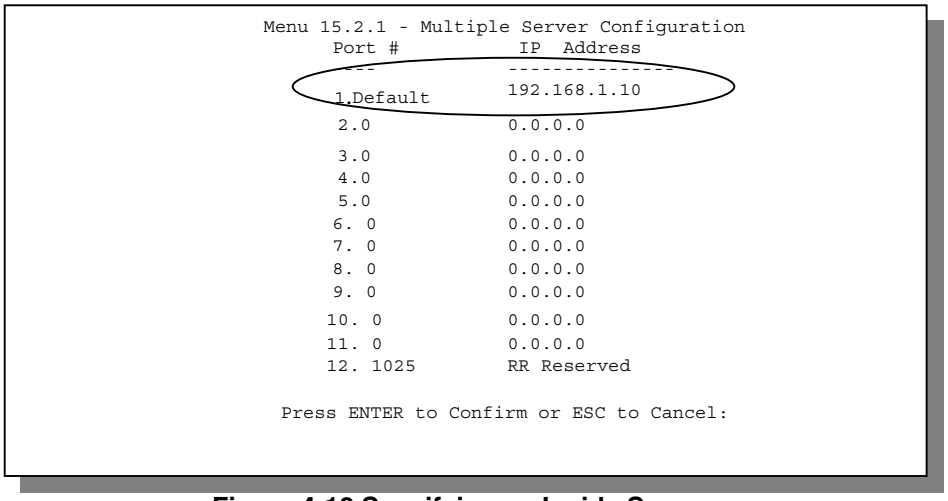


Figure 4-18 Specifying an Inside Sever

4.6.3 Example 3 – General Case

In this example, we have 3 IGAs from our ISP. We have many departments but two have their own FTP server. All departments share the same router. We want to reserve 1 IGA for each department with an FTP server and the other IGA is used by all. We want to map the FTP servers to the first two of our IGAs and the other LAN traffic to the remaining IGA. We also want to map out third IGA to an inside web server and mail server. We need to configure 4 rules, 2 bi-directional and 2 one directional as follows.

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

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

Rule 3. We map our other outgoing LAN traffic to IGA3 (**Many : 1** mapping).

Rule 4. We also map our third IGA to our web server and mail server on the LAN. Type **Server** allows us to specify multiple servers, of different types, to other machines behind NAT on the LAN.

Our situation looks somewhat like this:

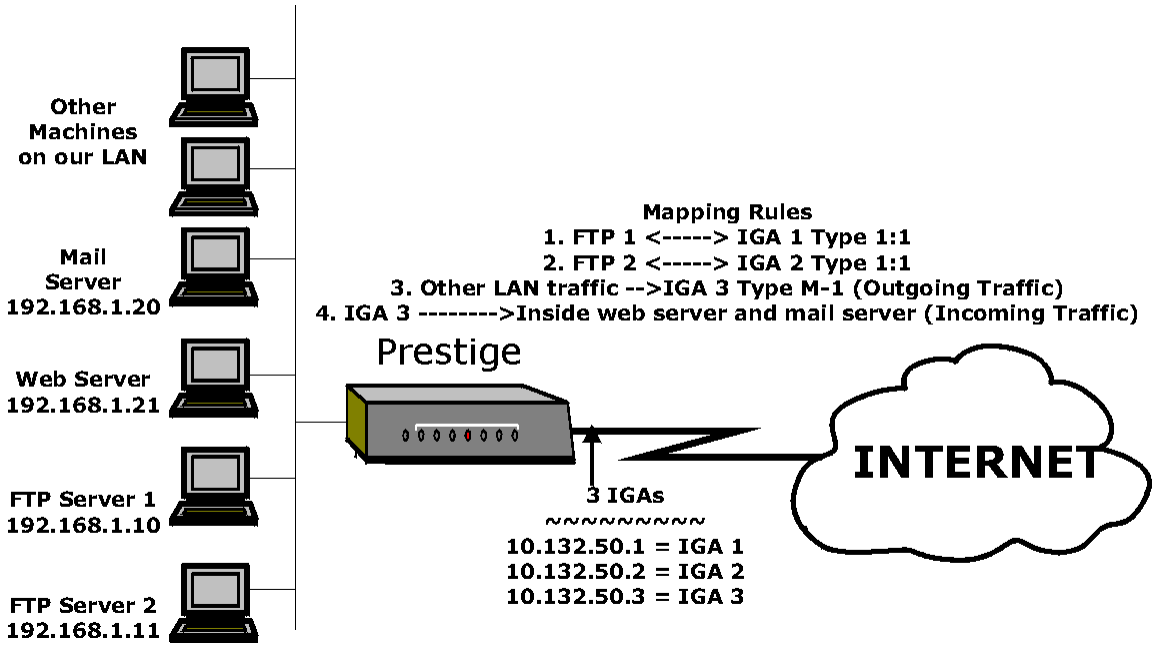


Figure 4-19 NAT - Example 3

In this case we need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets.** Therefore we must choose the **Full Feature** option from the **Network Address Translation** field in Menu 4 or Menu 11.3 and select an available NAT Server Set, say Server Set 2, that we configure later.

Step 1. Enter **15** from the Main Menu.

Step 2. Enter **1** to configure the Address Mapping Sets.

Step 3. Choose 1 to begin configuring this new set. Enter a **Set Name**, choose the **Edit Action** and then select **1** from **Select Rule** field. Press [ENTER] to confirm.

Step 4. Select **Type=** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (*See Figure 4-20)*

Step 5. Repeat the previous step for rules 2 to 4 as outlined above.

Step 6. When finished, Menu 15.1.1 should look like as shown in *Figure 4-21.*

The following figure shows how to configure the first rule.

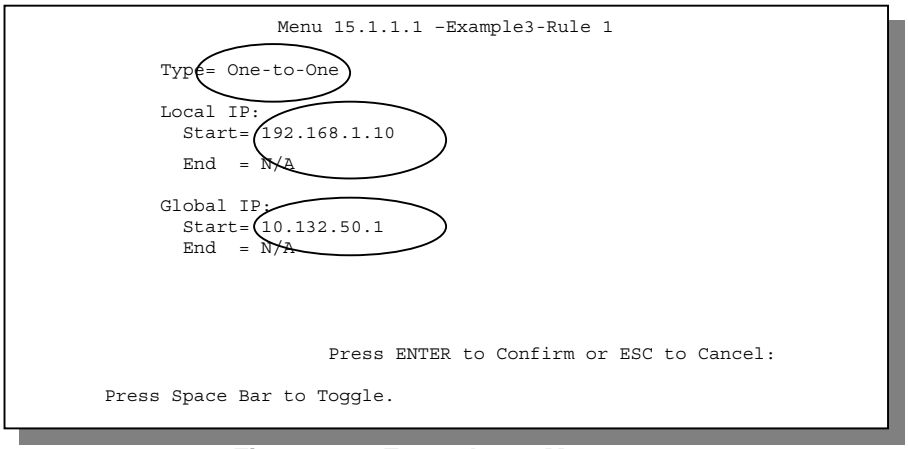


Figure 4-20 Example 3 – Menu 15.1.1.1

When we have configured all four rules, Menu 15.1.1 should look as follows.

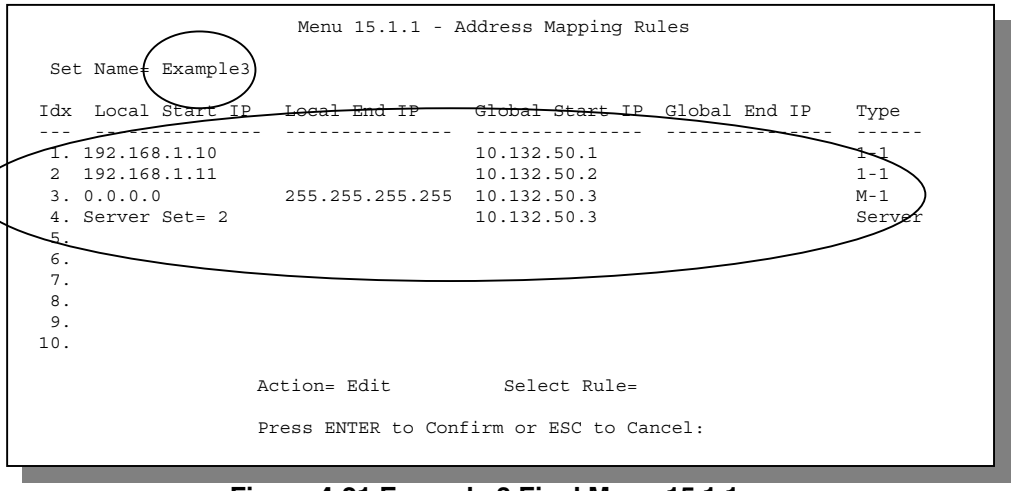


Figure 4-21 Example 3 Final Menu 15.1.1

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

Step 7. Enter **15** from the Main Menu.

Step 8. Now enter **2** from this menu, enter 2 again to select Server Set 2 and configure it as shown in *Figure 4-22*.

```
Menu 15.2.1 - Multiple Server Configuration
      Port #            IP  Address
      ----              ---------------
      1.Default         0.0.0.0
      2.80              192.168.1.21
      3.25              192.168.1.20
      4.0               0.0.0.0
      5.0               0.0.0.0
      6. 0              0.0.0.0
      7. 0              0.0.0.0
      8. 0              0.0.0.0
      9. 0              0.0.0.0
      10. 0             0.0.0.0
      11. 0             0.0.0.0
      12. 1025          RR Reserved

  Press ENTER to  onfirm or ES  to  an el:
```

Figure 4-22 Example 3 – Menu 15.2

4.6.4 Example 4 – Non NAT Friendly Application Programs

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

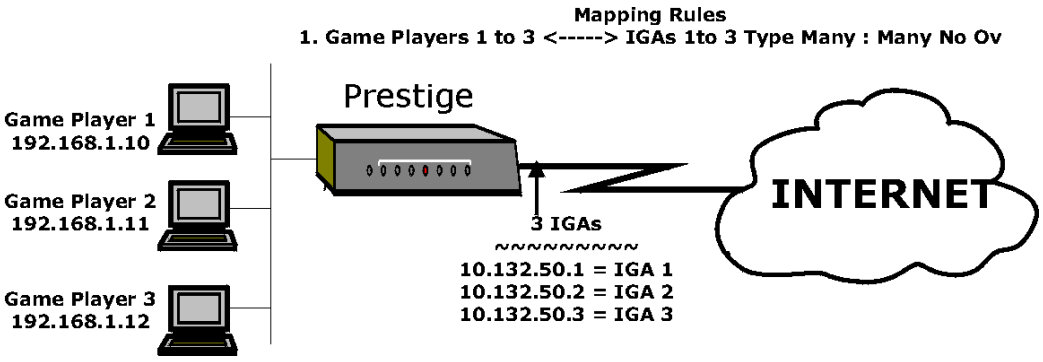


Figure 4-23 NAT Example 4

Some applications still won't work through NAT even when using types One-to-One **and** Many-to-Many No Overload **mapping types.**

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

```
                          Menu 15.1.1.1 -Example4- Rule 1

        Type= Many-to-Many No Overload

        Local IP:
          Start= 192.168.1.10
          End  = 192.168.1.12

        Global IP:
          Start= 10.132.50.1
          End  = 10.132.50.3









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

Figure 4-24 Example 4- Menu 15.1.1.1

After you've configured this menu, you should see the following screen.

```
                       Menu 15.1.1 - Address Mapping Rules

 Set Name= Example4

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

                  Action= Edit          Select Rule=

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

Figure 4-25 Example 4 - Menu 15.1.1 - Address Mapping Rules

Chapter 5: 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 of 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 (TCP/IP) will be covered in *Chapter 5*.

5.1 Remote Node Setup

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

5.1.1 Minimum Toll Period

Phone calls are normally charged per basic time unit with the time being rounded up to the nearest unit when bills are calculated. For example, the Prestige may make a call but drop the call after 10 seconds (maybe there was no reply) but the call would still be charged at a minimum time unit, let's say 3 minutes. With minimum toll period, the Prestige will try to use all the toll period. In the above case, the Prestige tries to extend the idle timeout to the nearest 3 minutes (basic charging unit of time). If there is traffic during the extended 2 minutes and 50 seconds, the idle timeout will be cleared and a second call is eliminated. Since the session time calculation by the Prestige is not always perfectly synchronized with your telephone company, the Prestige drops the channel 5 seconds before the toll period you set, to compensate for any lag. As such, you must not set the minimum toll period to less than 5 seconds.

5.1.2 Remote Node Profile

To configure a remote node, follow these steps:

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

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

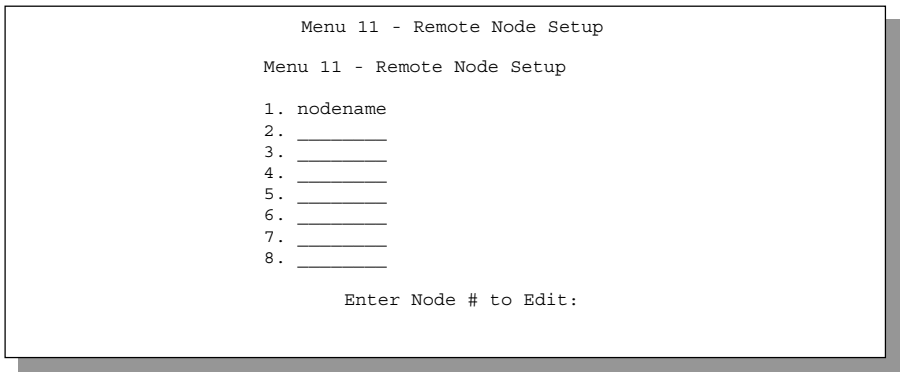


Figure 5-1 Menu 11 – Remote Node Setup

When Submenu 11.1 - Remote Node Profile appears, fill in the fields as described in the table below to define this remote profile. The Remote Node Profile Menu Fields table shows how to configure the Remote Node Menu.

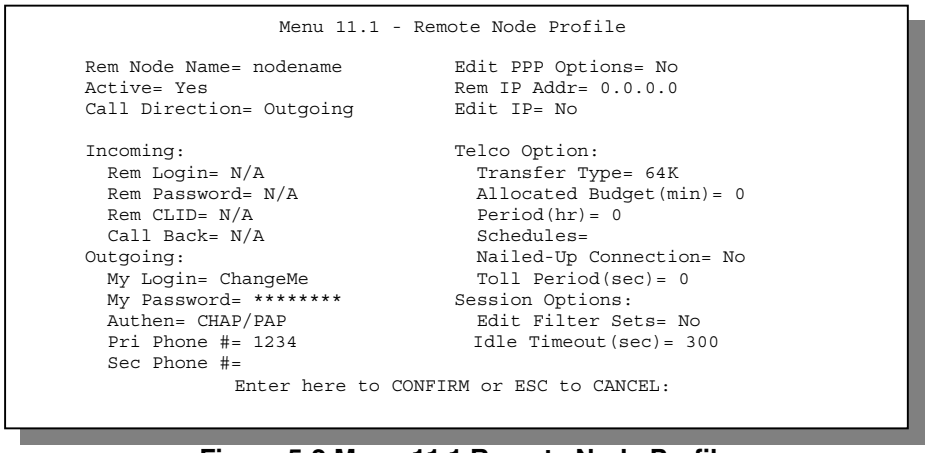


Figure 5-2 Menu 11.1 Remote Node Profile

Table 5-1 Remote Node Profile Menu Fields

Field	Description	Options
Rem Node Name	This is a required field [?]. Enter a descriptive name for the remote node, for example, Corp. This field can be up to eight characters. This name must be unique from any other remote node name or remote dial-in user name.	
Active	Press 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 **Yes/No**
Call Direction	● If this parameter is set to **Both**, your Prestige can both place and receive calls to/from this remote node. ● If set to **Incoming**, your Prestige will not place a call to this remote node. ● If set to **Outgoing**, your Prestige will drop any incoming calls from this remote node. Several other fields in this menu depend on this parameter. For example, in order to enable **Callback**, the **Call Direction** must be **Both**.	**Both** **Incoming** **Outgoing**
Incoming: Rem Node Login Name	Enter the login name that this remote node will use when it calls your Prestige. The login name in this field combined with the Rem Node Password will be used to authenticate this node.	
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, a **N/A** appears in the field. This is the Calling Line ID (the telephone number of the calling party) of this remote node. 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, a **N/A** appears in the field. This field determines whether or not your Prestige will call back after receiving a call from this remote node. 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** **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.	
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. Options for this field are: ● **CHAP/PAP** - Your Prestige will accept either CHAP or PAP when requested by this remote node. ● **CHAP** - accept CHAP only. ● **PAP** - accept PAP only.	**CHAP/PAP** **CHAP** **PAP**
Outgoing:	Pri(mary) Sec(ondary) Phone Numbers	Your Prestige always calls this remote node using the Primary Phone number first for a dial-up line. If the Primary Phone number is busy or does not answer, your Prestige will dial the Secondary Phone number if available. 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.	
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.	

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
Transfer Type	This field specifies the type of connection between the Prestige and this remote node. When set to **Leased**, the **Allocated Budget** and **Period** do not apply.	**64k/ Leased**
Period (hr)	This field sets the time interval to reset the above outgoing call budget control.	
Schedules	Apply up to 4 schedules sets, separated by commas to your remote node here. Please see later for a full discussion on schedules.	
Nailed-up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. See below for more details.	**Yes/No**
Toll Period	This is the basic unit of time for charging purposes, e.g., 25 cents every 3 minutes – then 3 minutes is the toll period. The minimum toll period is 5 seconds.	
Session Option: Edit Filter Sets	Use the space bar to toggle this field to **Yes** and press [Enter] to open Menu 11.5 to edit the filter sets. See the Remote Node Filter section for more details.	Default= **No**
Session Option: 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). *This option only applies when the Prestige initiates the call.*	Default=300 secs for an unconfigured remote node. 0 secs means the remote node will never be automatically disconnected.
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.		

5.1.3 Outgoing Authentication Protocol

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

successful authentication, please make sure that you specify the correct authentication protocol when connecting to such an implementation.

5.1.4 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.

Due to the fragmentation/reconstruction overhead associated with MP, you may not get a linear increase in throughput when a link is added.

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

5.1.5 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.

The configuration of bandwidth on demand focuses on the Base Transmission Rate (BTR) and the Maximum Transmission Rate (MTR). The relationship between BTR and MTR are shown below:

Table 5-2 BTR v MTR for BOD

BTR & MTR Setting	No. of channel(s) used	Max No. of channel(s) used	Bandwidth on demand
BTR = 64, MTR = 64	1	1	Off
BTR = 64, MTR = 128	1	2	On
BTR = 128, MTR = 128	2	2	Off

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

The **Target Utility** specifies the line utilization range at which you want the Prestige to add or subtract bandwidth. The range is 30 to 64 Kbps (kilobits per second). The parameters are separated by a '-'. For example, '30-60' means the add threshold is 30 Kbps and subtract threshold is 60 Kbps. The Prestige performs bandwidth on demand only if it initiates the call. Addition and subtraction are based on the value set in the **BOD Calculation** field. If this field is set to **Transmit or Receive**, then traffic in either direction will be included 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 to make this determination.

If, after making the call to bring up a second channel, the second channel does not succeed in joining the Multilink Protocol bundle (because the remote device does not recognize the second call as coming from the same device), the Prestige will hang up the second call and continue with the first channel alone.

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

5.1.6 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 below.

```
                    Menu 11.2 - Remote Node PPP Options

                  Encapsulation= Standard PPP
                  Compression= No

                  Multiple Link Options:
                    BOD Calculation= Transmit or Receive
                 Base Trans Rate(Kbps)= 64
                 Max Trans Rate(Kbps)= 64
                    Target Utility(Kbps)= 32-48
                    Add Persist(sec)= 5
                    Subtract Persist(sec)= 5



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

Figure 5-3 Menu 11.2 - Remote Node PPP Options

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

Table 5-3 Remote Node PPP Options Menu Fields

Field	Description	Option
Encapsulation	Select the CISCO PPP only when this remote node is a Cisco machine; otherwise, select the Standard PPP.	**Standard PPP** **CISCO PPP**
Compression	Turn on/off Stac Compression. The default for this field is **Off**.	**On/Off** (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**
Base Trans Rate	Select the base data transfer rate for this remote node in Kbps. There are two choices for this field- **64** where only one channel is used or **128** where two channels are used as soon as a packet triggers a call	**64/128**
Max Trans Rate	Enter the maximum data transfer rate allowed for this remote node. This parameter is in kilobits per second. There are two choices for this field- same as above.	**64/128**
Target Utility (Kbps)	Enter the two thresholds separated by a [-] for subtracting and adding the second port.	Default=10-20
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.		

5.1.7 Remote Node Filter

Use **Menu 11.5 – Remote Node Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige and to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by comma, e.g., 1, 5, 9, 12, in each **filter** field.

Note that spaces are accepted in this field. For more information on defining the filters, *see Chapter 9:* . The Prestige comes with a prepackaged filter set, NetBIOS_WAN, that blocks NetBIOS packets (call protocol filter = 1). You can include this in the call filter sets if you wish to prevent NetBIOS packets from triggering calls to a remote node.

```
                    Menu 11.5 - Remote Node Filter

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




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

Figure 5-4 Menu 11.5 – Remote Node Filter

Chapter 6: Remote Node TCP/IP Configuration

This chapter shows you how to configure the TCP/IP parameters of a remote node. A typical LAN-to-LAN application is to use your Prestige to connect a branch office to the headquarters, as depicted in the following diagram.

6.1 LAN-to-LAN Application

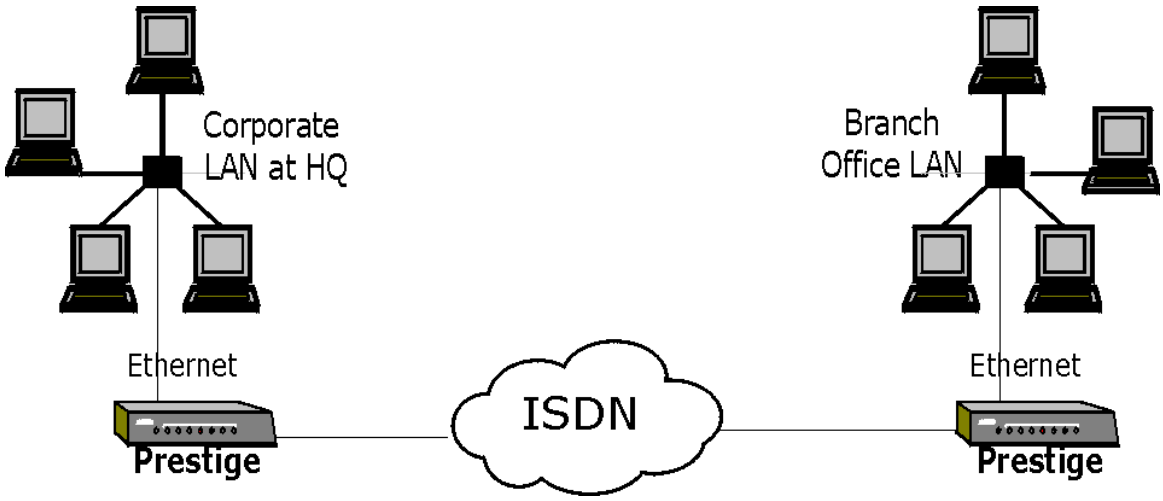


Figure 6-1 TCP/IP LAN-to-LAN Application

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.

6.1.1 Remote Node Setup

Follow the procedure below to configure the TCP/IP parameters in Menu 11 - Remote Node Profile.

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

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

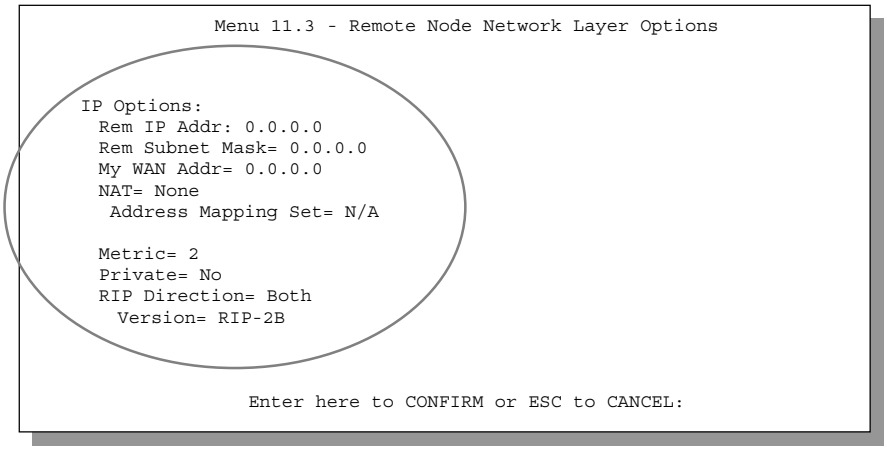


Figure 6-2 Menu 11.3- Remote Node TCP/IP Options

The following diagram explains the Sample IP Addresses to help you to understand the field of **My Wan Addr** in Menu 11.3.

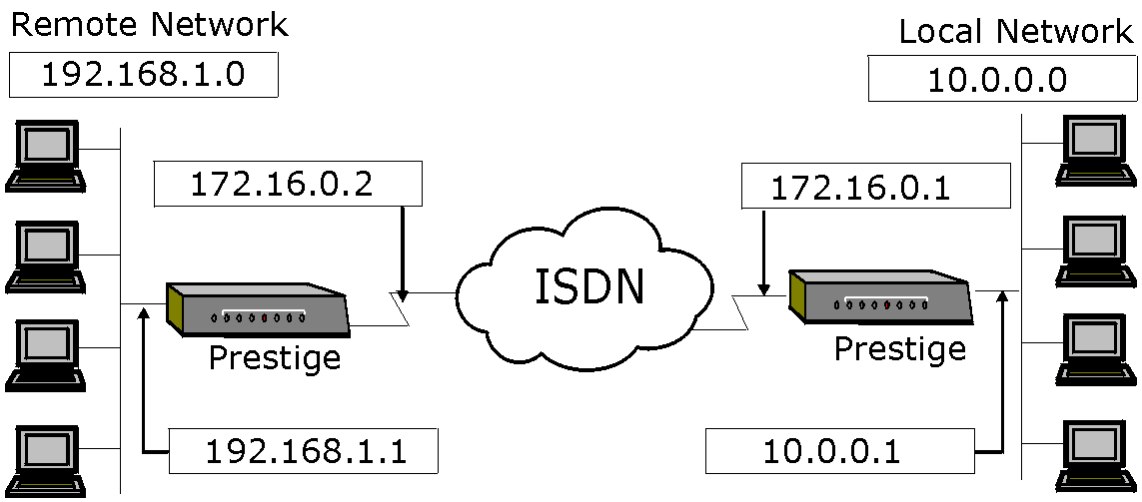


Figure 6-3 Sample IP Addresses for a TCPI/IP LAN-to-LAN Connection

To configure the TCP/IP parameters of a remote node, first configure the two fields in **Menu 11 – Remote Node Profile**, as shown in the table below.

Table 6-1 TCP/IP related fields in Remote Node Profile

Field	Description	Option
Rem IP Address	Enter the IP address of the remote gateway in **Menu 11.1 - Remote Node Profile**. You must fill in either the remote Prestige WAN IP address or the remote Prestige LAN IP address. This depends on the remote router's WAN IP i.e., for the (remote) Prestige, the **My WAN Addr** settings in **Menu 4**. For example (*see Figure 6-3*), if the remote WAN IP is set to 172.16.0.2 (the remote router's WAN IP), then you should enter 172.16.0.2 in the **Rem IP Address** field. If the remote WAN IP is 0.0.0.0, then enter 192.168.1.1(the remote router's LAN IP) in the **Rem IP Address** field).	
Edit IP	Press the space bar to select **Yes** and press **Enter** to go to **Menu 11.3 - Remote Node Network Layer Options** menu.	**Yes** (**Yes/No**)

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

Table 6-2 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. Note that this is the address assigned to your local Prestige WAN, not the remote router. If the remote router is a Prestige, then this entry determines the local Prestige **Rem IP Address** in menu 11.1 (*see Table 6-1*).	
NAT Address Mapping Set=	Choose from None, Full Feature or SUA Only. *See Chapter 4:* for a full discussion of this new feature. A NAT Server Set is a list of LAN side servers mapped to external ports (similar to the old SUA menu 15.1 before). You may enter any server set number up to 10, but the first one is used foe SUA only.	
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	**1** to **15**
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.	**Yes/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.

6.1.2 Static Route Setup

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

Each remote node specifies only the network to which the gateway is directly connected, and the Prestige has no knowledge of the networks beyond. For instance, the Prestige knows about network N2 in the following diagram through remote node Router 1. However, the Prestige is unable to route a packet to network N3 because it doesn't know that there is a route through remote node Router 2. The static routes are for you to tell the Prestige about the networks beyond the remote nodes.

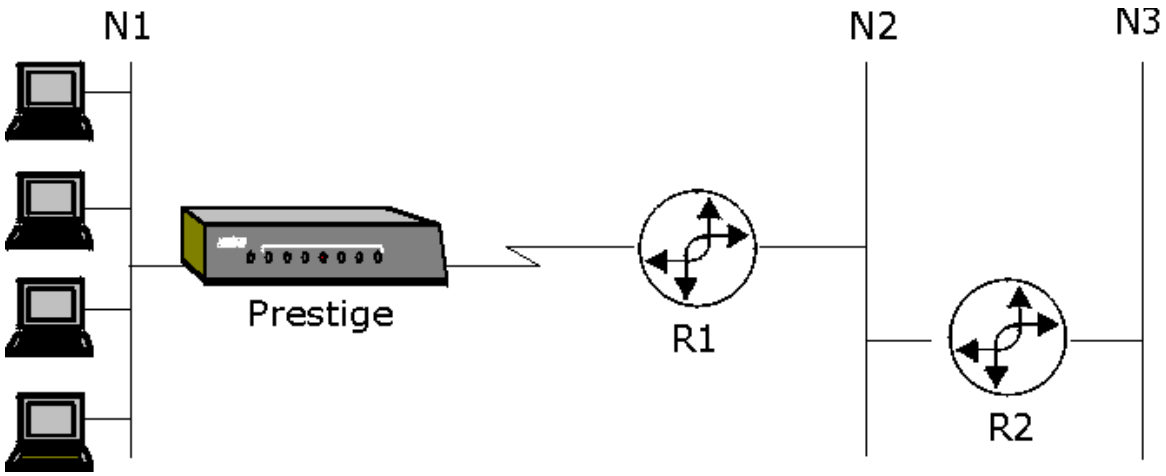


Figure 6-4 Example of Static Routing Topology

To configure an IP static route, use Menu 12, Static Route Setup, as displayed below.

From Menu 12, select one of the available IP static routes to open Menu 12.1 - IP Static Route Setup, as shown below.

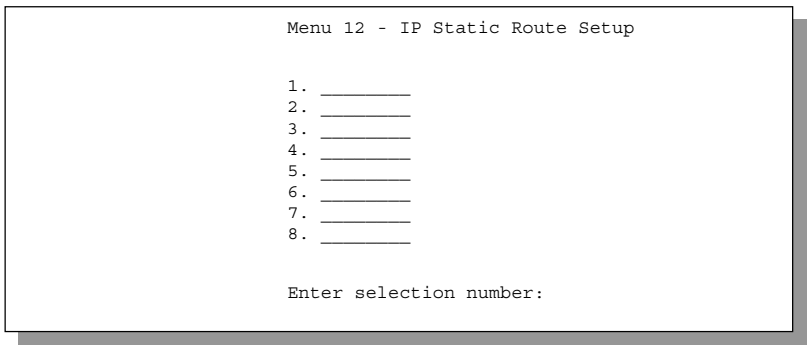


Figure 6-5 Menu 12.1 - IP Static Route Setup

Choosing a static route to edit produces the following screen.

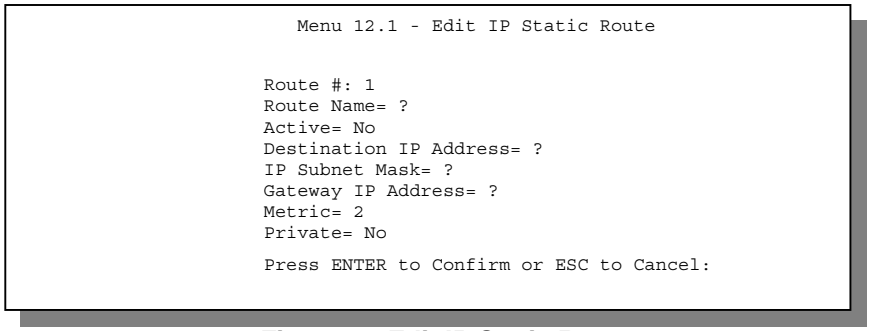


Figure 6-6Edit IP Static Route

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

Table 6-3 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.
Private	Same meaning as those in the Remote Node Setup.

Chapter 7:
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 the table below.

Table 7-1 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 calls 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.

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.

7.1 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. 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

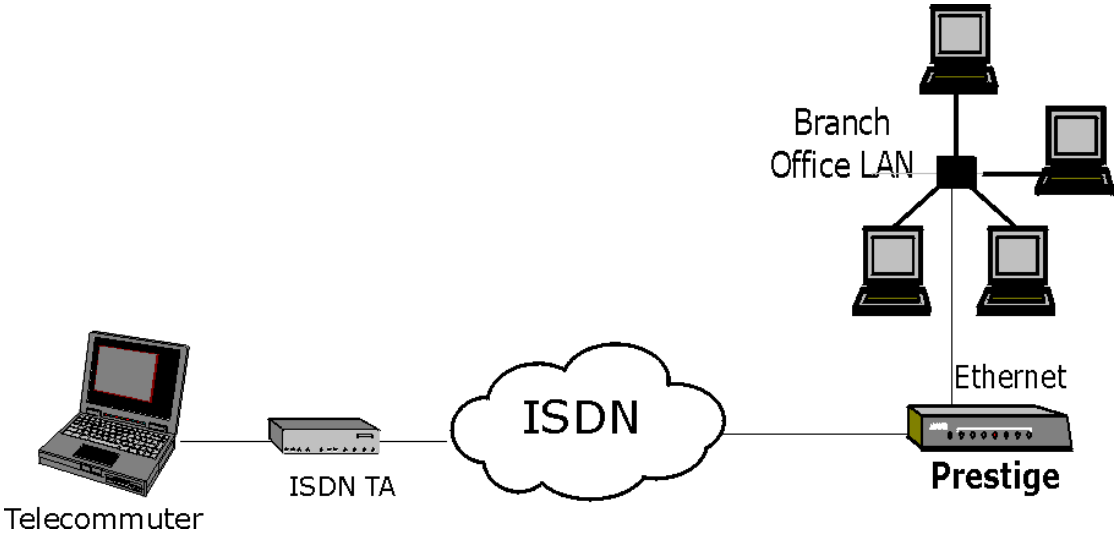


Figure 7-1 Example of Telecommuting LAN-to-LAN Server Application

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:*).

An example of your Prestige being used as a LAN-to-LAN server is shown next.

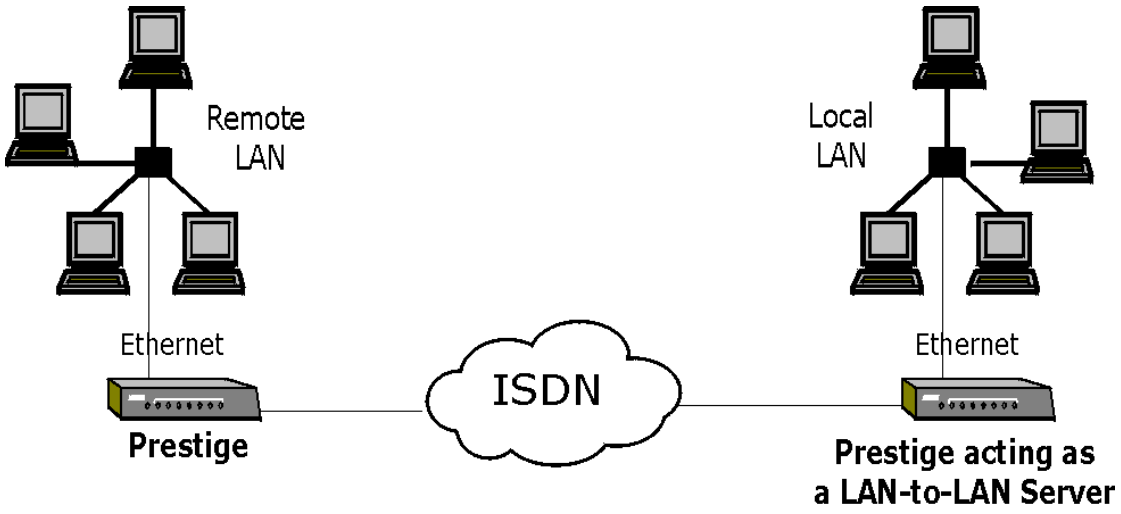


Figure 7-2 Example of a LAN-to-LAN Server Application

7.2 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.

7.2.1 CLID Callback Support For Dial-In Users

CLID is an authentication method to identify a dial-in user. CLID callback is used as an ISDN toll saving feature because the call can be disconnected immediately without picking up the phone. In previous ZyNOS versions, only the remote node was capable of CLID callback because there was no outgoing information for dial-in users. 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, please fill in the **O/G Login** and **O/G Password** fields. You must also fill in these fields when a dial-in user to whom we are calling back requests authentication. In this ZyNOS version, the CLID outgoing information will be set in Menu 13, and dial-in users can avail of callback.

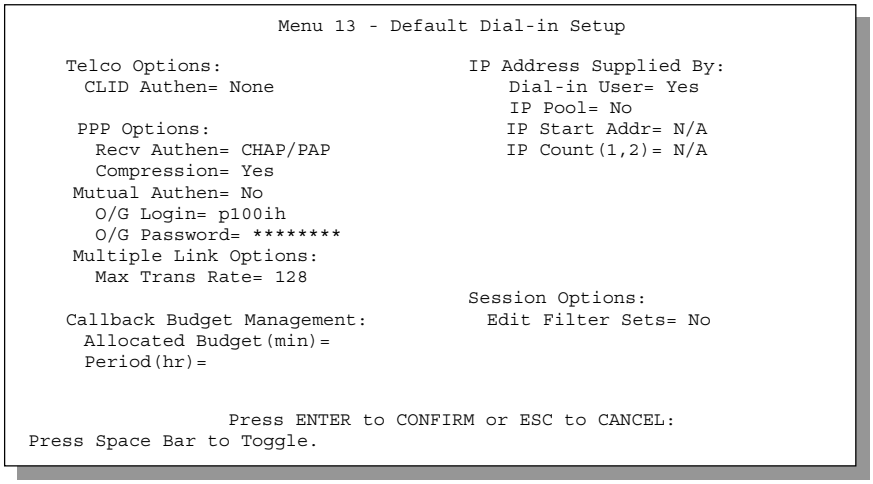


Figure 7-3 Menu 13 – Default Dial-in Setup

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.

The table below describes and contains information on how to configure each parameter in Menu 13 – Default Dial-in Setup.

Table 7-2 Default Dial-in Setup Fields

Field	Description	Options
Telco Options: CLID Authen	This field sets the CLID authentication parameter for all incoming calls. There are three options for this field: ● **None** - No CLID is required. ● **Required** – CLID must be available, or the Prestige will not answer the call. ● **Preferred** - If the CLID is available then CLID will be used; otherwise, authentication is performed in PPP negotiation.	**None** **Required** **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: ● **CHAP/PAP** - Your Prestige will try CHAP first, but PAP will be used if CHAP is not available. ● **CHAP** – Use CHAP only. ● **PAP** – Use PAP only. ● **None** – Your Prestige tries to acquire CHAP/PAP first, but no authentication is required if CHAP/PAP is not available.	**CHAP/PAP** **CHAP** **PAP** **None**
Compression	Turn on/off Stac Compression. The default for this field is **Off**.	**On** **Off**
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**
O/G Login	Enter in the login name to be used to respond to the peer's authentication request.	
O/G Password	Enter in the outgoing password to be used to respond to the peer's authentication request.	
Multiple Link Options:		
Max Trans Rate	Enter the maximum data transfer rate between your Prestige and the remote dial-in user. **64** - At most, one B channel is used. **128** - A maximum of two channels can be used. When the Prestige calls back to the remote dial-in user, the maximum data transfer rate is always **64.**	**64/128**
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**
Period (hr)	This field sets the time interval to reset the above callback budget control.	

IP Address Supplied By:		
Dial-in User	If set to **Yes**, the Prestige will allow a remote host to specify its own IP address. 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**) **Yes/No**
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** (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. The IP pool contains contiguous IP addresses and this field specifies the first one in the pool.	
IP Count (1,2)	In this field, enter the number (**1** or **2**,) 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**
Session Options: Edit Filter Sets	Press **Yes,** then [Enter] to edit the filter sets. Keep in mind that the filter set(s) will only apply to remote dial-in users but not the remote nodes. Note that spaces and [-] symbol, are accepted in this field. For more information on customizing your filter sets, *see Chapter 8 - Filter Configuration*. The default is blank, i.e., no filters.	Default = **No**
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.		

7.2.2 Default Dial-in Filter

Use **Menu 13.1 – Default Dial-in Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between all dial-in users and your Prestige. Note that the filter set(s) only applies to the dial-in users

but not the remote nodes. You can specify up to 4 filter sets separated by comma, e.g., 1, 5, 9, 12, in each **filter** field. The default is no filters.

Spaces are accepted in this field. For more information on defining the filters, *see Chapter 9:* .

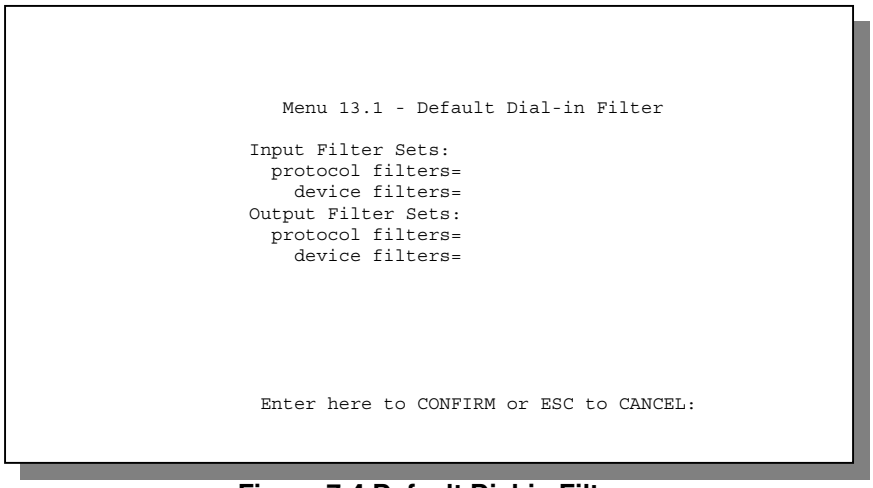


Figure 7-4 Default Dial-in Filter

7.3 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 the next figure.

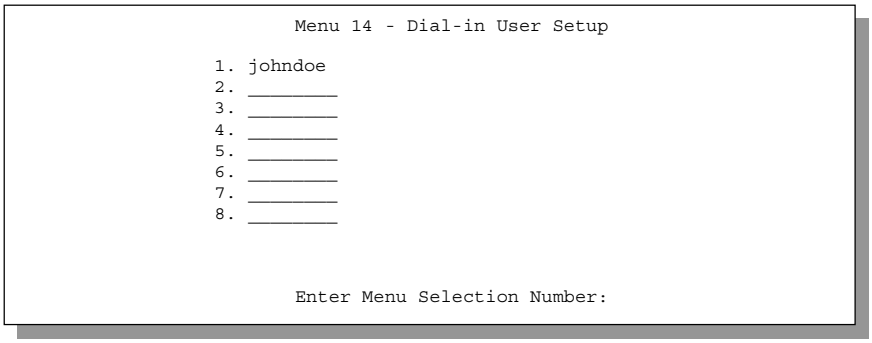


Figure 7-5 Menu 14 - Dial-in User Setup

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

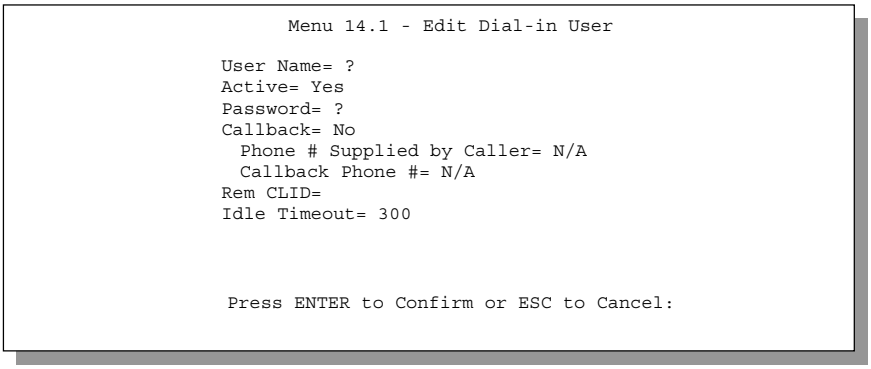


Figure 7-6 Edit Dial-in User

The following table provides instructions on how to fill in the Edit Dial-In User fields.

Table 7-3 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** **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). ● **No** - The default is no callback. ● **Optional** - The user can choose to disable callback. ● **Mandatory** - The user can not disable callback.	Default=**No** **No** **Optional** **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. ● If the setting is **Yes**, the user can specify and send to the Prestige the callback number of his/her choice. ● The default is **No**, i.e., your Prestige always calls back to the fixed callback number.	Default=**No** **Yes** **No**
Callback Phone #	If **Phone # Supplied by Caller** is **No**, 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 7-4 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 will 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. 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.		

7.3.1 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.

7.3.2 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 is charged to the company instead of the employees, and your accounting department can avoid the hassles of accountability and reimbursement.

Chapter 8: Advanced Phone Services

The Prestige 100 and 100IH support a comprehensive set of advanced calling features known as Supplemental Services. European and North American ISDN Supplemental Services may vary and have different naming conventions that can be generalized as follows. Please check with your telephone company for the services it offers.

Table 8-1 Supplemental Services by region

Europe	North America
Call Waiting Call Hold Call Retrieve	Additional Call Offering (ACO) — Call Waiting, Call Hold, Call Retrieve
Three Party Conference	Flexible Calling (FC) — Conference, Drop, Transfer
Call Forwarding — Call Forwarding Busy (CFB) Call Forwarding Unconditional (CFU) Call Forwarding No Reply (CFNR)	Call Forwarding
	Reminder Ring

Table 8-2 Supplemental Services by switch type.

Feature:	US[9]	DSS-1	1TR6
Call Waiting/Call Hold/Call Retrieve	✓	✓	×
Three Way Calling (Conference/Transfer/Drop)	✓	✓	×
Call Forwarding	✓	✓	×
Reminder Ring	✓	×	×

8.1 Getting Started

8.1.1 Things you need to know before you start using Supplemental Services.

- In North America, Additional Call Offering (ACO) is required on your ISDN line in order to use the Call Waiting feature. Flexible Calling is required on your ISDN line in order to use the Three-Way-Calling or Call Transfer features. You need to check with your telephone company to confirm if these services are available to you and if so, are there any additional charges for them.
- In some cases, your telephone company may only enable these features on your first directory (phone) number. In this case, you may want to request that the features be enabled on your second directory number as well.

8.2 Setting Up Supplemental Phone Service

All Supplemental Phone Services are enabled by default except for Call Waiting, which is disabled by default but can be enabled in **Menu 2.1- ISDN Advanced Setup.** The **Calling Line Indication**, or Caller ID, also in this menu decides whether the other party can see your number when you call. If set to **Enable** (default), the Prestige sends the caller ID and the party you call can see your number, otherwise if set to **Disable**, the caller ID is blocked.

8.3 The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same

[9] "US" refers to a broad range of switch types supported in the USA.

effect. However, using the flash key is preferred since the timing is much more precise. With manually tapping, if the duration is too long, it may be interpreted as hanging up by the Prestige.

8.4 Call Waiting

ISDN Call Waiting allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

By default call waiting is enabled on both telephone ports (except France where the default is disabled), but can be toggled on either port from **Menu 2.1**.

8.4.1 How to use call waiting

The Call Waiting feature on your ISDN line works in exactly the same way as it does on a regular analog line (which almost everyone is familiar with). To put the current call on hold and answer the incoming call, press the flash key after hearing a call waiting indicator tone.

Dropping current call to switch to incoming/holding call.

After hearing a Call Waiting indicator tone, simply hang up the telephone and wait for the telephone to ring before answering the incoming/holding call.

Notes: An incoming caller receives a busy signal if

- You have two calls active (one active and one on hold, or both active using Three Way Calling) already.
- You are dialing a number on the B-Channel the incoming caller is attempting to reach, but have not yet established a connection.

8.5 Three Way Calling

Three Way Calling allows you to add a third party to an existing call. This service must be subscribed from your telephone company.

8.5.1 How To Use Three Way Calling

If you wish to call someone and conference him/her in with an existing call:

- Press the flash key to put the existing call on hold and receive a dial tone.
- Dial the third party's telephone number.
- When you are ready to conference the calls together, press the flash key again to establish a Three Way Conference Call.

Note: If you wish to cancel your attempt to establish the conference call because the third party's line in busy or if they don't answer, simply hang-up the telephone and pick it back up after it starts ringing to return to the first caller.

To drop the last call added to the three-way-call:

Simply press the flash key. The last call that was added to the conference is dropped.

To drop yourself from the conference call:

If you hang up your telephone during a three-way-call and the two other callers remain on the line, the ISDN network will do an implicit transfer to directly connect the two remaining callers together.

8.6 Call Transfer

Call Transfer allows you to transfer an active call to a third party. This service must be subscribed from your telephone company.

8.6.1 How To Use Call Transfer

Transferring an active call to a third party:

- Once you have an active call (Caller A), press the flash key to put Caller A on hold and receive a dial tone.
- Dial the third party's telephone number (Caller B).
- When you are ready to conference the two calls together, press the flash key to establish a Three-Way-Conference call.
- Hang up the telephone. The ISDN network does an implicit transfer to directly connect Caller A with Caller B.

8.6.2 To Do A Blind Transfer:

- Once you have an active call (Caller A), press the flash key to put the existing call on hold and receive a dial tone.
- Dial the third party's telephone number (Caller B).
- Before Caller B picks up the call, you can transfer the call by pressing the flash key. The call is automatically transferred.

8.7 Call Forwarding

Call forwarding means the switch will ring another number at a place where you will be when someone dials your directory number.

There are two methods to activate call forwarding. The first is exactly the same as on an analog line, i.e., you pick up the handset and dial the access code assigned by your telephone company and the number that you want the calls forwarded. Check with your telephone company for this access code.

The second is with the "phone flash" commands where you pick up the handset and press the flash key before dialing the following:

Table 8-3 Phone Flash Commands

Command	Meaning
*20*forward-number#	Activate CFB (Call Forwarding Busy)
*21*forward-number#	Activate CFU (Call Forwarding Unconditional)
*22*forward-number#	Activate CFNR (Call Forwarding No Reply)
#20#	Deactivate CFB
#21#	Deactivate CFU
#22#	Deactivate CFNR

Either method should work fine, and you can use whichever one you are most comfortable with.

8.8 Reminder Ring

The Prestige sends a single short ring to your telephone every time a call has been forwarded (US switches only).

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 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 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 9-2 Outgoing Packet* Filtering Process.

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

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

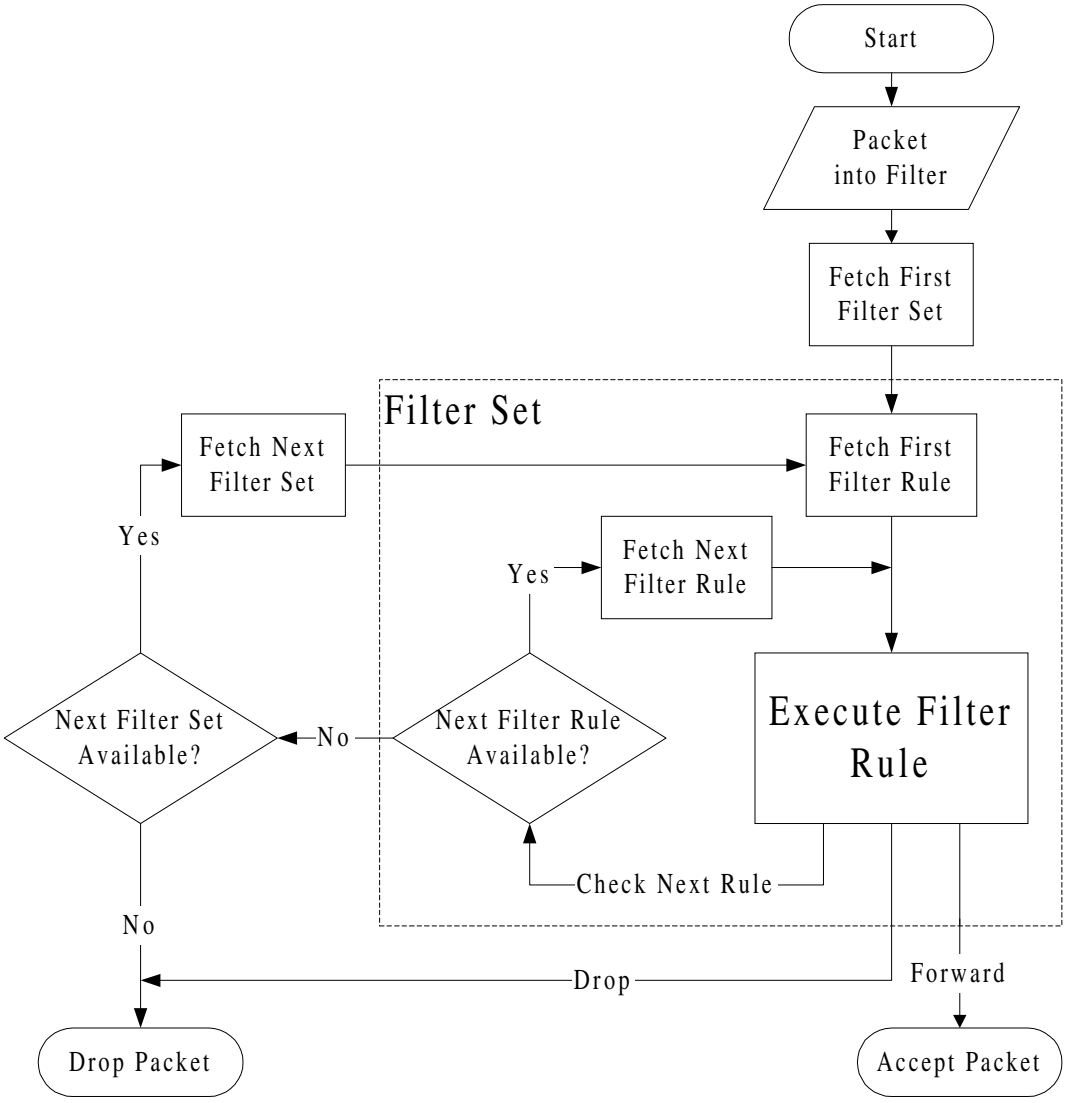


Figure 9-1 Filter Rule Process

You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

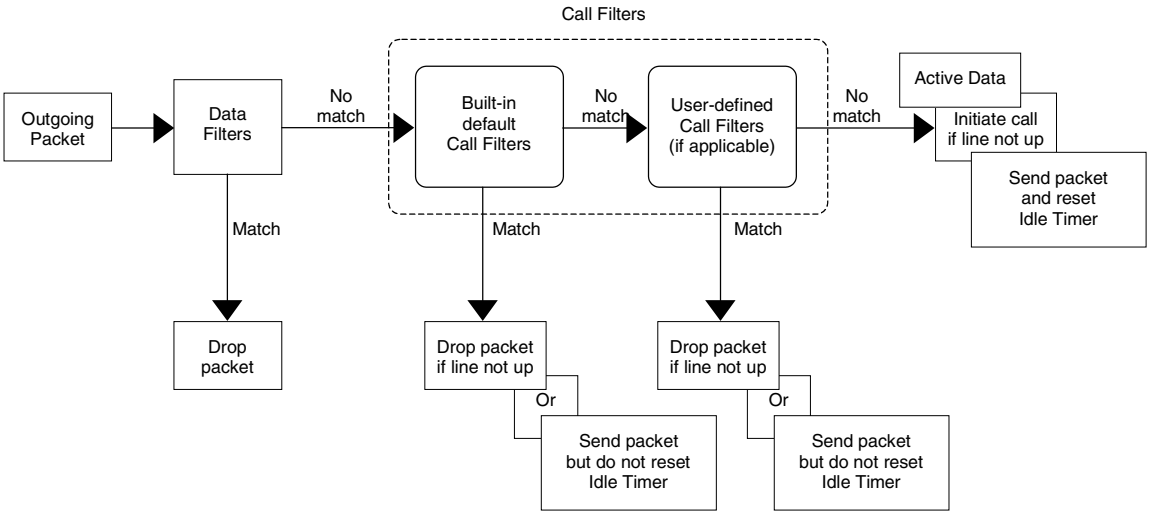


Figure 9-2 Outgoing Packet Filtering Process

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           NetBIOS_WAN               7           _________________
2           NetBIOS_LAN               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 9-3 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 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137                     N D N
2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138                     N D N
3 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139                     N D N
4 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137                    N D N
5 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138                    N D N
6 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139                    N D F


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

Figure 9-4 Menu 21.1 - Filter Rules Summary

```
                    Menu 21.2 - Filter Rules Summary

# A Type                        Filter Rules                        M m n
- - ---- ------------------------------------------- --------- - - -
1 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53              N D F
2 Y
3 Y
4 Y
5 Y
6 Y

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

Figure 9-5 Menu 21.2 - 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. [N] means the filter rule is inactive.

Abbreviations	Description	Display
Type	Refers to the type of filter rule. This shows GEN for generic, IP for TCP/IP	[GEN] for Generic [IP] for TCP/IP
Filter Rules	The filter rule parameters will be displayed here (see below).	
M	Refers to More. [Y] means an action can not yet be taken as there are more rules to check, which are concatenated with the present rule to form a rule chain. When the rule chain is complete an action can be taken. [N] means you can now specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked. If More is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**	[Y] means there are more rules to check. [N] means there are no more rules to check.
m	Refers to **Action Matched**. [F] means to forward the packet immediately and skip checking the remaining rules.	[F] means to forward the packet. [D] means to drop the packet. [N] means check the next rule.
n	Refers to **Action Not Matched.** [F] means to forward the packet immediately and skip checking the remaining rules.	[F] means to forward the packet. [D] means to drop the packet. [N] means check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

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

Table 9-2 Abbreviations Used If Filter Type Is IP

Abbreviation	Description
Pr	Protocol
SA	Source Address

Abbreviation	Description
SP	Source Port number
DA	Destination Address
DP	Destination Port number

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

Table 9-3 Abbreviations Used If Filter Type Is GEN

Abbreviation	Description
Off	Offset
Len	Length

Refer to the next section for information on configuring the filter rules.

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 two types of filter rules: **TCP/IP** 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 Filter Types and NAT

The network layer filters are collectively called protocol filters. When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the Prestige applies the protocol filters to the “native” IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic, or device, filters are applied to the raw packets that appear on the wire. They are applied at the point when the Prestige is receiving and sending the packets; i.e. the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

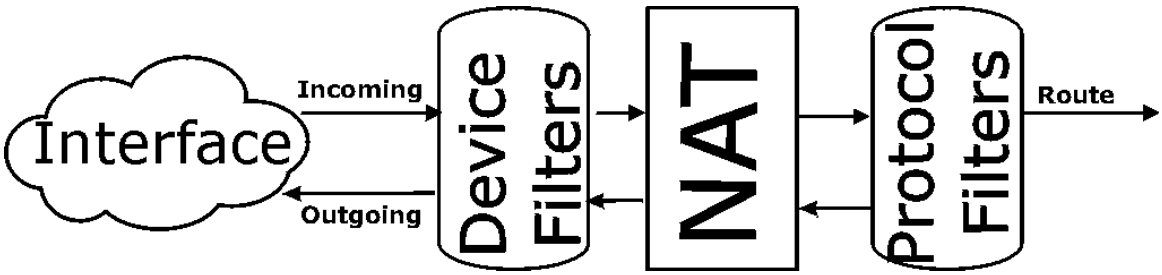


Figure 9-6 Protocol and Device Filter Sets

To speed up filtering, all rules in a filter set must be of the same class, i.e., protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filters field or vice versa, the Prestige will warn you and will not allow you to save.

9.3.2 TCP/IP Filter Rule

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

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

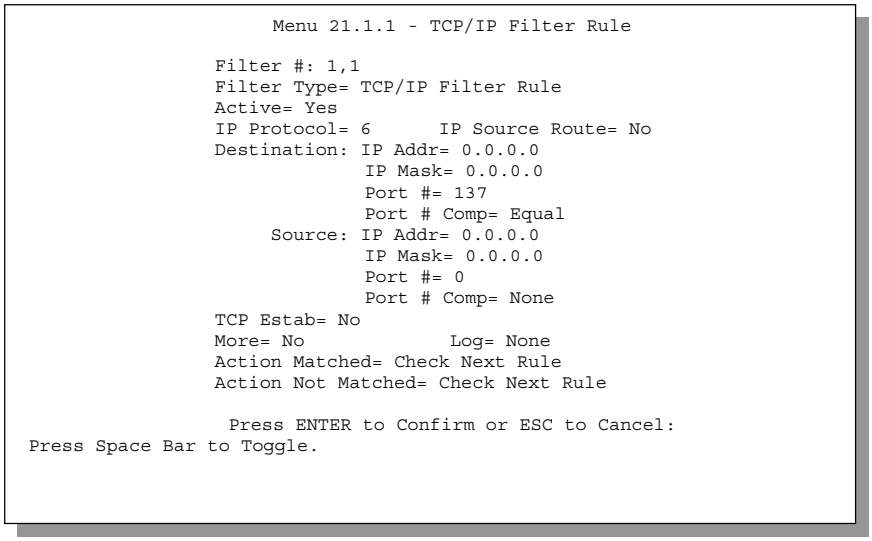


Figure 9-7 Menu 21.1.1 - TCP/IP Filter Rule

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

Table 9-4 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	0-65535

Field	Description	Option
	filter. The range of this field is 0 to 65535. This field is a don't-care if it is 0.	
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 #.	**None/Less/Greater/ Equal/Not Equal**
TCP Estab	This field is applicable only when IP Protocol field is 6, TCP. If yes, the rule matches only established TCP connections; else the rule matches all TCP packets.	**Yes/No**
More	If yes, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields. If More is **Yes**, then Action Matched and Action Not Matched will be **N/A**.	**Yes / N/A**
Log	Select the logging option from the following: ● **None** – No packets will be logged. ● **Action Matched** - Only packets that match the rule parameters will be logged. ● **Action Not Matched** - Only packets that do not match the rule parameters will be logged. ● **Both** – All packets will be logged.	**None** **Action Matched** **Action Not Matched** **Both**
Action Matched	Select the action for a matching packet.	**Check Next Rule** **Forward** **Drop**
Action Not Matched	**Select the action for a packet not matching the rule.**	**Check Next Rule**

Field	Description	Option
		Forward **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.		

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

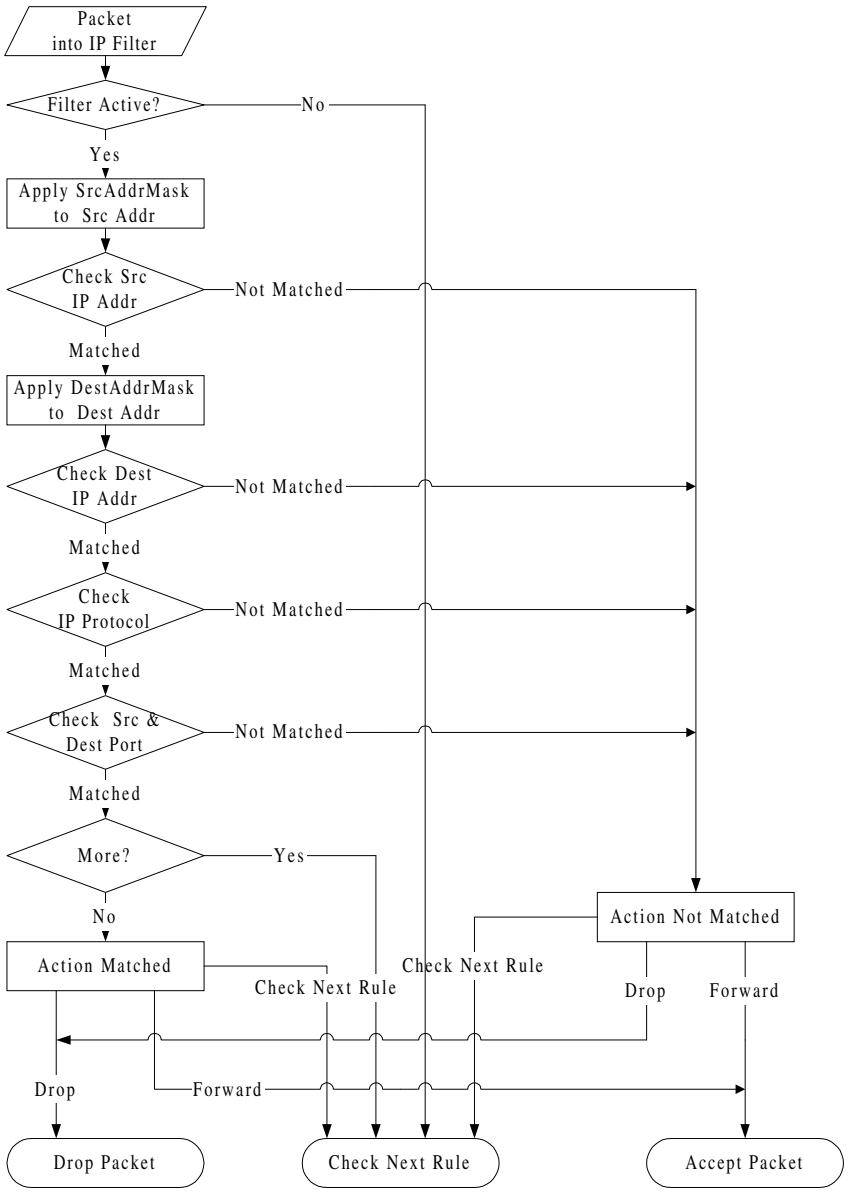


Figure 9-8 Executing an IP Filter

9.3.3 Generic Filter Rule

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

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

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

```
                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 9-9 Menu 21.1.2 - Generic Filter Rule

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

Table 9-5 Generic Filter Rule Menu Fields

Field	Description	Option
Filter #	This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third rule of that set.	
Filter Type	Use the space bar to toggle between both types of rules. Parameters displayed below each type will be different.	**Generic Filter Rule/ TCP/IP Filter Rule**
Active	Select **Yes** to turn on the filter rule.	**Yes/No**
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.	Default = 0
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.	Default = 0
Mask	Enter the mask (in Hexadecimal) to apply to the data portion before comparison.	
Value	Enter the value (in Hexadecimal) to compare with the data portion.	
More	If yes, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields. If More is **Yes**, then Action Matched and Action Not Matched will be **N/A**.	**Yes / N/A**
Log	Select the logging option from the following: ● **None** – No packets will be logged. ● **Action Matched** - Only packets that match the rule parameters will be logged. ● **Action Not Matched** - Only packets that do not match the rule parameters will be logged. ● **Both** – All packets will be logged.	**None** **Action Matched** **Action Not Matched** **Both**
Action Matched	Select the action for a matching packet.	**Check Next Rule** **Forward** **Drop**

Field	Description	Option
Action Not Matched	**Select the action for a packet not matching the rule.**	**Check Next Rule** **Forward** **Drop**
Once you have completed filling in Menu 21.1.2 - 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.		

9.4 Applying a Filter and Factory Defaults

This section shows you where to apply the filter(s) after you design it (them). Two sets of factory default filter rules have been configured in Menu 21 to prevent NetBIOS traffic from triggering calls (see Figure 8-7 Menu 21 - Filter Set Configuration).

9.4.1 Ethernet traffic

You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to Menu 3.1 (shown below) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11.

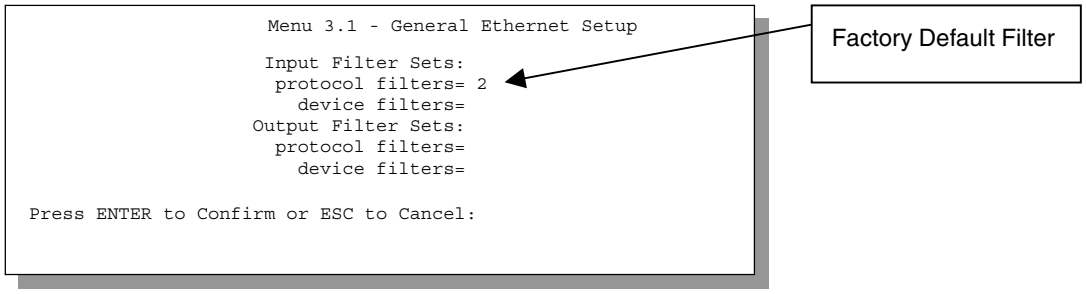


Figure 9-10 Filtering Ethernet traffic

9.4.2 Remote Node Filters

Go to Menu 11.5 (shown below) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas. The factory default filter set, NetBIOS_WAN, is inserted in ***protocol filters*** field under ***Call Filter Sets*** in Menu 11.5 to block local NetBIOS traffic from triggering calls to the remote node.

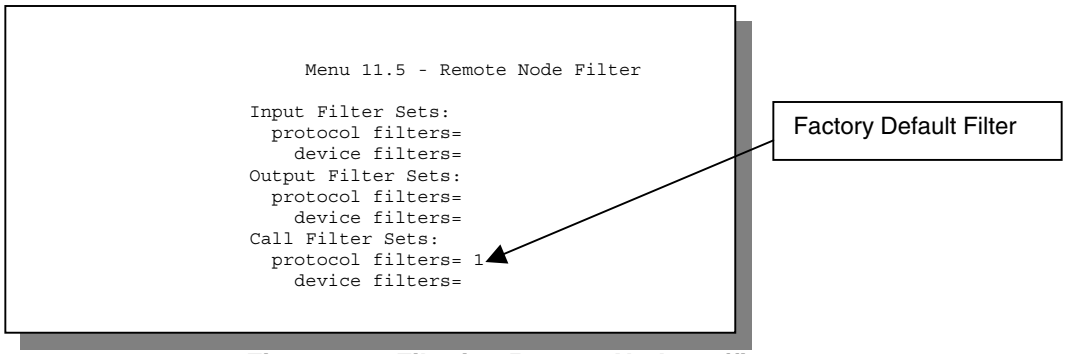


Figure 9-11 Filtering Remote Node traffic

9.4.3 Default Dial-in Filter

Use **Menu 13.1 – Default Dial-in Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between all dial-in users and your Prestige. Note that these filter set(s) only apply to the dial-in users but not the remote nodes. You can specify up to 4 filter sets separated by comma, e.g., 1, 5, 9, 12, in each **filter** field. The default is no filters.

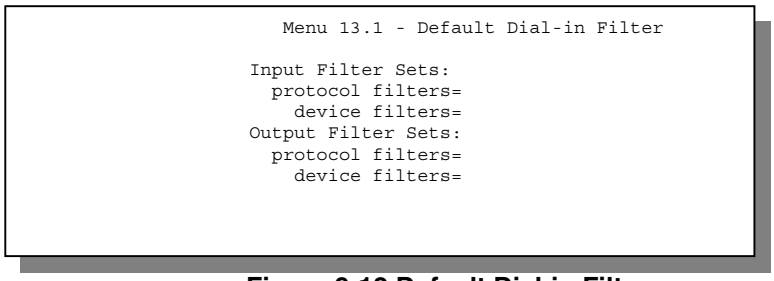


Figure 9-12 Default Dial-in Filter

Chapter 10: Telnet Configuration and Capabilities

10.1 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 below.

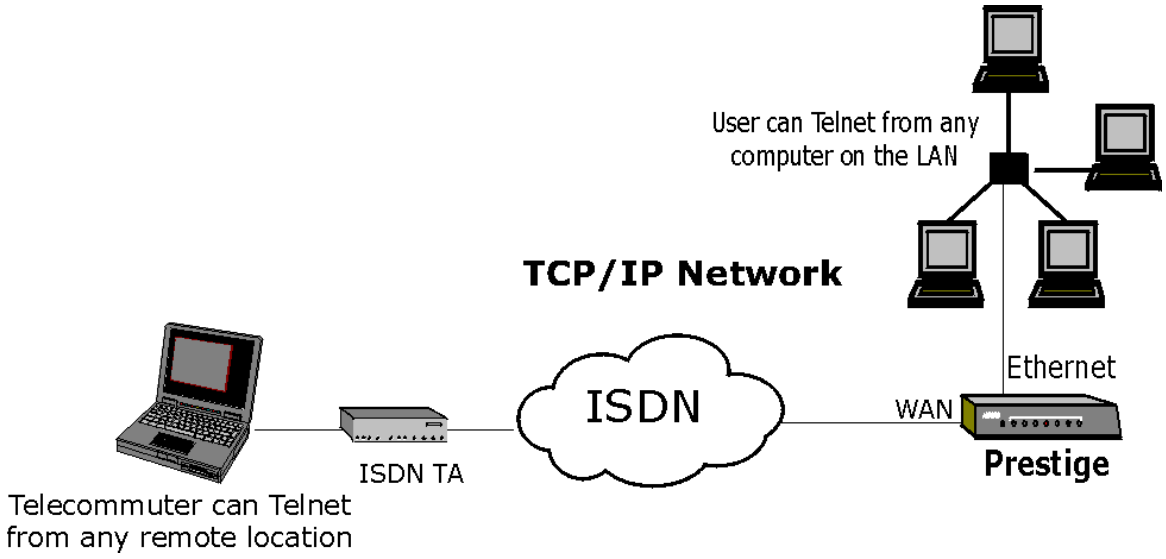


Figure 10-1 Telnet Configuration on a TCP/IP Network

10.2 Telnet Under NAT

When NAT is enabled and an inside telnet 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.

10.3 Telnet Capabilities

10.3.1 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.

10.3.2 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 11: 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 below.

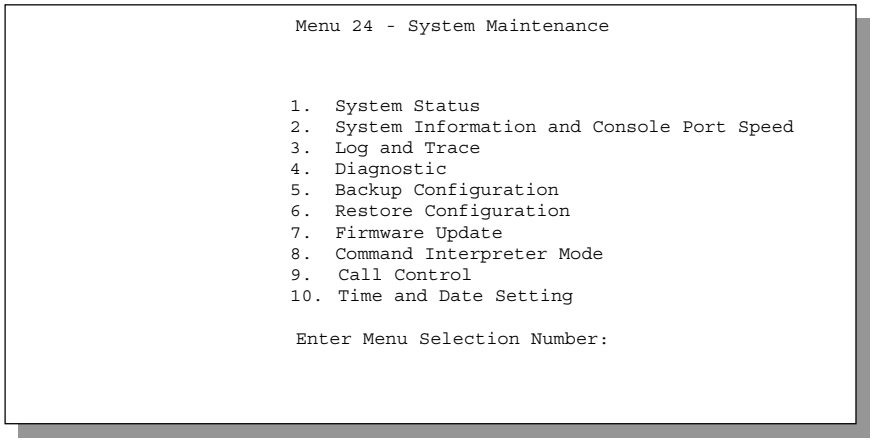


Figure 11-1 Menu 24 - System Maintenance

11.1 System Status

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

To get to the System Status, select number **24** to go to **Menu 24 - System Maintenance.** From this menu, select number **1, System Status.** There are five commands in **Menu 24.1 - System Maintenance - Status**. Entering **1** disconnects the current B1 channel call; **2** disconnects the current B2 channel call, **3** resets the counters, **4** drops both B1 and B2 and **ESC** takes you back to the previous screen.

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

```
                    Menu 24.1 -- System Maintenance - Status

Chan   Link     Type        TXPkts  RXPkts   Errors      CLU      ALU       Up Time
 --    Down     0Kbps            0       0        0       0%       0%       0:00:00
 --    Down     0Kbps            0       0        0       0%       0%       0:00:00
   Total Outcall Time:         0:00:00

   Ethernet:                          WAN:
     Status: 10M/Half Duplex            Chan 1 IP Addr:
     TX Pkts: 230                       Chan 2 IP Addr:
     RX Pkts: 0                         Chan 1 CLID:
     Collisions: 0                      Chan 2 CLID:

   LAN Packet Which Triggered Last Call:

                                Press Command:
    COMMANDS: 1-Drop B1  2-Drop B2  3-Reset Counters  4-Drop All    ESC-Exit
```

Figure 11-2 Menu 24.1 - System Maintenance – Status

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

Table 11-1 System Maintenance - Status Menu Fields

Field	Description
Chan	Shows statistics for **B1** and **B2** channels respectively. This is the information displayed for each channel:
Link	Shows the name of the remote node or the user the channel is currently connected to or the status of the channel (Down, Idle, Calling or Answering).

Field	Description
Type	The current connecting speed (**56K** or **64K**).
TXPkt	The number of transmitted packets on this channel.
RXPkt	The number of received packets on this channel.
Error	The number of error packets on this channel.
CLU	(Current Line Utilization) percentage of current bandwidth used on this channel
ALU	(Average Line Utilization) a 5-second moving average of channel usage for this channel.
Up Time	Time this channel has been connected to the current remote node.
Total Outgoing call Time	Shows the total outgoing call time for both **B1** and **B2** channels since the system has been powered up.
Ethernet	
Status	Shows the current status of the Ethernet link.
TX Pkt	The number of transmitted packets to LAN.
RX Pkt	The number of received packets from LAN.
Collision	Number of collisions.
WAN	
Chan 1 IP Addr	Refers to the IP address of the Prestige on Channel 1.
Chan 2 IP Addr	Refers to the IP address of the Prestige on Channel 2.
Chan 1 CLID	Shows the Caller ID of the peer on Channel 1.
Chan 2 CLID	Shows the Caller ID of the peer on Channel 2.

Field	Description
LAN Packet Which Triggered Last Call	Shows the first 48 octets of the LAN packet that triggered the last outgoing call.

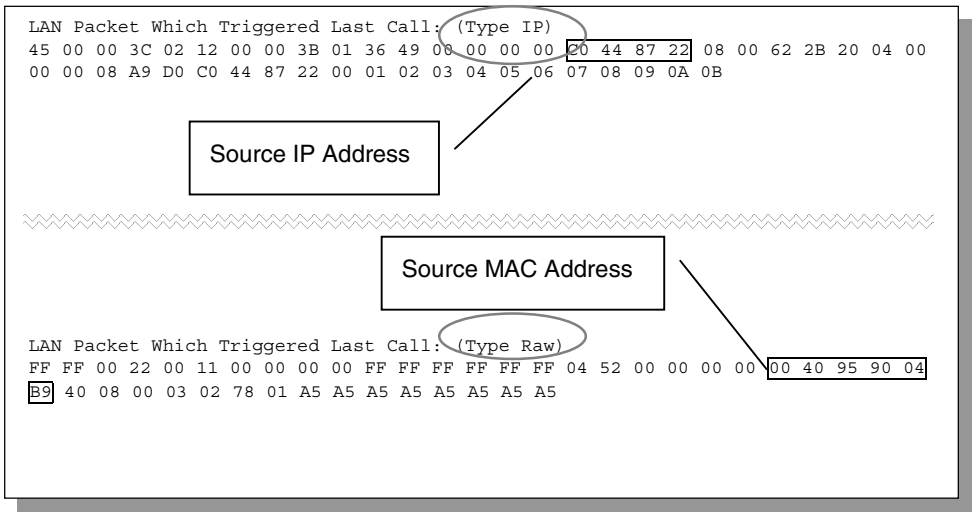


Figure 11-3 LAN Packet That Triggered Last Call

The figure above 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.

11.1.1 System Information

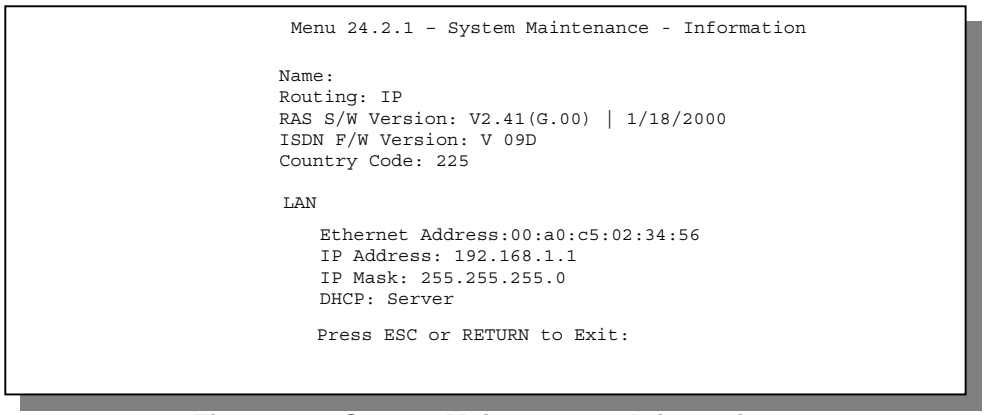


Figure 11-4 System Maintenance - Information

Table 11-2 Fields in System Maintenance

Field	Description
Name	displays the system name of your Prestige. This information can be modified in **Menu 1 - General Setup**.
Routing	refers to the routing protocol used.
RAS S/W Version	refers to the version of the ZyNOS software.
ISDN F/W Version	refers to the version of the ISDN firmware.
Country Code	refers to the one byte country code value (in decimal notation),
Ethernet Address	refers to the Ethernet MAC (Media Access Control) of your Prestige.
IP Address	This is the IP address of the Prestige in dotted decimal notation.
IP Mask	This shows the subnet mask of the Prestige.
DHCP	This field shows the DHCP setting (**None, Relay** or **Server**) of the Prestige.

11.1.2 Console Port Speed

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

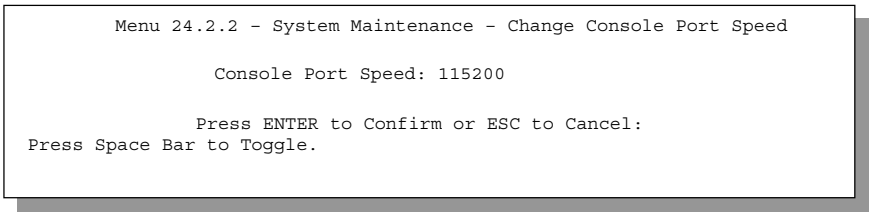


Figure 11-5 Menu 24.2.2 – System Maintenance – Change Console Port Speed

11.2 Log and Trace

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

11.2.1 Viewing Error Log

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

Step 1. 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 the error log, you will have the option to clear it.

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

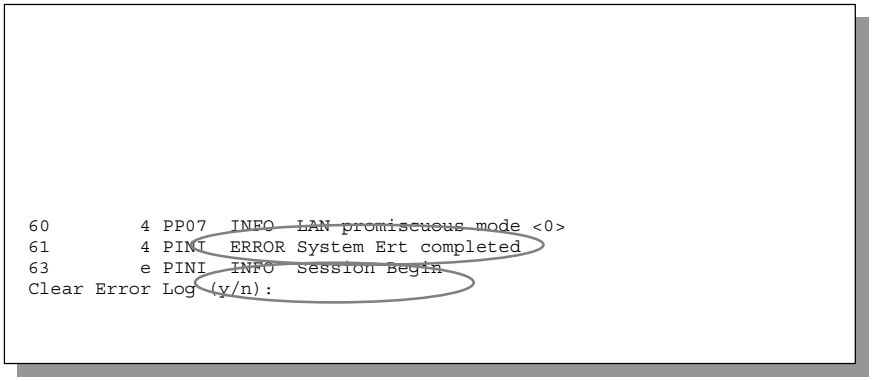


Figure 11-6 Examples of Error and Information Messages

11.2.2 Syslog And Accounting

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

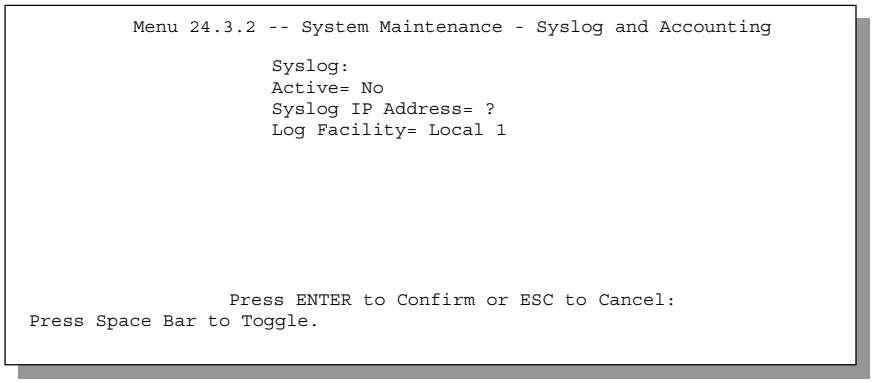


Figure 11-7 Menu 24.3.2 - System Maintenance - Syslog and Accounting

You need to configure the following 3 parameters described in the table below to activate syslog.

Table 11-3 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:

1. 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
```

2. Error Information Messages:

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

3. Session Information Messages:

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

11.3 Diagnostic

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

```
              Menu 24.4 - System Maintenance - Diagnostic

ISDN                                  System
  1.  Hang Up B1 Call                   21. Reboot System
  2.  Hang Up B2 Call                   22. Command Mode
  3.  Reset ISDN
  4.   ISDN Connection Test
  5.   Manual Call

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

                     Enter Menu Selection Number:

                Manual Call Remote Node= N/A
                Host IP Address= N/A
```

Figure 11-8 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 describes the diagnostic tests available in Menu 24.4 for your Prestige and the connections.

Table 11-4 System Maintenance Menu Diagnostic

Field	Description
Hang Up B1 Call	This command hangs up the B1 channel. This is only applicable if the B1 channel is currently in use.
Hang Up B2 Call	This tool hangs up the B2 channel. This is only applicable if the B2 channel is currently in use.
Reset ISDN	This command re-initializes the ISDN link to the telephone company.
ISDN Connection Test	You can test to see if your ISDN line is working properly by using this option. This command triggers the Prestige to perform a loop-back test to check the functionality of the ISDN line. If the test is not successful, note the error message that you receive and consult your network administrator.
Manual Call	This provides a way for you to place a call to a remote node manually. This tests the connectivity to that remote node. When you use this command, the screen displays what is happening during the call setup and protocol negotiation. Below is an example of a successful connection.
Internet Setup Test	This test checks to see if your Internet access configuration has been done correctly. When this option is chosen, the Prestige places a manual call to the ISP remote node. If everything is working properly, you will receive an appropriate response. Otherwise, note the error message and consult your network administrator.
Ping Host	This diagnostic test pings the host, which determines the functionality of the TCP/IP protocol on both systems and the links in between.
Reboot System	This option reboots the Prestige.
Command Mode	This option allows you to enter the command mode. This mode allows you to diagnose and test your Prestige using a specified set of commands.

The following figure shows an example of a successful connection after selecting option **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<64000> chan<2> prot<1>
LCP up
CHAP send response
CHAP login to remote OK!
IPCP negotiation started
IPCP up
```

Figure 11-9 Display for a Successful Manual Call

This figure shows an 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 11-10 Display for a Failed Authentication

11.4 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.

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

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

Figure 11-11 Backup Configuration

Step 2. Press “Y” to indicate that you want to continue.

The following procedure is for the HyperTerminal program. The procedure for other serial communications programs should be similar. Run the HyperTerminal program.

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

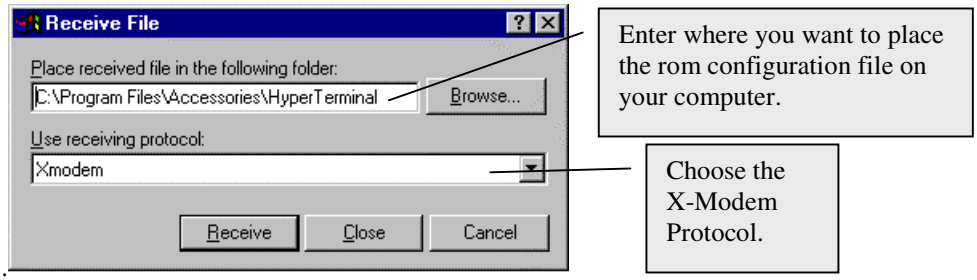


Figure 11-12 HyperTerminal Screen

Step 2. Enter a path and name for the rom configuration file on your computer (*see section 2.7 Filename conventions*) and make sure you choose the X-Modem Protocol. Then press “Receive”.

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

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

Figure 11-13 Successful Backup

11.5 Restore Configuration

Select 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.

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

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

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

Figure 11-14 Restore Configuration

Step 2. Press “Y” to indicate that you want to continue.

The following procedure is for the HyperTerminal program. The procedure for other serial communications programs should be similar. Run the HyperTerminal program.

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

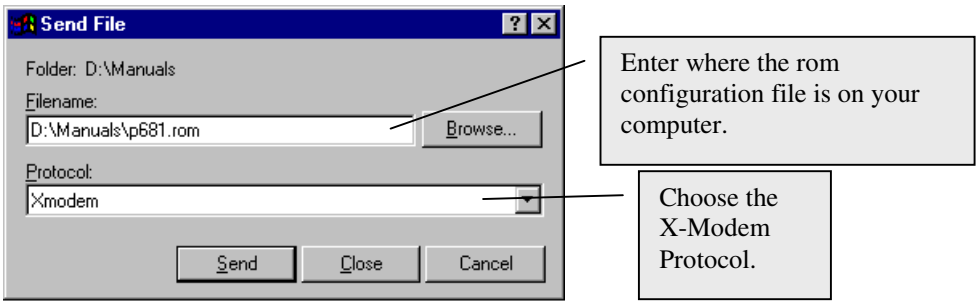


Figure 11-15 HyperTerminal Screen

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

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

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

Figure 11-16 Successful Restoration

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

11.6 Firmware Upload

Menu 24.7 -- System Maintenance - Upload Firmware allows you to upgrade the firmware and the configuration file via the console port. The firmware and configuration file may also be uploaded via FTP. There are 2 components in the system: the router firmware and the configuration file, as shown in the next figure. Restoring the configuration as in menu 24.6 copies your (customized) backup configuration from your computer to the Prestige. Note you must be able to access the SMT to do this. Uploading the configuration file via menu 24.7.2 on the other hand rewrites all configuration data, as well as system-related data, the error log and the trace log. If you forget your password for instance (see section 2.7.1) you will need to use menu 24.7.2 as you can use this method in debug mode. However, your customized settings will be reset to the default values (including your password being reset to 1234, the Prestige default password).

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


                  Enter Menu Selection Number:
```

Figure 11-17 Menu 24.7 - System Maintenance - Upload Firmware

11.6.1 Upload Router Firmware

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

Step 1. Enter "`atur`" after the "`Enter Debug Mode`" message.

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

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

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

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

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




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

Figure 11-18 Menu 24.7.1 - Uploading Router Firmware

11.6.2 Uploading Router Configuration File

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

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

Step 1. Enter "atur3" after the "Enter Debug Mode" message.

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

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

If you replace the current configuration file with the default configuration file, i.e., P100IH.rom, you will lose all configurations that you had before and the speed of the console port will be reset to the default of 9600 bps with 8 data bit, no parity and 1 stop bit (8n1). You will need to change your serial communications software to the default before you can connect to the Prestige again. The password will be reset to the default of 1234, also.

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

To upload router configuration file:
1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atur3" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
   Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart the
   router.

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

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

Figure 11-19 Menu 24.7.2 - System Maintenance - Upload Router Configuration File

11.6.3 TFTP Transfer

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

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

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

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

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

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

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

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

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer.

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

Example Using the Walusoft TFTP client

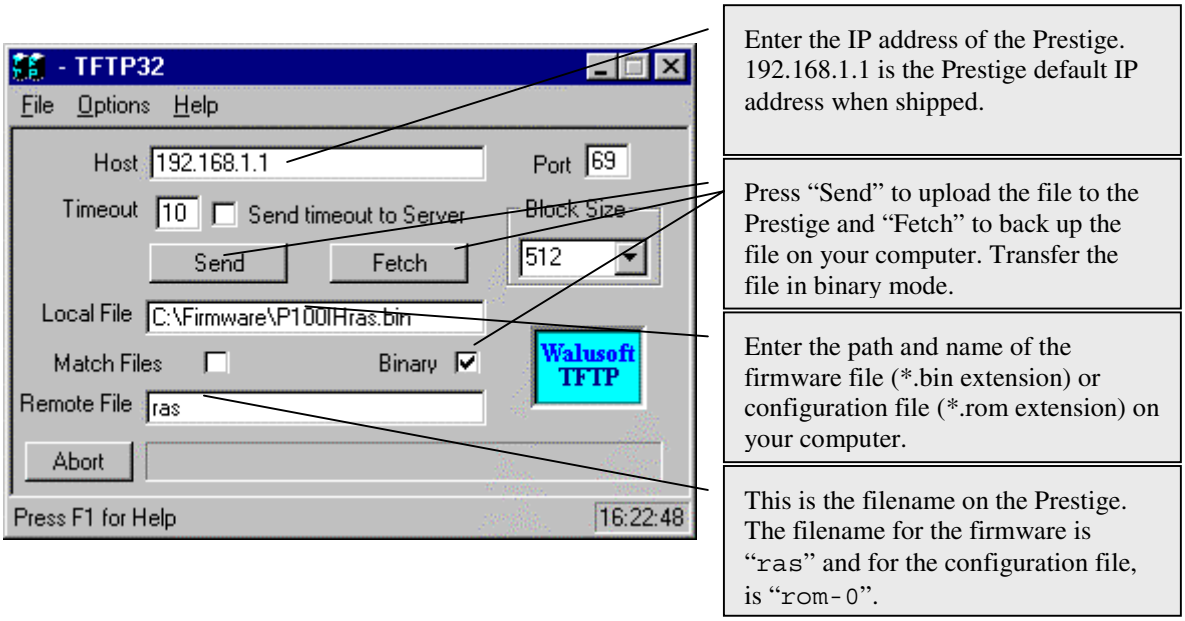


Figure 11-20 TFTP Example

11.6.4 Boot module commands

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

```
======= Debug Command Listing =======
ATHE      print help
ATGO      boot system
ATUR      upload RAS code
ATUR3     upload RAS configuration file
ATBAx     change baud rate. 1:38.4,2:19.2,3:9.6,4:57.6,5:115.2
ATTD      download configuration to PC
ATSE      display seed for password generation
ATSH      display Revision and etc
```

Figure 11-21 Boot module commands

11.7 Command Interpreter Mode

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

```
                        Enter Menu Selection Number: 8


Copyright (c) 1994 - 2000 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            device          ether
isdn            ip              ppp             hdap
```

Figure 11-22 Command mode

11.8 Call Control

The Prestige provides four call control functions: call control parameters, blacklist, budget management and call history.

Call control parameters allow you to set a dial out time limit, the number of times a number should be called before it is added to the blacklist and the interim between calls.

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.

Call history chronicles preceding incoming and outgoing calls.

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 the table below.

```
Menu 24.9 - System Maintenance - Call Control


   1.  Call Control Parameters
   2.  Blacklist
   3.  Budget Management
   4.  Call History




        Enter Menu Selection Number:
```

Figure 11-23 Menu 24.9 - System Maintenance - Call Control

11.8.1 Call Control Parameters

```
                Menu 24.9.1 - Call Control Parameters


                Dialer Timeout:
                 Digital Call(sec)= 30


               Retry Counter= 0
               Retry Interval(sec)= N/A
Press ENTER to confirm or ESC to Cancel:
```

Figure 11-24 Call Control Parameters

Table 11-5 Call Control Parameters Fields

Field	Description
Dialer Timeout: Digital Call (sec)	The Prestige will timeout if it can not set up an outgoing digital call within the timeout value. The default is **30**.
Retry Counter	How many times a busy or 'no answer' telephone number is retried before it is put on the blacklist. The default is **0** and the blacklist control is not enabled.
Retry Interval (sec)	Elapsed time after a call fails before another call may be retried. This applies before a telephone number is blacklisted.

11.8.2 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 11-25 Menu 24.9.2 – Blacklist

11.8.3 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. --------                         ---                             ---
6. --------                         ---                             ---
7. --------                         ---                             ---
8. --------                         ---                             ---
9. Dial-in User                  No Budget                       No Budget









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

Figure 11-26 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.

11.8.4 Call History

This is the fourth option in Call Control and relays information about past incoming and outgoing calls.

```
                          Menu 24.9.4 - Call History

Phone Number     Dir      Rate        #call        Max         Min         Total
   1.
   2.
   3.
   4.
   5.
   6.
   7.
   8.
   9.
  10.

Enter Entry to Delete(0 to exit):
```

Figure 11-27 Call History

Table 11-6 Call History Fields

Field	Description
Phone Number	This is the telephone number of past incoming and outgoing calls.
Dir	This shows whether the call was incoming or outgoing.
Rate	This is the transfer rate of the call.
#call	This is the number of calls made to or received from that telephone number.
Max	This is the length of time of the longest telephone call.
Min	This is the length of time of the shortest telephone call.
Total	This is the total length of time of all the telephone calls to/from that telephone number.

11.9 Time and Date Setting

This feature allows the Prestige to connect to a time server to synchronize its system clock when it is booting. There is no Real Time Chip (RTC) chip in the Prestige, so this software mechanism allows you to

get the current time and date from an external server when you power up your Prestige. Go to **Menu 24.10** to update the time and date settings of your Prestige.

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


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

            Current Time:                          00 : 00 : 00
            New Time (hh:mm:ss):                   1  : 3  : 16

            Current Date:                          1970 - 01 - 01
            New Date (mm-dd-yyyy):                 2000  -  1 - 4

            Time Zone= GMT+0800




                     Press ENTER to Confirm or ESC to Cancel:

    Press Space Bar to Toggle.
```

Figure 11-28 System Maintenance – Time and Date Setting

Table 11-7 Time and Date Setting Fields

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

Chapter 12: Call Scheduling

The call scheduling feature allows the Prestige to manage a remote node and dictate when a remote node should be called and for how long. This feature is just like the scheduler in a video recorder (record the program you want in a specified time). You can apply up to 4 schedule sets in **Menu 11.1 - Remote Node Profile.** You configure each schedule in **Menu 26 - Schedule Setup**.

```
          Copyright (c) 1994 - 1999 ZyXEL Communications Corp.

                            Prestige 100IH Main Menu

    Getting Started                       Advanced Management
      1. General Setup                        21. Filter Set Configuration
      2. ISDN Setup
      3. Ethernet Setup                       23. System Password
      4. Internet Access Setup                24. System Maintenance

    Advanced Applications                     26. Schedule Setup
      11. Remote Node Setup
      12. Static Routing Setup
      13. Default Dial-in Setup
      14. Dial-in User Setup
      15. NAT Setup                           99. Exit

                         Enter Menu Selection Number:
```

Figure 12-1 Schedule Setup

```
                          Menu 26 - Schedule Setup

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

                  Enter Schedule Set Number to Configure=
                  Edit Name=
                 Press ENTER to CONFIRM or ESC to CANCEL:
```

Figure 12-2 Schedule Setup

As we can have multiple sets that are applied in turn, lowered numbered sets take precedence over higher numbered sets in case of conflict. For example, if we apply sets 1,2,3,4 in a remote node, then set 1 will

take precedence over set 2, 3 and 4 as it is applied first. Set 2 will take precedence over set 3 and 4, and so on.

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

To delete a schedule set, enter the set number and press the [Space Bar] (or delete) in the Edit Name field to delete the set name.

To setup a schedule set select the schedule set you want to setup from **Menu 26** (no. 1-12) and press [Enter] to see **Menu 26.1 - Schedule Set Setup** as shown next.

```
                Menu 26.1 - Schedule Set Setup

Active= Yes
Start Date (mm/dd/yyyy) = 1990-1-1
How Often= Once
Once:
  Date (mm/dd/yyyy) = 1990-1-2
Weekdays:
  Sunday= N/A
  Monday= N/A
  Tuesday= N/A
  Wednesday= N/A
  Thursday= N/A
  Friday= N/A
  Saturday= N/A
Start Time (hh : mm) = 10 : 20
Duration (hh : mm) = 01 :00
Action= Forced On
Press ENTER to Confirm or ESC to Cancel:
```

Figure 12-3 Schedule Set Setup

The action for a remote node configured with a schedule set is **Forced On**, **Forced Down, Enable Dial-On-Demand**, or **Disable Dial-On-Demand**. **Forced On** means that the connection is maintained whether or not there is a demand call on the line and persist for the time period specified in the **Duration** field. **Forced Down** means that the connection is blocked whether or not there is a demand call on the line. **Enable Dial-On-Demand** means that this schedule permits a demand call on the line. **Disable Dial-On-Demand** means that this schedule prevents a demand call on the line. If a connection has been already established, it will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

Table 12-1 Schedule Set Setup Fields

Field	Description	Option
Active	Press the [Space Bar] to toggle between **Yes** and **No**. Choose **Yes** and press [Enter] to activate the set.	**Yes** **No**
Start Date	Enter the start date that you wish the set to take effect in year-month-date format. Valid dates are from January 1, 1990 to February 5, 2036.	
How Often	Should this schedule set recur weekly or be used just once only? Press the [Space Bar] to toggle between **Once** and **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A.** When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses.	**Once** **Weekly**
Once: Date	If you selected **Once** in the **How Often** field above, then enter the date the set should activate here in year-month-date format.	
Weekday: Day	If you selected Weekly in the **How Often** field above, then select the day(s) the set should activate (and recur) by going to that day(s) and pressing the [Space Bar], then [Enter] to select Yes.	**Yes** **No** **N/A**
Start Time	Enter the start time that you wish the set to take effect in hour : minute format.	
Duration	Enter the maximum duration allowed in hour : minute format for this scheduled connection per call.	
Action	Press the [Space Bar] to toggle between these options. Choose one and then press [Enter].	**Forced On, Forced Down, Enable Dial-On-Demand, or Disable Dial-On-Demand.**

12.1.1 Applying A Schedule Set

After you've configured your schedule sets, you must apply them to the desired remote node(s). Enter **11** from the **Main Menu** and then enter the target remote node index. You can apply up to 4 schedule sets, separated by commas, for one remote node.

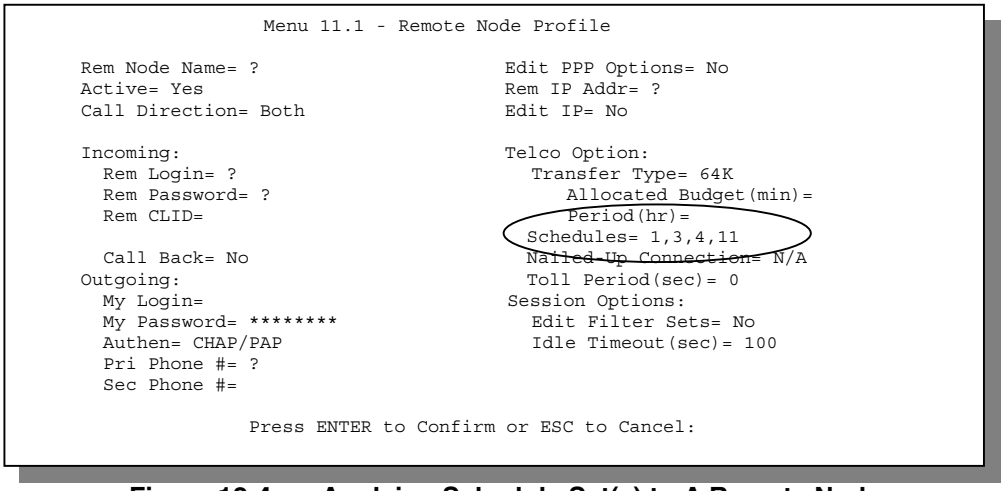


Figure 12-4 Applying Schedule Set(s) to A Remote Node

Chapter 13: 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.

13.1 Problems Starting Up the Prestige

Table 13-1 Troubleshooting the Start-Up of your Prestige

<table>
<tr><th>Problem</th><th colspan="2">Corrective Action</th></tr>
<tr><td>None of the LEDs are on when you power on the Prestige</td><td colspan="2">Check the connection between the AC adapter and the Prestige.
If the error persists, you may have a hardware problem. In this case you should contact technical support.</td></tr>
<tr><td rowspan="4">Cannot access the Prestige via the console port.</td><td colspan="2">1.Check to see if the Prestige is connected to your computer’s serial port.</td></tr>
<tr><td rowspan="3">2. Check to see if the communications program is configured correctly. The communications software should be configured as follows:</td><td>VT100 terminal emulation</td></tr>
<tr><td>9600 bps</td></tr>
<tr><td>No parity, 8 Data bits, 1 Stop bit.</td></tr>
</table>

13.2 Problems With the ISDN Line

Table 13-2 Troubleshooting the ISDN Line

Problem	Corrective Action
The ISDN initialization failed. This problem occurs when you attempt to save the parameters entered in menu 2, but receive the message, 'Save successful, but Failed to initialize ISDN; Press ESC to exit'.	Check the error log (in **menu 24.3.1**), you should see a log entry for the ISDN initialization failure in the format, '**ISDN init failed. code<n>...**'. Note the code number, n.
	If the code is **1**, the ISDN link is not up. This problem could be either the ISDN line is not properly connected to the Prestige or the ISDN line is not activated. Verify that the ISDN line is connected to the Prestige and to the wall telephone jack.
	If the code is **3**, this indicates a general failure. Verify the provisioning information for your switch by contacting your telephone company.
The ISDN loopback test failed.	If the ISDN initialization is successful, then the loopback test should also work. Verify the telephone numbers that have been entered in **menu 2**. The loopback test dials the number entered in the 2nd Phone # field (except for switch types with only one phone number). If you need to dial a prefix (e.g., '9') to get an outside line, then you have to enter the telephone number as '95551212' or '914085551212'. If it is an internal line, you may only need to enter the last four or five digits (according to your internal dialing plan), e.g., 51212.

13.3 Problems with the LAN Interface

Table 13-3 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.

13.4 Problems Connecting to a Remote Node or ISP

Table 13-4 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.

13.5 Problems for Remote User to Dial-in

Table 13-5 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.
	Is the remote dial-in user negotiating using IPX? The P100IH does not support IPX.

Appendix
Acronyms and Abbreviations

AUI	Attachment Unit Interface
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
DOVBS	Data Over Voice Bearer Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DTE	Data Terminal Equipment
IANA	Internet Assigned Number Authority
IP	Internet protocol
IPCP	(PPP) 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
RFC	Request For Comment
RIP	Routing Information Protocol
SAP	(IPX) Service Advertising Protocol
SNMP	Simple Network Management Protocol
SUA	Single User Account
TA	(ISDN) Terminal Adapter
TFTP	Trivial File Transfer Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair (cable)
WAN	Wide Area Network

Index