Prestige 202

User's Guide

Version 2.50

(June, 2000)

ZyXEL

TOTAL INTERNET ACCESS SOLUTION

Prestige 202

ISDN Router

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

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Federal Communications Commission (FCC) Interference Statement

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

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

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

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

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

NOTICE 1

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

NOTICE 2

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

Information for Canadian Users

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

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

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

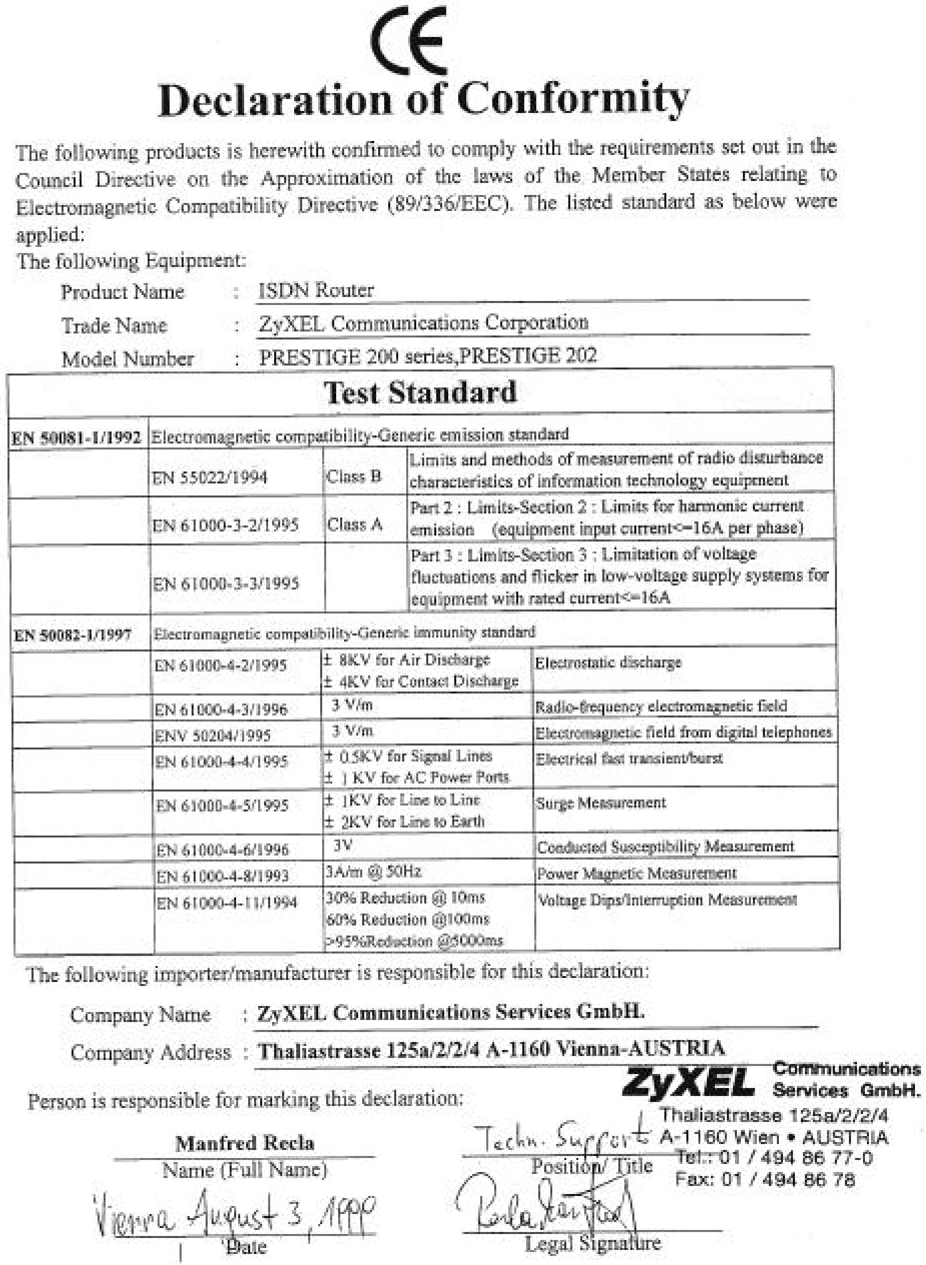
For their own protection, users should ensure that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

CAUTION

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

NOTE

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



CE

Declaration of Conformity

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

The following Equipment:

Product Name : ISDN Router

Trade Name : ZyXEL Communications Corporation

Model Number : PRESTIGE 200 series,PRESTIGE 202

Test Standard			
EN 50081-1/1992	Electromagnetic compatibility-Generic emission standard		
	EN 55022/1994	Class B	Limits and methods of measurement of radio disturbance characteristics of information technology equipment
	EN 61000-3-2/1995	Class A	Part 2 : Limits-Section 2 : Limits for harmonic current emission (equipment input current<=16A per phase)
	EN 61000-3-3/1995		Part 3 : Limits-Section 3 : Limitation of voltage fluctuations and flicker in low-voltage supply systems for equipment with rated current<=16A
EN 50082-1/1997	Electromagnetic compatibility-Generic immunity standard		
	EN 61000-4-2/1995	± 8KV for Air Discharge ± 4KV for Contact Discharge	Electrostatic discharge
	EN 61000-4-3/1996	3 V/m	Radio-frequency electromagnetic field
	ENV 50204/1995	3 V/m	Electromagnetic field from digital telephones
	EN 61000-4-4/1995	± 0.5KV for Signal Lines ± 1 KV for AC Power Ports	Electrical fast transient/burst
	EN 61000-4-5/1995	± 1KV for Line to Line ± 2KV for Line to Earth	Surge Measurement
	EN 61000-4-6/1996	3V	Conducted Susceptibility Measurement
	EN 61000-4-8/1993	3A/m @ 50Hz	Power Magnetic Measurement
	EN 61000-4-11/1994	30% Reduction @ 10ms 60% Reduction @100ms >95%Reduction @5000ms	Voltage Dips/Interruption Measurement

The following importer/manufacturer is responsible for this declaration:

Company Name : **ZyXEL Communications Services GmbH.**

Company Address : **Thaliastrasse 125a/2/2/4 A-1160 Vienna-AUSTRIA**

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

Person is responsible for marking this declaration:

Manfred Recla
Name (Full Name)

Techn. Support
Position/ Title

Vienna August 3, 1999
Date

Legal Signature

Declaration of Conformity

We, the Manufacturer/Importer

ZyXEL Communications Services GmbH.

Thaliastrasse 125a/2/2/4
A-1160 Vienna – AUSTRIA

declare that the product

Prestige 202

is in conformity with

(Reference to the specification under which conformity is declared)

STANDARD	STANDARD ITEM	VERSION
• EN 55022	Radio disturbance characteristics – Limits and method of measurement.	1994
• EN 61000-3-2	Disturbance in supply system caused by household appliances and similar electrical equipment “Harmonics”.	1995
• EN 61000-3-3	Disturbance in supply system caused by household appliances and similar electrical equipment “Voltage fluctuations”.	1995
• EN 61000-4-2	Electrostatic discharge immunity test – Basic EMC Publication.	1995
• EN 61000-4-3	Radiated, radio-frequency, electromagnetic field immunity test.	1996
• EN 61000-4-4	Electrical fast transient/burst immunity test – Basic EMC Publication.	1995
• EN 61000-4-5	Surge immunity test.	1995
• EN 61000-4-6	Immunity to conducted disturbances, induced by radio-frequency fields.	1996
• EN 61000-4-8	Power Magnetic Measurement.	1993
• EN 61000-4-11	Voltage dips, short interruptions and voltage variations immunity tests.	1994

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 and 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.

Online Registration

Do not forget to register your Prestige (fast, easy online registration at www.zyxel.com for free future product updates and information.

Customer Support

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

METHOD	EMAIL – SUPPORT	TELEPHONE	WEB SITE	REGULAR MAIL
REGION	EMAIL – SALES	FAX	FTP SITE	
WORLDWIDE	support@zyxel.com.tw support@europe.zyxel.com	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, HsinChu, Taiwan.
	sales@zyxel.com.tw	+886-3-578-2439	ftp.europe.zyxel.com	
NORTH AMERICA	support@zyxel.com	+1-714-632-0882 800-255-4101	www.zyxel.com	ZyXEL Communications Inc., 1650 Miraloma Avenue, Placentia, CA 92870, U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.zyxel.com	
SCANDINAVIA	support@zyxel.dk	+45-3955-0700	www.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark.
	sales@zyxel.dk	+45-3955-0707	ftp.zyxel.dk	
AUSTRIA	support@zyxel.at	+43-1-4948677-0 0810-1-ZyXEL 0810-1-99935	www.zyxel.at	ZyXEL Communications Services GmbH., Thaliastrasse 125a/2/2/4, A-1160 Vienna, Austria
	sales@zyxel.at	+43-1-4948678	ftp.zyxel.at **NOTE:** for Austrian users with *.at domain only!	
GERMANY	support@zyxel.de	+49-2405-6909-0 0180-5213247 Tech Support hotline 0180-5099935 RMA/Repair hotline	www.zyxel.de	ZyXEL Deutschland GmbH., Adenauerstr. 20/A4, D-52146 Wuerselen, Germany.
	sales@zyxel.de	+49-2405-6909-99	ftp.europe.zyxel.com	

Table of Contents

List of Figures

List of Tables

Preface

About Your Prestige

Congratulations on your purchase of the Prestige 202 ISDN Router.

The Prestige 202 is a high-performance router that offers a complete Internet Access solution.

You do not need to set any switches to configure the Prestige. The user-friendly Prestige Network Commander (PNC) is a C++ utility that allows you to manage the Prestige via a Graphical User Interface (GUI). 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.

Please visit our web site at www.zyxel.com for the latest release notes and other information about this product.

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 reference:
   - ISDN switch type
   - ISDN telephone number(s)
   - ISDN Service Profile Identifiers (SPID) number(s) (only for North America)

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 an internet 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.

Related Documentation

➢ PNC Disk

More detailed information about the Prestige and examples of its use can be found in our PNC (Prestige Network Commander – an alternative windows-based configuration wizard) Disk. This disk contains information on configuring your Prestige for Internet Access, a General FAQ, an Advanced FAQ, Applications Notes, Troubleshooting, Reference CI Commands as well as bundled software.

➢ Read Me First

Our Read Me First was designed to help you get your Prestige up and running right away. It contains a detailed easy to follow connection diagram, Prestige default settings, handy checklists and information on setting up your PC.

➢ *ZyXEL Web Page and FTP Server Site*

You can access release notes for firmware upgrades and other information at ZyXEL web pages and FTP server sites. Refer to the *Customer Support* page in this User's Guide for more information.

➢ Support Notes

More detailed information about the Prestige and examples of its use can be found in the Support Notes accessible through the ZyXEL web page.

➢ Packing List Card

Finally, you should have a Packing List Card that lists all items that should have come with your Prestige 202.

Syntax Conventions

- "Enter" means for you to type one or more characters and press the carriage return. "Select" or "Choose" means for you to select one from the predefined choices.
- The SMT menu titles and labels are in **Bold Times** font. The choices of a menu item are in **Bold Arial** font. A single keystroke is in Arial font and enclosed in square brackets, for instance, [Enter] means the Enter, or carriage return key; [Esc] means the Escape key.
- For brevity's sake, we will use "e.g.," as a shorthand for "for instance", and "i.e.," as a shorthand for "that is" or "in other words" throughout this manual.
- The Prestige 202 may also be referred to as the Prestige or the P202 from now on, in this manual.

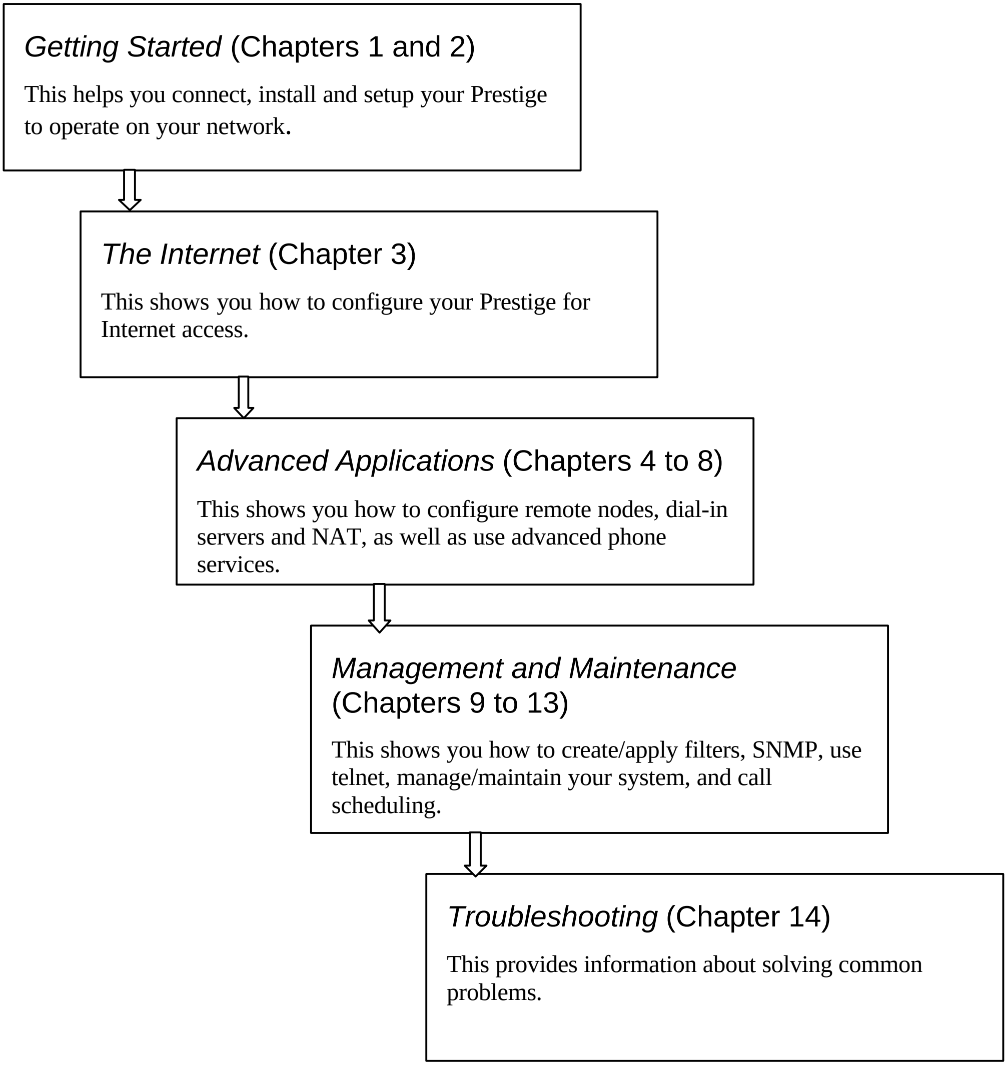
Prestige Scenarios

For fast access to sample SMT menus, refer to the following sections on how to configure the Prestige for various possible scenarios.

SCENARIO	GO TO SECTION
To reset your Prestige	2.8.1
DHCP	3.2.4
Internet Access	3.6
LAN-to-LAN application	5.1
Remote Access under Windows®	6.4.1
Callback	6.4.3
Callback with CLID	6.4.4
To configure NAT	7.5
To apply filters	9.4

Table 1-1 Prestige Scenarios

General Structure of This Manual



Getting Started (Chapters 1 and 2)

This helps you connect, install and setup your Prestige to operate on your network.

The Internet (Chapter 3)

This shows you how to configure your Prestige for Internet access.

Advanced Applications (Chapters 4 to 8)

This shows you how to configure remote nodes, dial-in servers and NAT, as well as use advanced phone services.

Management and Maintenance (Chapters 9 to 13)

This shows you how to create/apply filters, SNMP, use telnet, manage/maintain your system, and call scheduling.

Troubleshooting (Chapter 14)

This provides information about solving common problems.

Part I:

GETTING STARTED

Chapters 1 to 3 are structured as a step-by-step guide to help you connect, install and setup your Prestige to operate on your network and access the Internet.

Chapter 1

Getting to Know Your ISDN Router

This chapter covers the key features and main applications of your Prestige.

1.1 Features of the Prestige

Time and Date Setting

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

Call Scheduling

This feature allows the Prestige to manage and time a call to a remote node as well as set the call duration.

NAT (Network Address Translation)

ZyXEL's SUA (Single User Account) has now been replaced by the all new NAT support. 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 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.

SNMP (Simple Network Management Protocol – version 1)

SNMP, a member of the TCP/IP protocol suite, allows you to exchange management information between network devices. Your Prestige supports SNMP agent functionality that allows a manager station to manage and monitor the Prestige through the network.

NOTE: SNMP is only available if TCP/IP is configured on your Prestige.

IP Alias

This feature is described as the ability to partition a physical network into logical networks over the same Ethernet interface. You can use three logical LAN interfaces via a single physical Ethernet interface, with the Prestige acting as the gateway for all the LAN networks. You can also route packets from one network to another and, it allows your Prestige to have extra IP addresses.

10/100MB Auto-negotiation Ethernet/Fast Ethernet Interface

This auto-negotiation feature allows the Prestige to detect the speed of incoming transmissions and adjust appropriately, providing a faster data transfer on the Ethernet network as required.

ISDN Data Link Connection

The Prestige supports two types of ISDN Data Link Connection namely: point-to-multipoint and point-to-point. When you select point-to-multipoint, the TEI value is assigned by negotiation with the switch. When you select point-to-point, the TEI value will be assigned a unique value of 0.

ISDN Phone Bearer Capability

The Prestige supports two types of ISDN phone bearer capability namely: 3.1K and speech. You can set the Phone bearer capability “3.1K” using the CI command [isdn param set bearcapb 0] and set the Phone bearer capability “speech” using the CI command [isdn param set bearcapb 1].

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, you can configure the Prestige to act 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 (Multilink Protocol) 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.

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.

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 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

The Prestige Network Commander is a C++ based utility designed to allow users to access the Prestige’s management settings via a Worldwide Web browser.

Upgrade Firmware via LAN

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

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 Calling)
- Call Transfer
- Call Forwarding
- Reminder Ring

Caller ID Display Services on Analog PSTN Lines

The Prestige supports Caller ID information on both phone ports. To use Caller ID Display you need a special telephone or display unit that can show and store incoming telephone numbers.

1.2 Internet Access With the Prestige

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 next.

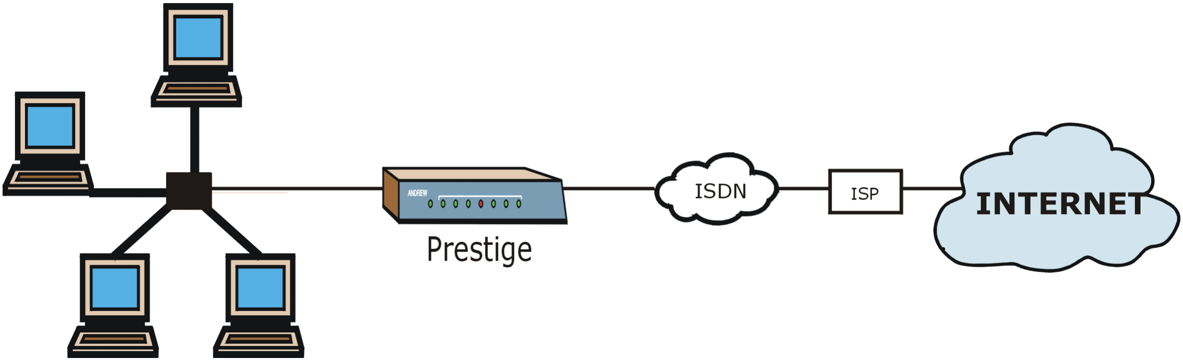


Figure 1-1 Internet Access Application

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 as follows.

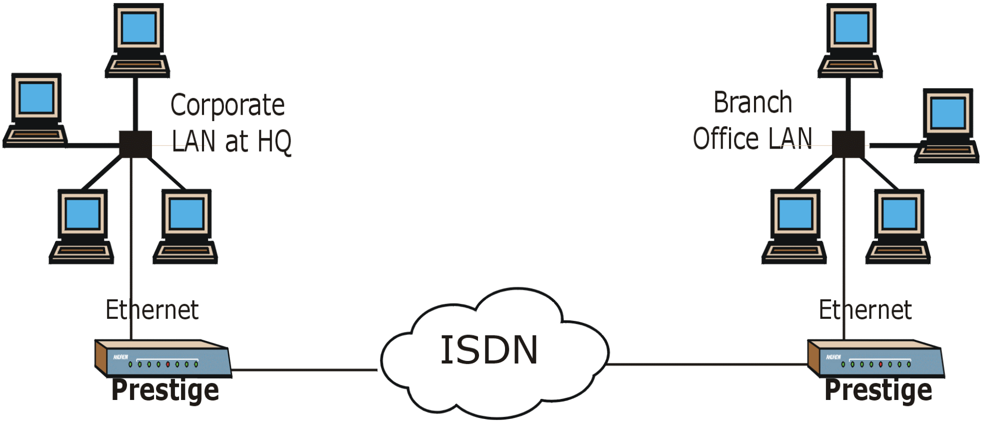


Figure 1-2 LAN-to-LAN Connection Application

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® 98, 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.

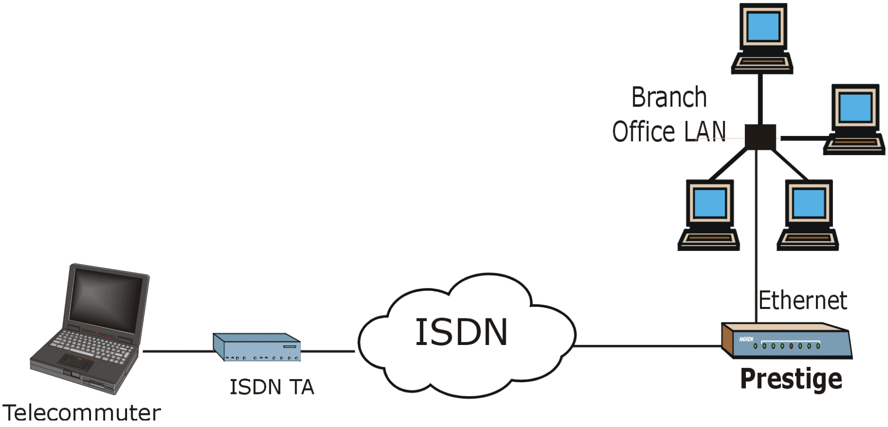


Figure 1-3 Remote Access

Chapter 2
Hardware Installation and Initial Setup

This chapter shows you how to make the cable connections to your Prestige as well as set up your ISDN connection using the SMT.

2.1 Front Panel LEDs of Prestige 202

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

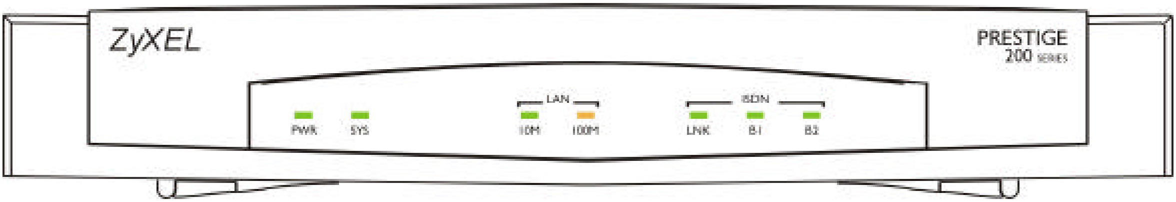


Figure 2-1 Front Panel of Prestige 202

Table 2-1 LED Functions

LED	DESCRIPTION
PWR	The PWR (power) LED is on when power is applied to the Prestige.
SYS	A steady on SYS (system) LED indicates the Prestige is on and functioning properly while an off SYS LED indicates the system is not ready or a malfunction. The system is rebooting when the SYS LED is blinking.
LAN 10M	A steady *green* light indicates a successful 10Mb Ethernet connection. The LED will blink when data is being sent/received.
LAN 100M	A steady *orange* light indicates a successful 100Mb Ethernet connection. The LED will blink when data is being sent/received.
ISDN (Europe) **LNK, B1, B2**	The LNK LED is on when the Prestige is connected to an ISDN switch and the line has been successfully initialized. The B1 (B2) LED remains steady on when data is

LED	DESCRIPTION
	being sent/received on the B1 (B2) bearer channel.
ISDN (North America)	Similar to European version but there are 4 LNK LED status. Off There is no ISDN link. Fast Blinking The LED blinks quickly when there is an ISDN link but SPID negotiation is still in progress. Slow Blinking The LED blinks slowly when SPID negotiation has failed. On The LED is steady on when SPID negotiation has been successful and the ISDN line has been successfully initialized.

2.2 Prestige 202 Rear Panel and Connections

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

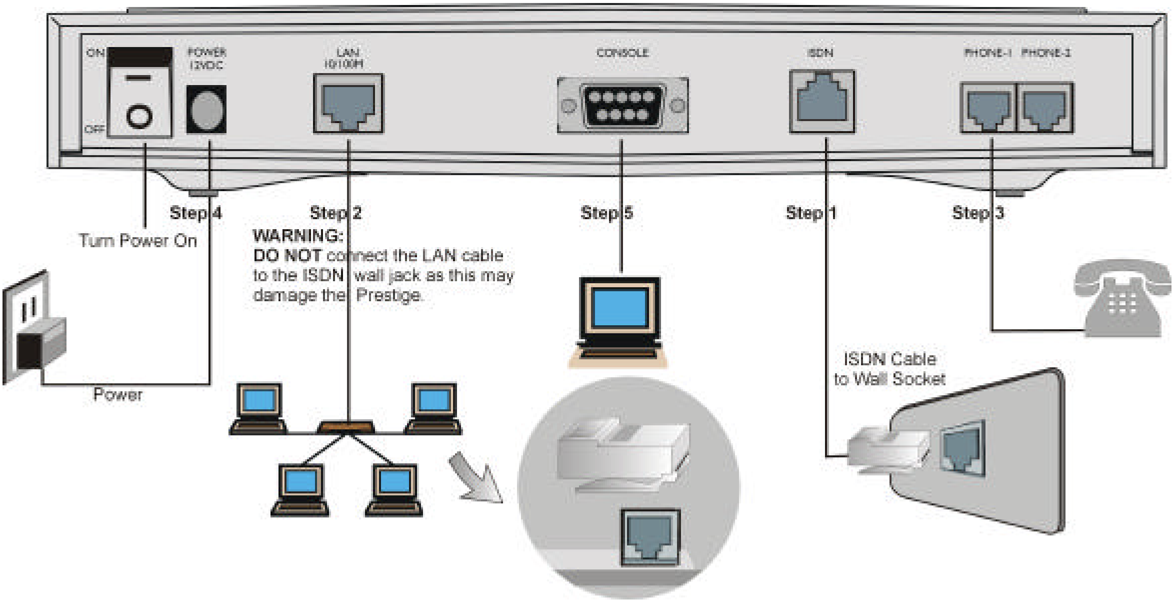

ON
OFF
POWER 12VDC
LAN 10/100M
CONSOLE
ISDN
PHONE-1
PHONE-2
Step 4
Turn Power On
Step 2
WARNING:
DO NOT connect the LAN cable to the ISDN wall jack as this may damage the Prestige.
Step 5
Step 1
Step 3
Power
ISDN Cable to Wall Socket

Figure 2-2 Prestige 202 Rear Panel

This section outlines how to connect your Prestige to the LAN and to the ISDN network.

Step 1. *Connecting the ISDN Line*

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

Step 2. *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. Use the crossover cable to connect your Prestige to a computer directly or use straight-through Ethernet cable to connect to an external hub.

Step 3. *Connecting a Telephone/Fax to the Prestige*

If you wish, 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 4. *Connecting the Power Adapter to your Prestige*

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

CAUTION: To prevent damage to the Prestige, first make sure you have the correct AC power adapter specifications (refer to the Appendix section) for your particular region.

Step 5. *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-232C cable if the enclosed one is too short.

After the initial setup, you can modify the configuration remotely through telnet connections. See the *Telnet Configuration and Capabilities* chapter for detailed instructions on using telnet to configure 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 Baud.
- No parity, 8 Data bits, 1 Stop bit, no Flow Control.

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

2.4 Housing

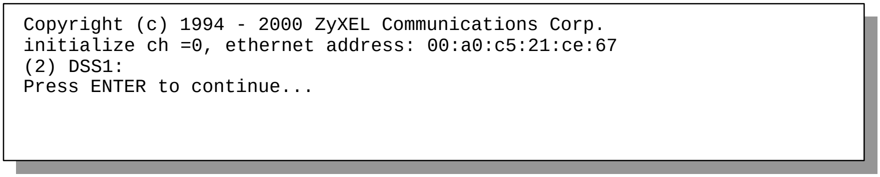
Your Prestige's housing has ventilation slots for cooling and clip-out legs that fit snugly into grooves for sturdy stacking with better airflow. ZyXEL recommends that you do not stack more than 4 routers for maximum stack stability and cooling.

2.5 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 the on position (**I** is ON, **O** is OFF).

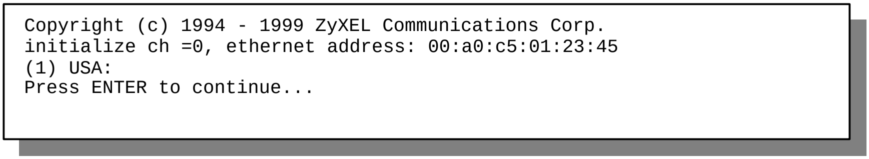
Step 1. Initial Screen

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.
initialize ch =0, ethernet address: 00:a0:c5:21:ce:67
(2) DSS1:
Press ENTER to continue...
```

Figure 2-3 Power-On Display for DSS1 Switch



```
Copyright (c) 1994 - 1999 ZyXEL Communications Corp.
initialize ch =0, ethernet address: 00:a0:c5:01:23:45
(1) USA:
Press ENTER to continue...
```

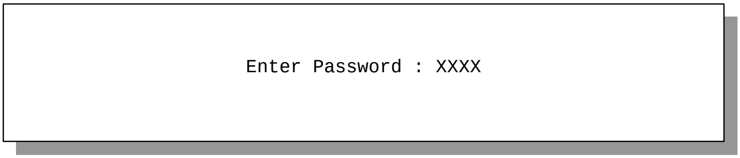
Figure 2-4 Power-On Display for USA Switches

Step 2. Entering Password

The login screen appears after you press [Enter], prompting you to enter the password as shown in the following figure.

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

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



```
Enter Password : XXXX
```

Figure 2-5 Login Screen

2.6 Navigating the SMT Interface

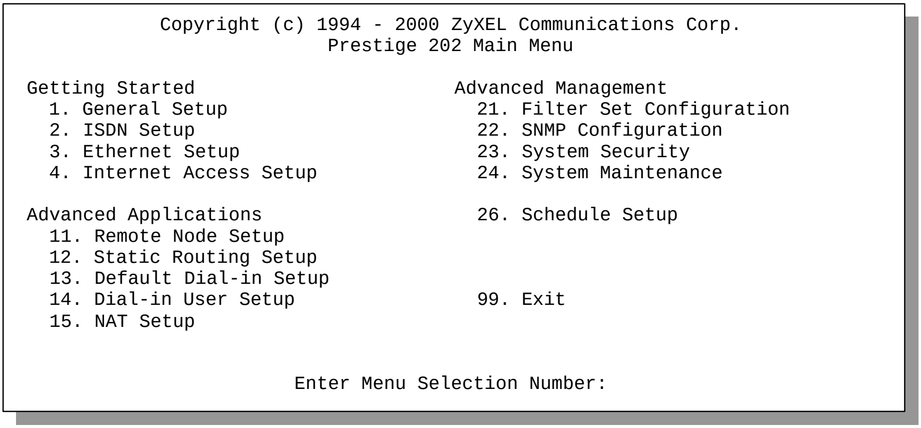
The SMT (System Management Terminal) is the interface that you use to configure your Prestige.

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

Table 2-2 Main Menu Commands

OPERATION	KEYSTROKES	DESCRIPTION
Move forward to another menu	[Enter]	To move forward to another menu, type in the number of the desired 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 submenu	Press [space bar] to change **No** to **Yes** then press [Enter]	Fields beginning with "Edit" have a default setting of **No**. Press [space bar] to change **No** to **Yes**, then press [Enter] to go to a submenu.
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 [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 [space bar].
Required fields	<?>	All fields with the symbol <?> must be filled in order to be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[Enter]	Save your configuration by pressing [Enter] at the message [Press ENTER to confirm or ESC to cancel]. Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [Enter]	Type 99 at the Main Menu prompt and press [Enter] to exit the SMT interface.

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



```
                 Copyright (c) 1994 - 2000 ZyXEL Communications Corp.
                              Prestige 202 Main Menu

 Getting Started                       Advanced Management
   1. General Setup                      21. Filter Set Configuration
   2. ISDN Setup                         22. SNMP Configuration
   3. Ethernet Setup                     23. System Security
   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                99. Exit
   15. NAT Setup


                           Enter Menu Selection Number:
```

Figure 2-6 SMT Main Menu

2.6.1 System Management Terminal Interface Summary

Table 2-3 Main Menu Summary

No.	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to setup general information.
2	ISDN Setup	Use this menu to setup the ISDN.
3	Ethernet Setup	Use this menu to setup Ethernet.
4	Internet Access Setup	A quick and easy way to setup Internet connection.
11	Remote Node Setup	Use this menu to setup the Remote Node for LAN-to-LAN connection, including Internet connection.
12	Static Routing Setup	Use this menu to setup static route for different protocols.
13	Default Dial-in Setup	Use this menu to setup default dial-in parameters so that your Prestige can be used as a dial-in server.
14	Dial-in User Setup	Use this menu to setup dial-in users.
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.
22	SNMP Configuration	Use this menu to setup SNMP-related parameters.
23	System Security	Use this menu to setup security-related parameters.

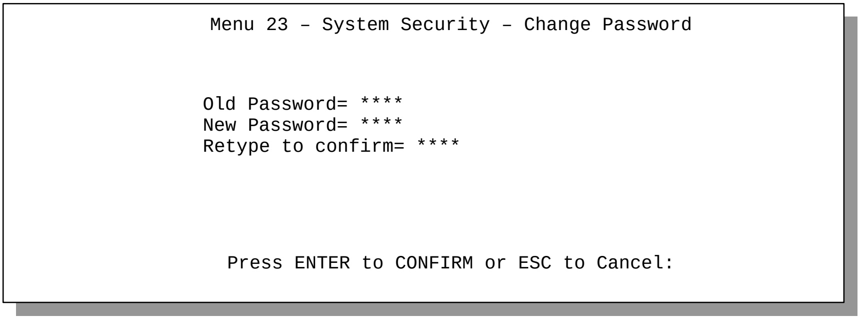
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
26	Schedule Setup	This menu allows the Prestige to manage a remote node and dictate when a remote node should be called and for how long.
99	Exit	To exit from SMT and return to the blank screen.

2.7 Changing the System Password

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

Step 1. Enter 23 in the Main Menu to open **Menu 23 – System Security – Change Password** as shown in the following figure.

When this menu appears, type in your existing system password, i.e., 1234, and press [Enter].



```
                 Menu 23 – System Security – Change Password



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





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

Figure 2-7 Menu 23.1 – System Password

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

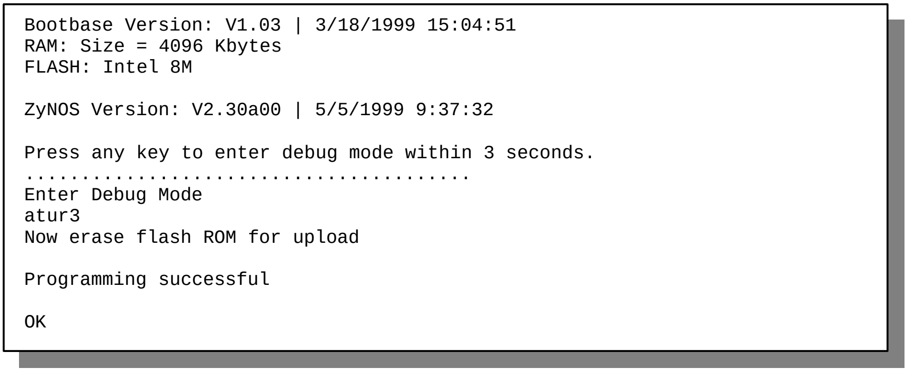
Step 3. Re-type your new system password for confirmation and press [Enter].

NOTE: As you type a password, the screen displays an (*) for each character you typed.

2.8 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 one 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 9600 bps with 8 data bit, no parity, 1 stop bit (8n1), and no Flow Control. The password will be reset to the default of 1234, also.

Turn off the Prestige and begin a Terminal session with the current console port settings. Turn on the Prestige again. You should see the following screen. 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 "romfile.zip" file from the Internet and unzipped it.



```
Bootbase Version: V1.03 | 3/18/1999 15:04:51
RAM: Size = 4096 Kbytes
FLASH: Intel 8M

ZyNOS Version: V2.30a00 | 5/5/1999 9:37:32

Press any key to enter debug mode within 3 seconds.
........................................
Enter Debug Mode
atur3
Now erase flash ROM for upload

Programming successful

OK
```

Figure 2-8 Booting Up the Prestige

Perform the following procedures to upload the configuration file:

1. Enter “`atlc`” after the “`Enter Debug Mode`” message.
2. Wait for the “`Starting XMODEM upload`” message before activating XMODEM upload on your terminal.
3. After a successful firmware upload, enter “`atgo`” to restart the Prestige.

The Prestige is now reinitialized with a default configuration file including the default password of 1234.

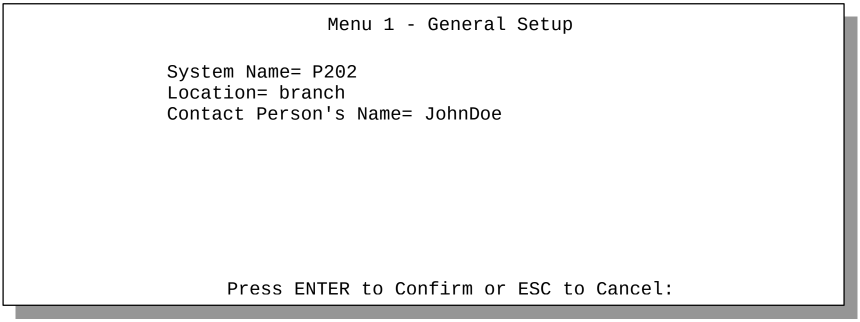
2.9 General Setup

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

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

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

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



```
                                    Menu 1 - General Setup

                    System Name= P202
                    Location= branch
                    Contact Person's Name= JohnDoe








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

Figure 2-9 Menu 1 – General Setup

Table 2-4 General Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
System Name	Choose a descriptive name, up to 30 alphanumeric characters long (no spaces, but dashes "–" and underscores "_" are accepted) for identification purposes. This name can be retrieved remotely via SNMP, used for CHAP authentication, and displayed at the prompt in the Command Mode.	P202
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 your Prestige.	JohnDoe

2.10 ISDN Setup Menus

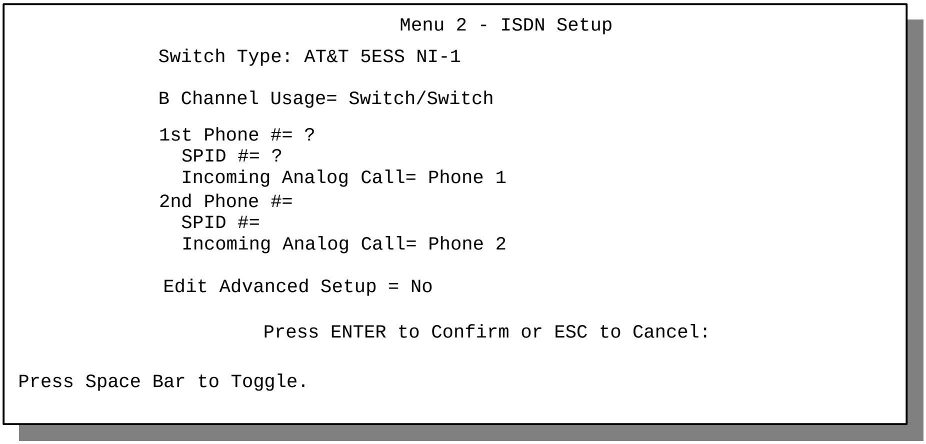
Menu 2 is for you to enter the information about your ISDN line. Different telephone companies deploy different types of switches for ISDN service. Depending on the switch for your particular installation, you will have a different number of telephone numbers. If you are in North America, you may also have SPIDs (Service Profile Identifiers). The SPID is a number used by a switch for identification purposes. Make sure that you have the correct and complete telephone numbers and SPIDs. You need to pass the ISDN setup before your system can make an outgoing call or answer an incoming call. The following table will help you decide the number of telephone numbers and SPIDs (if any) for your geographic location. The majority of switches in North America run NI-1.

Table 2-5 SPIDs, Phone Numbers, Switch Types

SWITCH TYPE	GEOGRAPHY	No. of Phone #'s	No. of SPIDs
AT&T 5ESS NI-1	North America	2	2
AT&T 5ESS Point-to-Point	North America	1	0
AT&T 5ESS Multipoint	North America	2	2
Northern Telecom NI-1	North America	2	2
Northern Telecom Custom	North America	2	2
DSS1	Europe, Asia	1+	N/A

2.10.1 North American ISDN Setup Menus

Menu 2 for North American switches is displayed next.



```
                              Menu 2 - ISDN Setup
             Switch Type: AT&T 5ESS NI-1

             B Channel Usage= Switch/Switch

             1st Phone #= ?
               SPID #= ?
               Incoming Analog Call= Phone 1
             2nd Phone #=
               SPID #=
               Incoming Analog Call= Phone 2

              Edit Advanced Setup = No

                       Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 2-10 North American ISDN Setup

Table 2-6 North American ISDN Menu Setup Fields

FIELD	DESCRIPTION
Switch Type	If your switch type is not currently shown, press [space bar] to change to the next switch; repeat until you see the correct switch type. The majority of switches run NI-1; if the link LED does not come up, try NI-1. The Prestige will not be able to place or to receive calls if the wrong switch type is specified. If you are not sure, contact your telephone company to confirm the exact switch type.
B Channel Usage	In general, this will be **Switch/Switch** (default). If you are only using one B channel (e.g., your Prestige is sharing the ISDN BRI line with another device), then select **Switch/Unused**. If your second B channel is a leased line, select **Switch/Leased.** Press [space bar] to toggle through all the options. The options are: ♦ **Switch/Switch** ♦ **Switch/Leased** ♦ **Leased/Switch** ♦ **Leased/Unused** ♦ **Unused/Leased** ♦ **Leased/Leased** ♦ **Switch/Unused**
Telephone Number(s)	Enter the telephone number(s) assigned to your ISDN line by your telephone company. Some switch types only have one telephone number. For North America, these phone numbers should be in a standard seven-digit format (e.g., 5551212). Note that the Prestige only accepts digits; please do not include '–' and spaces in this field. This field should be no longer than 25 digits.

FIELD	DESCRIPTION
Incoming Analog Call	This tells the Prestige how to route an incoming analog call. Set to **Phone1** if you wish to route the incoming analog call for this telephone number to the PHONE port 1 (a.k.a., 'POTS' port in North America and 'A/B Adapter' in Europe). Set to **Phone2** if you wish to route the incoming analog call for this telephone number to PHONE port 2. Set to **DOVBS** if you wish to receive incoming Data Over Voice Bearer Service call. Note that in this case both phone ports will handle incoming analog calls as **DOVBS**.
SPID Number(s)	Depending on your switch type, you may have zero, one, or two SPIDs assigned to your line. For example, if your switch type is Northern Telecom Custom, you will have to enter two SPID numbers.
Edit Advanced Setup	Advanced Setup features are configured when you select **Yes** to enter 2.1 Advanced Setup menu (see ahead). Refer to the Advanced Phone Services Chapter for detailed information.

Supplementary Voice Services

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

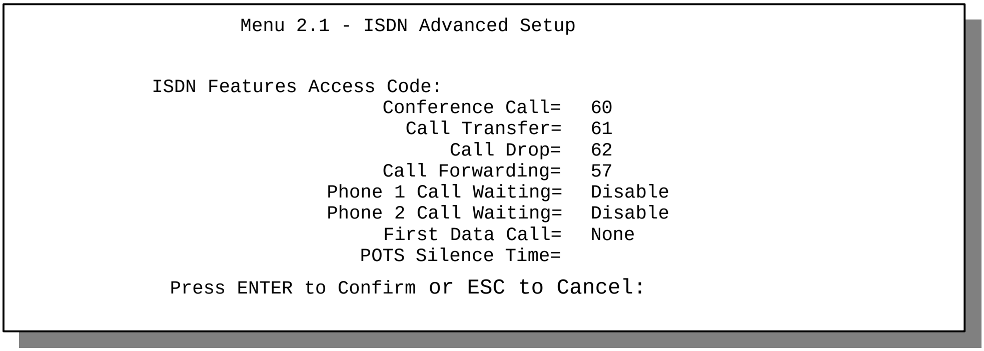
- Call Waiting
- Three Way Calling (Conference Call)
- Call Transfer
- Call Forwarding
- Reminder Ring
- Terminal Portability
- MSN/Subaddress

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:

Table 2-7 NI-1 Default Feature Key Settings

FEATURE	DEFAULT FEATURE KEY
3-Way Calling (Conference)	60
Call Transfer	61
Call Drop	62
Call Forwarding	57

If your phone company cannot support these default Feature Key settings, ask the phone company representative to provide you with settings which are within their support range. Then select **Yes** in the **Edit Advanced Setup** field in Menu 2 above and change the settings in **Menu 2.1 – ISDN Advanced Setup**.



```
                     Menu 2.1 - ISDN Advanced Setup


             ISDN Features Access Code:
                                 Conference Call=   60
                                   Call Transfer=   61
                                       Call Drop=   62
                                 Call Forwarding=   57
                            Phone 1 Call Waiting=   Disable
                            Phone 2 Call Waiting=   Disable
                                 First Data Call=   None
                               POTS Silence Time=

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

Figure 2-11 Menu 2.1 – ISDN Advanced Setup

Table 2-8 Menu 2.1 – ISDN Advanced Setup Fields

Call Waiting	**Enable** allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.
First Data Call	This field dictates which directory number (B-channel) you prefer to use for the first data call. **None** 1st phone number, no B-channel preference **1st** 1st phone number, B1 channel preference **2nd** 2nd phone number, B2 channel preference
POTS Silence Time	Some devices, e.g., some answering machines, only recognize that a calling party has hung up after a period of silence. This field sets the period of silence, which can be from 0 (default) to 10 seconds.

2.10.2 European (DSS1) ISDN 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

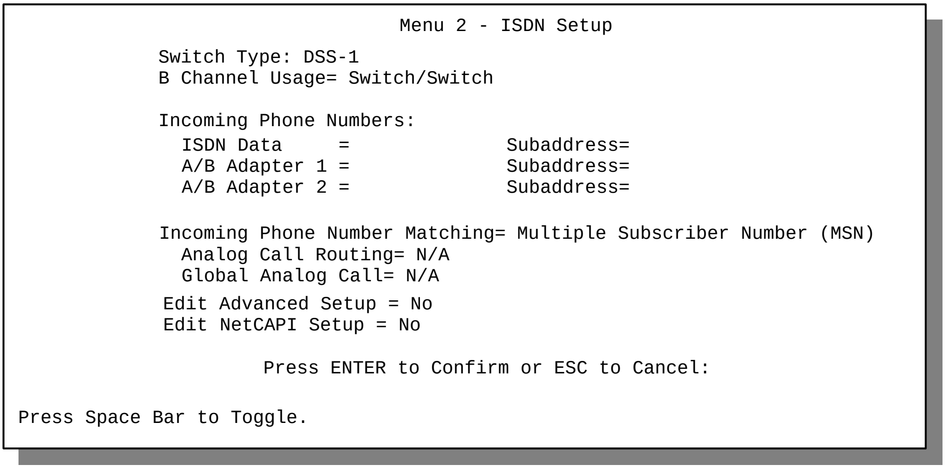
The **Incoming Phone Number Matching** setting governs how incoming calls are routed. If you select **Multiple Subscriber Number (MSN)** or **Called Party Subaddress**, a call (either ISDN data or analog) is routed to the port that matches the dialed number; if no match is found, the call is dropped.

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.



```
                                  Menu 2 - ISDN Setup
             Switch Type: DSS-1
             B Channel Usage= Switch/Switch

             Incoming Phone Numbers:
               ISDN Data     =              Subaddress=
               A/B Adapter 1 =              Subaddress=
               A/B Adapter 2 =              Subaddress=

             Incoming Phone Number Matching= Multiple Subscriber Number (MSN)
               Analog Call Routing= N/A
               Global Analog Call= N/A
             Edit Advanced Setup = No
             Edit NetCAPI Setup = No

                      Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 2-12 Menu 2 – ISDN Setup for DSS1

Table 2-9 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/Leased** ♦ **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).
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, Both** 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).
Edit NetCAPI Setup	(Please refer to the next section.)

2.11 NetCAPI

NetCAPI is ZyXEL's implementation of CAPI (Common ISDN Application Program Interface) capabilities over a network. It runs over DCP (Device Control Protocol) developed by RVS-COM.

NetCAPI can be used for applications such as Eurofile transfer, file transfer, G3/G4 Fax, Autoanswer host mode, telephony, etc. on Windows® 95/98/NT platforms.

2.11.1 CAPI

CAPI is an interface standard that allows applications to access ISDN services. Several applications can share one or more ISDN lines. When an application wants to communicate with an ISDN terminal it sends a series of standard commands to the terminal. The CAPI standard defines the commands and allows you to use a well-defined mechanism for communications using ISDN lines.

CAPI also simplifies the development of ISDN applications through many default values that do not need to be programmed. It provides a unified interface for applications to access the different ISDN services such as data, voice, fax, telephony, etc.

2.11.2 ISDN-DCP

ISDN-DCP allows a workstation on the LAN to use services such as transmitting and receiving faxes as well as placing and receiving phone calls.

Using ISDN-DCP, the Prestige acts as a DCP server. By default, the Prestige listens for DCP messages on TCP port number 2578 (the Internet-assigned number for RVS-COM DCP). When the Prestige receives a DCP message from a DCP client i.e., a workstation, the Prestige processes the message and acts on it. Your Prestige supports all the DCP messages specified in the ISDN-DCP specification.

2.11.3 RVS-CE and RVS-COM lite

RVS-CE (Core Engine) is an ISDN-CAPI 2.0 driver for Windows® 95/98/NT that can be used by different ISDN communication programs (such as Fritz or RVS-COM) to access the ISDN on the Prestige. NetCAPI can carry out CAPI applications only if the RVS-CE driver is installed on your workstation.

In addition to the RVS-CE driver, you will need a communication software program such as RVS-COM lite for users to access CAPI.

You can use other programs such as Fritz for this purpose however, you still need to install the RVS-CE driver because the software will search for the CAPI driver.

2.12 Configuring the Prestige as a NetCAPI Server

This section describes how to configure your Prestige to be a NetCAPI server using the SMT (System Management Terminal).

NOTE: When configuring your Prestige with the PNC, use PNC version 2.10 and higher.

By default, NetCAPI is enabled on your Prestige. When NetCAPI is enabled, the Prestige listens for incoming DCP messages from the workstations. By default, the Prestige listens for DCP messages on TCP port 2578.

The following figure illustrates the configuration used in this example.

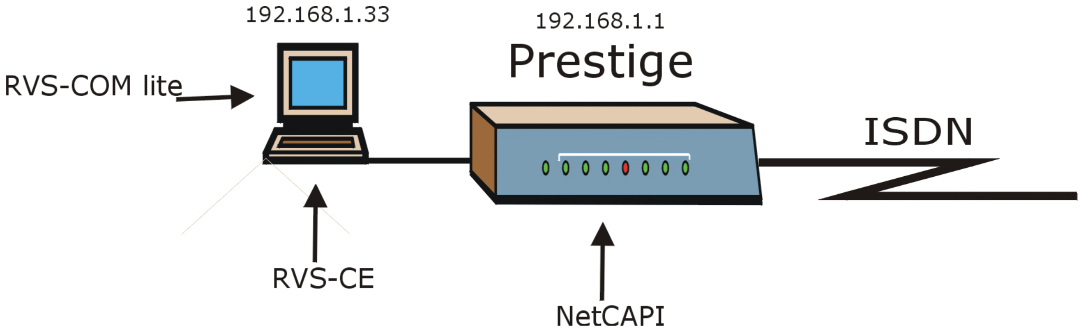


Figure 2-13 Sample Configuration

Before entering any configurations, you must install RVS-CE and RVS-COM lite on your workstation.

2.12.1 Installing RVS-CE and RVS-COM lite Software

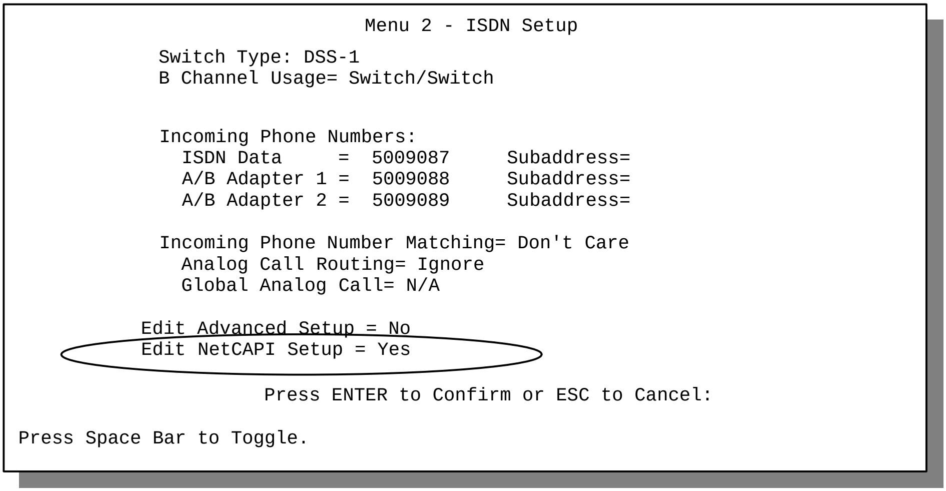
NOTE: Please uninstall previous versions of "RVS-CAPI" and "RVS-COM lite" before you install the new versions. You may use the Windows® "START | Settings | Control Panel | Add/Remove Programs" to uninstall RVS-CAPI and RVS-COM.

Install RVS-COM lite using the installation wizard and start the SETUP.EXE. Enter one of the license keys of your RVS-COM lite CD-ROM and follow the instructions.

**NOTE: The RVS-CE is automatically installed when you install RVS-COM lite v1.63 or later; but,
when installing RVS-COM lite v1.61 or older, install the RVS-CE first.**

2.12.2 Configuring NetCAPI

Step 1 Go to **Menu 2 – ISDN Setup**.

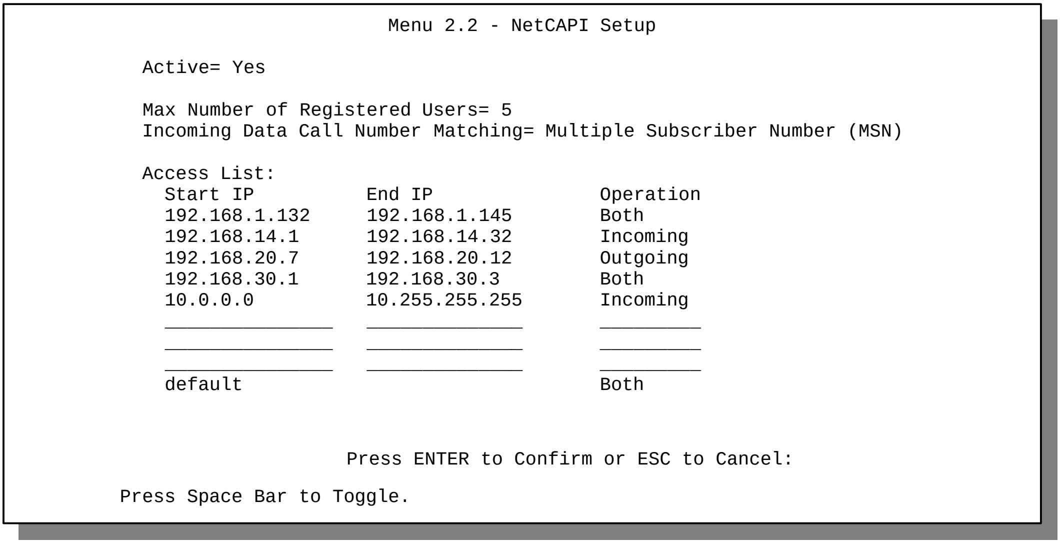


```
                                Menu 2 - ISDN Setup
                Switch Type: DSS-1
                B Channel Usage= Switch/Switch


                Incoming Phone Numbers:
                  ISDN Data     =  5009087     Subaddress=
                  A/B Adapter 1 =  5009088     Subaddress=
                  A/B Adapter 2 =  5009089     Subaddress=

                Incoming Phone Number Matching= Don't Care
                  Analog Call Routing= Ignore
                  Global Analog Call= N/A

              Edit Advanced Setup = No
              Edit NetCAPI Setup = Yes

                          Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 2-14 Menu 2 – ISDN Setup

NOTE: For more information about the various fields in this menu please refer to the previous section.

Step 2 Toggle [space bar] to select **Yes** in **Edit NetCAPI Setup** field and press [Enter] to go to **Menu 2.2 – NetCAPI Setup**.



```
                              Menu 2.2 - NetCAPI Setup

            Active= Yes

            Max Number of Registered Users= 5
            Incoming Data Call Number Matching= Multiple Subscriber Number (MSN)

            Access List:
              Start IP          End IP              Operation
              192.168.1.132     192.168.1.145       Both
              192.168.14.1      192.168.14.32       Incoming
              192.168.20.7      192.168.20.12       Outgoing
              192.168.30.1      192.168.30.3        Both
              10.0.0.0          10.255.255.255      Incoming
              _______________   ______________      _________
              _______________   ______________      _________
              _______________   ______________      _________
              default                               Both



                              Press ENTER to Confirm or ESC to Cancel:

          Press Space Bar to Toggle.
```

Figure 2-15 Menu 2.2 – NetCAPI Setup

Step 3 Set the fields in the above menu according to the following description.

Table 2-10 NetCAPI Setup Fields

FIELD	DESCRIPTION
Active	This field allows you to enable or disable NetCAPI. Press [space bar] to toggle between **Yes** and **No.**
Max Number of Registered Users	When you want to use NetCAPI to place outgoing calls or to listen to incoming calls, you must start RVSCOM on your workstation, and RVSCOM will register itself to the Prestige. This option is the maximum number of clients that the Prestige supports at the same time. The default value is **5**.
Incoming Data Call Number Matching	This field determines how incoming calls are routed. Press [space bar] to select **NetCAPI** if you want to direct all incoming data calls to NetCAPI. Select **MSN** if you want to direct all incoming call to the Prestige only when the incoming phone number matches the ISDN DATA number in Menu 2. If the incoming phone number does not match the ISDN DATA number, then the call will be routed to NetCAPI.

	Select **Called Party Subaddress** if you want to direct all incoming calls to the Prestige only when the incoming call matches the subaddress of ISDN DATA in Menu 2. If the incoming call does not match the subaddress of ISDN DATA, then the call will be routed to NetCAPI.
Access List	This list specifies users that can use NetCAPI. This access list controls if a client is allowed to use NetCAPI. The request is rejected when 1. The IP address of the workstation is not between **Start IP** and **End IP** or 2. The request from the workstation is not permitted as specified in the **Operation** field.
Start IP	Refers to the first IP address of a group of NetCAPI clients. Each group contains contiguous IP addresses.
End IP	Refers to the last IP address in a NetCAPI client group.
Operation	Press [space bar] to select **Incoming** if you wish to grant incoming calls permission. Select **Outgoing** if you wish to grant outgoing calls permission. Select **Both** if you wish to grant both incoming calls and outgoing calls permissions. Select **None** if you wish to deny all calls.

Advanced Setup

Select **Yes** in the **Edit Advanced Setup** field of **Menu 2 – ISDN Setup** (for DSS1) above to display Menu 2.1 as shown ahead.

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 disabled on both telephone ports, but can be enabled 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, determines 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.

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.

PABX Number (with S/T Bus Number) for Loopback

Enter the S/T bus number if the Prestige is connected to an ISDN PABX. If this field is left as blank then the ISDN loopback test will be skipped.

Outgoing Calling Party Number

If these fields are not blank, the Prestige will use these values as the *calling party number* for "ISDN Data", "A/B Adapter 1" and "A/B Adapter 2" outgoing calls. Otherwise, the individual entries for "ISDN Data", "A/B Adapter 1" and "A/B Adapter 2" will be used as the calling party number. You only need to fill in these fields if your switch or PABX requires a specific calling party number for outgoing calls, otherwise, leave them blank.
The following diagram illustrates the **PABX Number (with S/T Bus Number) for Loopback** and **Outgoing Calling Party Number** fields for a Prestige behind an ISDN PABX.

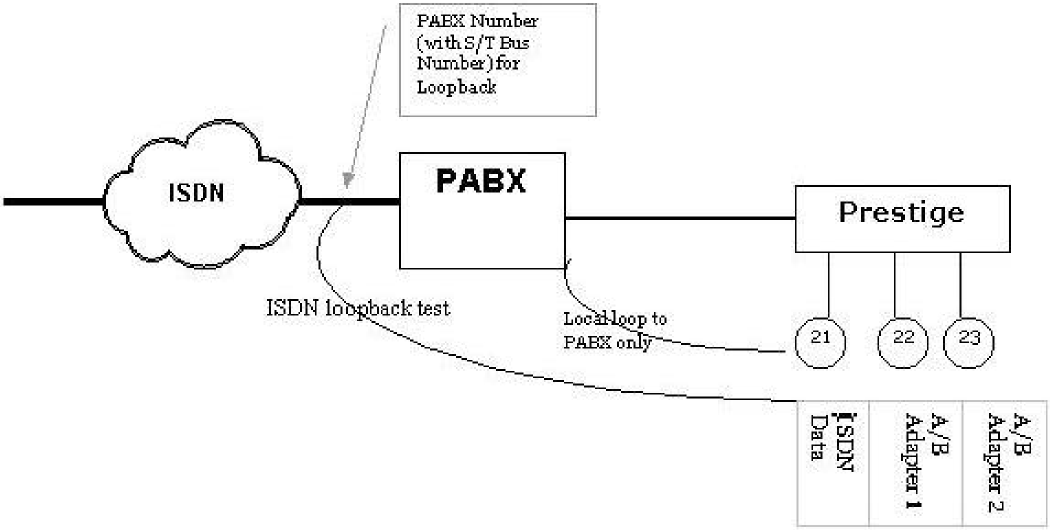


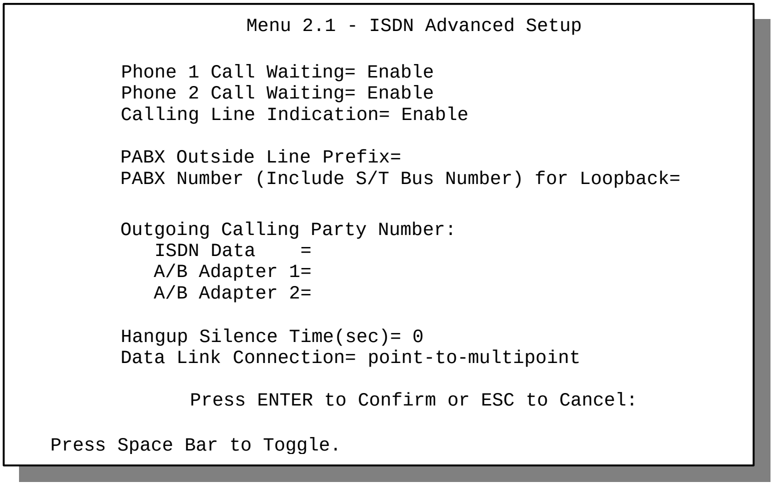
Figure 2-16 Prestige Behind a PABX

Hangup Silence Time

Some devices, e.g., some answering machines, only recognize that a calling party has hung up after a period of silence. This field sets the silence-time period, which can be from 0 (default) to 60 seconds.

Data Link Connection

There are two types of ISDN Data Link Connection namely: **point-to-multipoint** and **point-to-point**. When you select point-to-multipoint, the TE1 value will be assigned by negotiation with the switch. When you select point-to-point, the TE1 value will be assigned a unique value of 0.

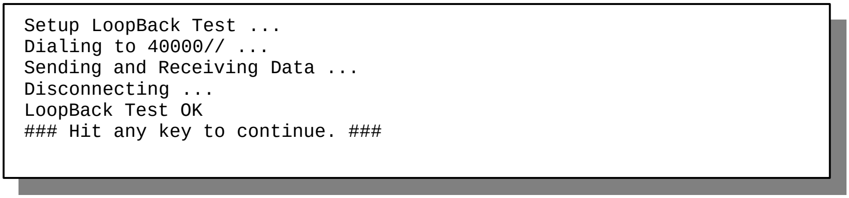


```
                 Menu 2.1 - ISDN Advanced Setup

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

      PABX Outside Line Prefix=
      PABX Number (Include S/T Bus Number) for Loopback=


      Outgoing Calling Party Number:
         ISDN Data    =
         A/B Adapter 1=
         A/B Adapter 2=

      Hangup Silence Time(sec)= 0
      Data Link Connection= point-to-multipoint

            Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 2-17 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.

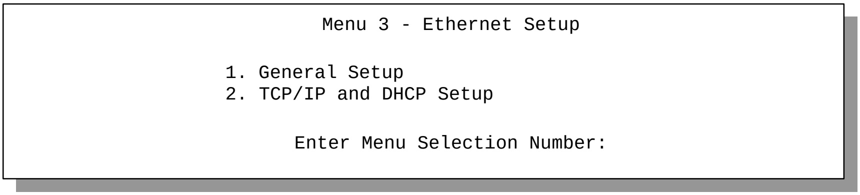


```
Setup LoopBack Test ...
Dialing to 40000// ...
Sending and Receiving Data ...
Disconnecting ...
LoopBack Test OK
### Hit any key to continue. ###
```

Figure 2-18 Loopback Test

2.13 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.

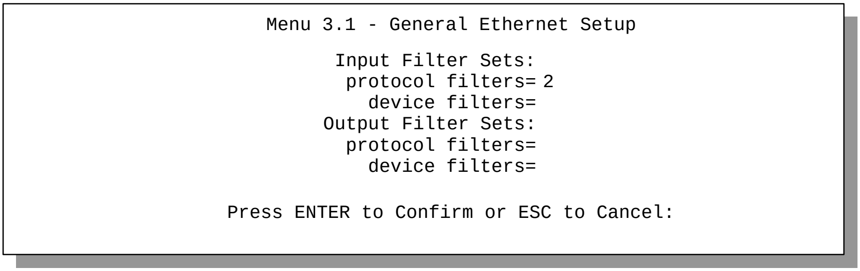


```
                         Menu 3 - Ethernet Setup

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

                       Enter Menu Selection Number:
```

Figure 2-19 Menu 3 – Ethernet Setup

2.13.1 General Ethernet Setup

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



```
                     Menu 3.1 - General Ethernet Setup

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

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

Figure 2-20 Menu 3.1 – General Ethernet Setup

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

2.14 Protocol Dependent Ethernet Setup

- For TCP/IP Ethernet setup refer to *Chapter 3 – Internet Access Application*.
- For remote node TCP/IP configuration refer to *Chapter 5 – Remote Node TCP/IP Configuration.*

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 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 us 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.

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 do not 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 an 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 can also act as a surrogate DHCP server where it relays IP address assignment from the actual DHCP server to the clients.

IP Pool Setup

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

DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, e.g., the IP address of *www.zyxel.com* is 204.217.0.2. The DNS server is extremely important because without it, a user must know the IP address of a machine before s/he can access it.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. If your ISP does give you the DNS server addresses, enter them in the **DNS Server** fields in **DHCP Setup**. The second is to leave this field blank, i.e., 0.0.0.0 – in this case the Prestige acts as a DNS proxy.

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 by 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.

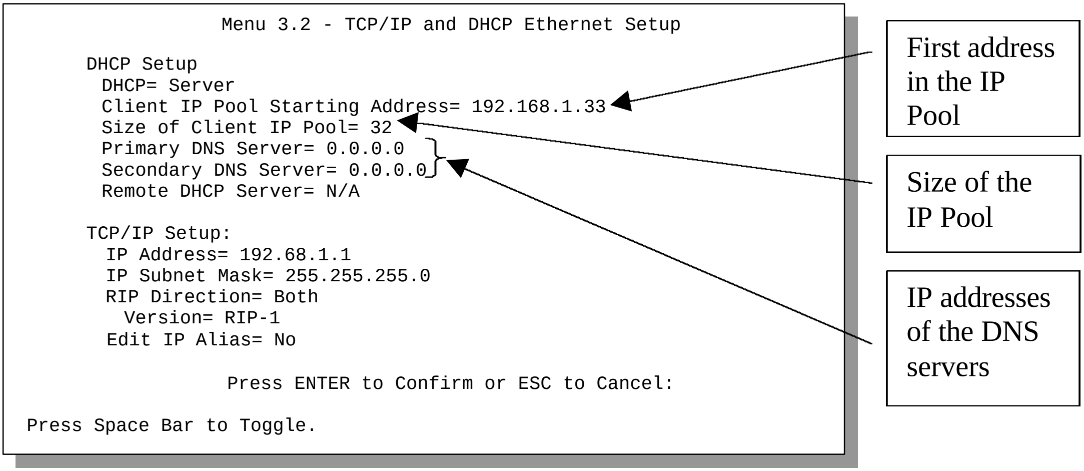
Example of Network Properties for LAN Servers With Fixed IP#

Choose an IP:	192.168.1.2 to 192.168.1.32; 192.168.1.65 to 192.168.1.254.
Netmask:	255.255.255.0
Gateway (or default route):	192.168.1.1 (Prestige LAN IP)
DNS server:	192.168.1.1
Domain:	(optional)

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.



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

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

       TCP/IP Setup:
         IP Address= 192.68.1.1
         IP Subnet Mask= 255.255.255.0
         RIP Direction= Both
           Version= RIP-1
         Edit IP Alias= No

                    Press ENTER 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 next 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/disables the DHCP server. If set to **Server**, your Prestige will act as a DHCP server. If set to **None**, the DHCP server will be disabled. If set to **Relay,** the Prestige acts as a surrogate DHCP server and relays requests and responses between the remote server and the clients. When set to **Server**, 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.	
Remote DHCP Server	If **Relay** is selected in the **DHCP** field above, then enter the IP address of the actual, remote DHCP server here.	

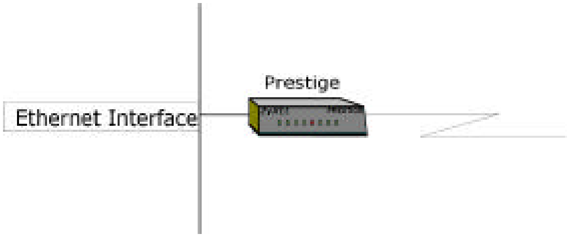
Perform the instructions in the following table to configure TCP/IP parameters for the Ethernet port.

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 [space bar] to select the RIP direction from **Both/None/In Only/ Out Only.**	**Both** (default)
Version	Press [space bar] to select the RIP version from **RIP-1/RIP-2B/ RIP-2M.**	**RIP-1** (default)
Edit IP Alias	Please refer to the next section.	
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 IP Alias

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



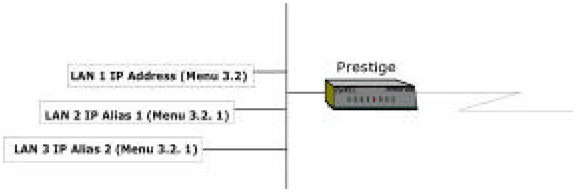
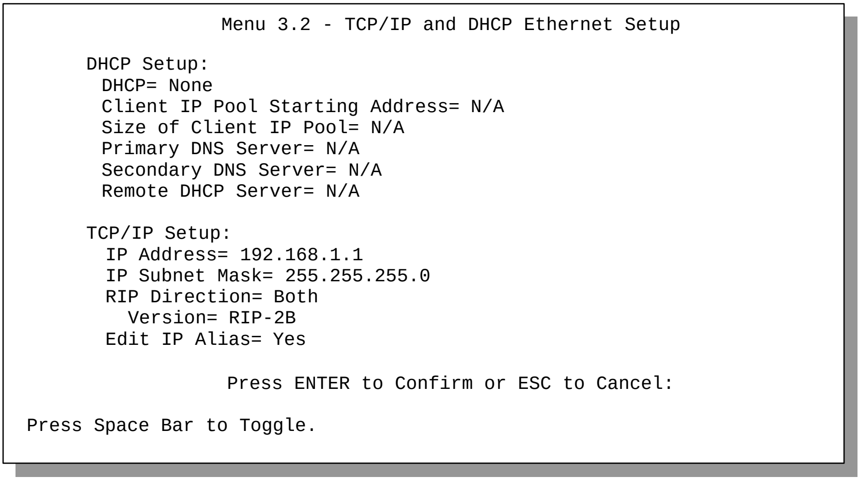

LAN 1 IP Address (Menu 3.2)
LAN 2 IP Alias 1 (Menu 3.2. 1)
LAN 3 IP Alias 2 (Menu 3.2. 1)
Prestige

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

Use Menu 3.2.1 to configure IP Alias on your Prestige.

3.5 IP Alias Setup

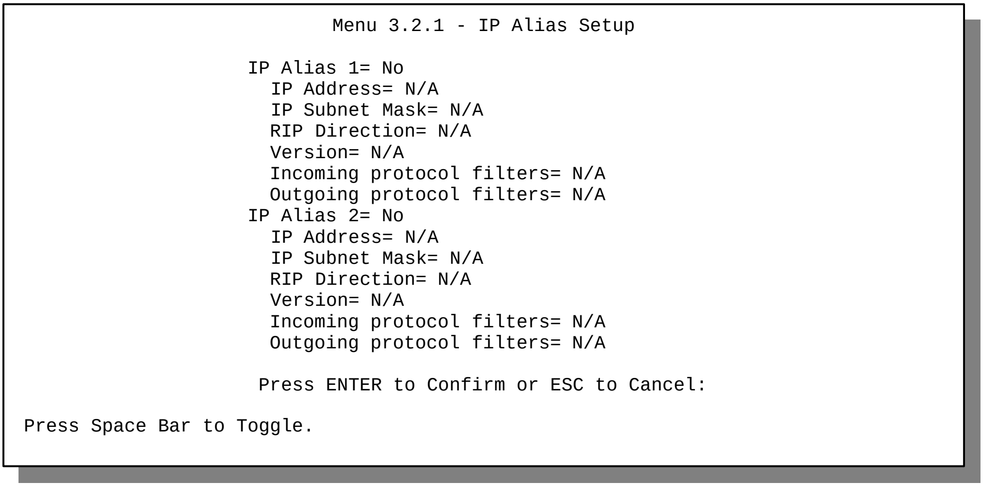
You must use **Menu 3.2** to configure the first network and move the cursor to **Edit IP Alias** field and toggle [space bar] to choose **Yes** and press [Enter] to configure the second and third network.



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

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

     TCP/IP Setup:
      IP Address= 192.168.1.1
      IP Subnet Mask= 255.255.255.0
      RIP Direction= Both
        Version= RIP-2B
      Edit IP Alias= Yes

                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

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

Pressing [Enter] opens **Menu 3.2.1 – IP Alias Setup**, as shown next.



```
                              Menu 3.2.1 - IP Alias Setup

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

                        Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 3-5 Menu 3.2.1 – IP Alias Setup

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

Table 3-3 IP Alias Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
IP Alias 1/2	Choose **Yes** to configure the LAN network for the Prestige.	**Yes/No**
IP Address	Enter the IP address of your Prestige in dotted decimal notation.	**192.168.2.1**
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige.	**255.255.255.0**
RIP Direction	Press [space bar] to select the RIP direction from **Both/In Only/Out Only.**	**Both**
Version	Press [space bar] to select the RIP version from **RIP-1/RIP-2B/RIP-2M.**	**RIP-1**
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the Prestige.	
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Prestige.	

When you have completed this menu, press [Enter] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [Esc] at any time to cancel.

3.6 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.

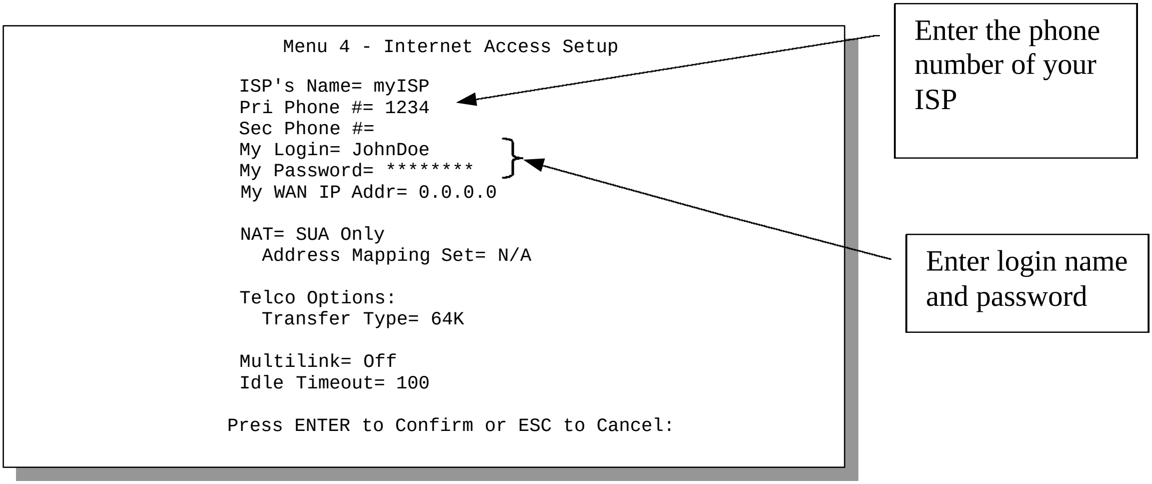
Table 3-4 Internet Account Information

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 shown in the following figure.

3.6.1 Sample Internet Access Configuration

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



```
     Menu 4 - Internet Access Setup

 ISP's Name= myISP
 Pri Phone #= 1234
 Sec Phone #=
 My Login= JohnDoe
 My Password= ********
 My WAN IP Addr= 0.0.0.0

 NAT= SUA Only
   Address Mapping Set= N/A

 Telco Options:
   Transfer Type= 64K

 Multilink= Off
 Idle Timeout= 100

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

Enter the phone number of your ISP

Enter login name and password

Figure 3-6 Menu 4 – Internet Access Setup

Table 3-5 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.
Pri Phone and Sec Phone #	Both the Primary and the Secondary Phone number refer to the number that the Prestige dials to connect to the ISP.
My Login	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	Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your Prestige. **NOTE:** This is the address assigned to your local Prestige WAN, not the remote router. If the remote router is a Prestige, then this entry determines the local Prestige **Rem IP Addr** in Menu 11.1.
NAT	Choose from **None**, **Full Feature** or **SUA Only**. *See ahead* for a full discussion of this new feature.
Address Mapping Set	A NAT Server Set is a list of LAN side servers mapped to external ports (similar to the old SUA menu). You may enter any server set number up to 10, but the first one is used for 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.** Options for this field are: **Off**/**BOD**/**Always**.
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.

Part II:

ADVANCED APPLICATIONS

Advanced Applications (Chapters 4 to 8) describe the advanced applications of your Prestige, such as Remote Node Configuration, Remote Node TCP/IP Configuration, Dial-in Server Configuration, NAT and Advanced Phone Services.

Chapter 4
Remote Node Configuration

This chapter covers the parameters that are protocol independent. The protocol-dependent configuration (TCP/IP) is covered in the next chapter.

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*.

4.1 Remote Node Setup

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

4.1.1 Minimum Toll Period

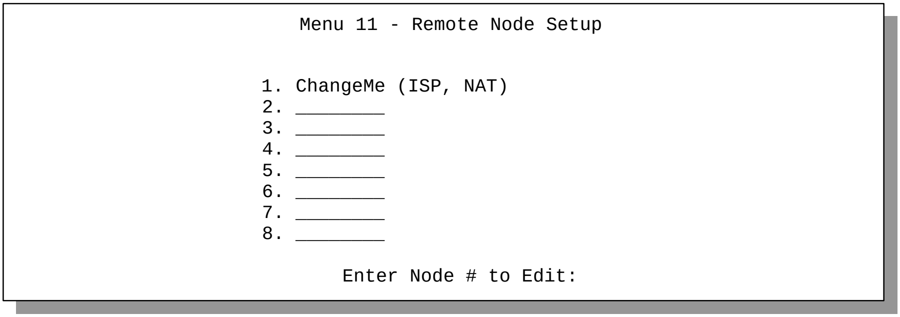
Phone calls are normally charged per basic time unit with the time being rounded up to the nearest unit when bills are calculated. For example, the Prestige may make a call but drop the call after 10 seconds (maybe there was no reply) but the call would still be charged at a minimum time unit, let us 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.

4.1.2 Remote Node Profile

To configure a remote node, follow these steps:

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

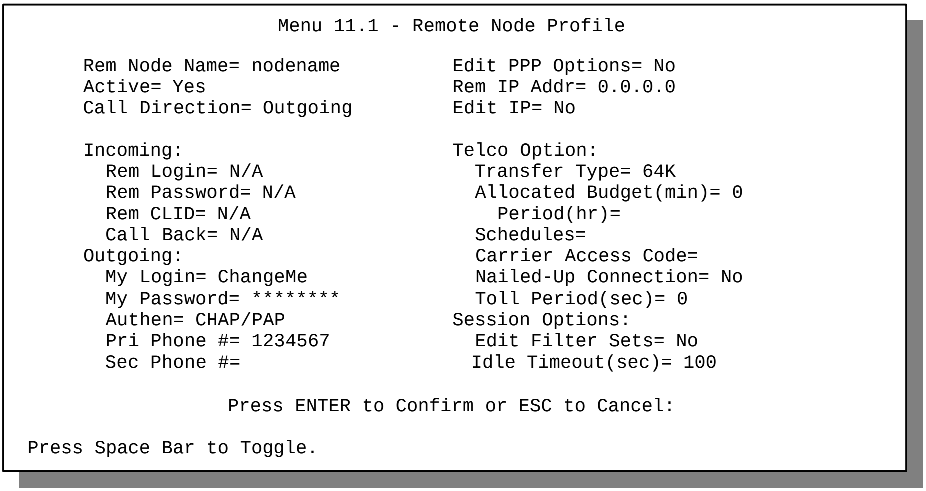
Step 2. When Menu 11 appears as shown in the following figure, enter the number of the remote node that you wish to configure.



```
                      Menu 11 - Remote Node Setup


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

                      Enter Node # to Edit:
```

Figure 4-1 Menu 11 – Remote Node Setup

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



```
                      Menu 11.1 - Remote Node Profile

       Rem Node Name= nodename          Edit PPP Options= No
       Active= Yes                      Rem IP Addr= 0.0.0.0
       Call Direction= Outgoing         Edit IP= No

       Incoming:                        Telco Option:
         Rem Login= N/A                   Transfer Type= 64K
         Rem Password= N/A                Allocated Budget(min)= 0
         Rem CLID= N/A                      Period(hr)=
         Call Back= N/A                   Schedules=
       Outgoing:                          Carrier Access Code=
         My Login= ChangeMe               Nailed-Up Connection= No
         My Password= ********            Toll Period(sec)= 0
         Authen= CHAP/PAP               Session Options:
         Pri Phone #= 1234567             Edit Filter Sets= No
         Sec Phone #=                     Idle Timeout(sec)= 100

                 Press ENTER to Confirm or ESC to Cancel:

  Press Space Bar to Toggle.
```

Figure 4-2 Menu 11.1 – Remote Node Profile

Table 4-1 Remote Node Profile Menu Fields

FIELD		DESCRIPTION	OPTIONS
Rem Node Name		This is a required field [?]. Enter a descriptive name for the remote node, for example, Corp. This field can be up to eight characters. This name must be unique from any other remote node name or remote dial-in user name.	
Active		Press [space bar] to toggle between **Yes** and **No**. Inactive nodes are displayed with a minus sign (–) at the beginning of the name in Menu 11.	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 set to **Both**.	**Both** **Incoming** **Outgoing**
Incoming:	Rem Login	Enter the login name that this remote node will use when it calls your Prestige. The login name in this field combined with the Rem Password will be used to authenticate this node.	
Incoming:	Rem 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 set to **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 Setup, 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 set to Required,	

FIELD	DESCRIPTION	OPTIONS
	the call will be dropped.	
Incoming: Call Back	This field is applicable only if **Call Direction** is set to **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 ahead).	**Yes/No**
Outgoing: My Login	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/PAP**
	● **CHAP** – accept CHAP only.	**CHAP**
	● **PAP** – accept PAP only.	**PAP**
Outgoing: Pri(mary) Sec(ondary) Phone #	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 [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]

FIELD	DESCRIPTION	OPTIONS
Rem IP Addr	This is a required field [?] if **Route** is set to **IP**. Enter the IP address of the remote gateway.	
Edit IP	Press [space bar] to select **Yes** and press [Enter] to go to Menu 11.3 – Remote Node Network Layer Options.	**No**/**Yes**
Telco Options:		
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**
Allocated Budget (min)	This field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 for no budget control.	Default = 0
Period (hr)	This field sets the time interval to reset the above outgoing call budget control.	
Schedules	Apply up to 4 schedule sets, separated by commas to your remote node here. Please see ahead for a full discussion on schedules.	
Carrier Access Code	In some European countries, you need to enter the access code number of your preferred telecommunications service provider. Your telephone company should supply you with this number.	
Nailed-up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. See the following section for more details.	**Yes/No**
Toll Period	This is the basic unit of time for charging purposes, e.g., 25 cents every 3 minutes – 3 minutes is the Toll Period.	
Session Options: Edit Filter Sets	Use [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 Options: 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 sec means the remote node will never be automatically disconnected.

FIELD	DESCRIPTION	OPTIONS
Once you have completed filling in Menu 11.1 – Remote Node Profile, press [Enter] at the message [Press ENTER to Confirm …] to save your configuration, or press [Esc] at any time to cancel.		

4.1.3 Outgoing Authentication Protocol

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

4.1.4 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.

4.1.5 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 in the following table:

Table 4-2 BTR vs MTR for BOD

BTR AND 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.

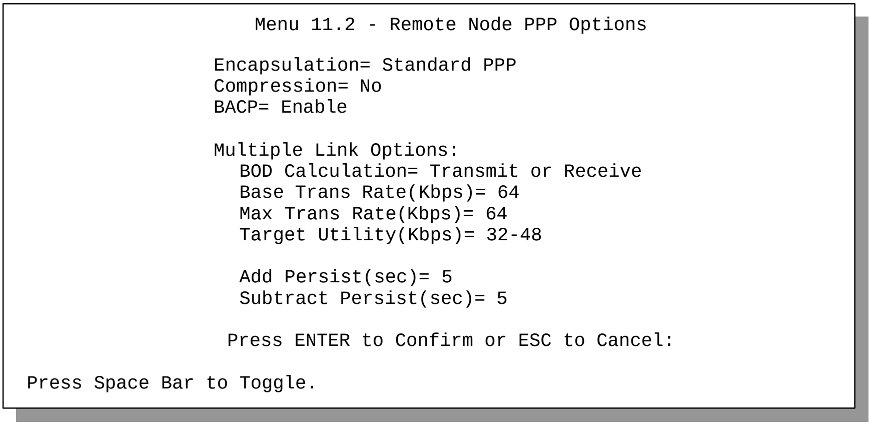
The **Target Utility** specifies the line utilization range at which you want the Prestige to add or subtract bandwidth. The range is 30 to 64 Kbps (kilobits per second). The parameters are separated by a '–'. For example, '30–60' means the add threshold is 30 Kbps and subtract threshold is 60 Kbps. 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 set through **Menu 11.2** – **Remote Node PPP Options**.

4.1.6 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 [space bar] to select **Yes**. Press [Enter] to open Menu 11.2, as shown next.



```
                   Menu 11.2 - Remote Node PPP Options

                Encapsulation= Standard PPP
                Compression= No
                BACP= Enable

                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 4-3 Menu 11.2 – Remote Node PPP Options

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

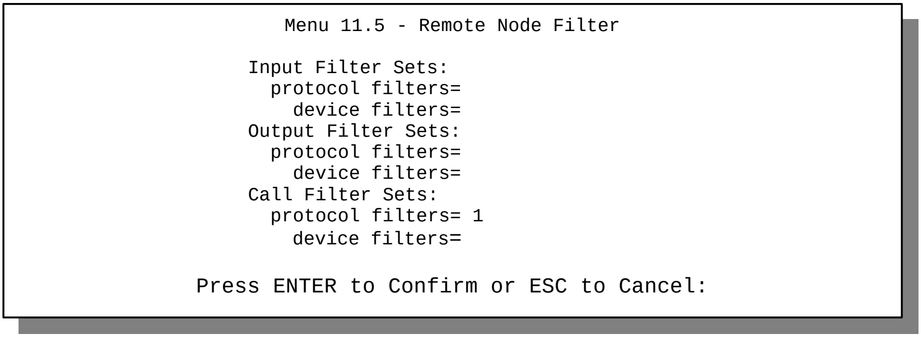
Table 4-3 Remote Node PPP Options Menu Fields

FIELD	DESCRIPTION	OPTION
Encapsulation	Select **CISCO PPP** only when this remote node is a Cisco machine; otherwise, select **Standard PPP**.	**Standard PPP** **CISCO PPP**
Compression	Turn on/off Stac Compression. The default for this field is **No**.	**Yes/No**
BACP	Your Prestige negotiates the Secondary Phone number for a dial-up line from the peer when BACP (Bandwidth Allocation Control Protocol) is enabled; otherwise it uses the Secondary Phone number set in Menu 11.1.	**Enable** (default)/ **Disable**
Multiple Link Options:		
BOD Calculation	Select the direction of the traffic you wish to use in determining when to add or subtract a link. Options for this field are: **Transmit or Receive**, **Transmit**, **Receive**.	**Transmit or Receive** (default**)**
Base Trans Rate (Kbps)	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 (Kbps)	Enter the maximum data transfer rate allowed for this remote node. This parameter is in kilobits per second.	**64/128**
Target Utility (Kbps)	Enter the two thresholds separated by a [–] for subtracting and adding the second port.	Default = 32–48
Add Persist	This parameter specifies the number of seconds where traffic is above the adding threshold before the Prestige will bring up the second link.	Default = 5 sec
Subtract Persist	This parameter specifies the number of seconds where traffic is below the subtraction threshold before your Prestige drops the second link.	Default = 5 sec
Once you have completed filling in Menu 11.2 – Remote Node PPP Options, press [Enter] at the message [Press ENTER to Confirm …] to save your configuration, or press [Esc] at any time to cancel.		

4.1.7 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 also 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. The default is no filters.

Note that spaces are accepted in this field. 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=

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

Figure 4-4 Menu 11.5 – Remote Node Filter

Chapter 5
Remote Node TCP/IP Configuration

This chapter shows you a sample LAN-to-LAN application and how to configure the TCP/IP parameters of a remote node.

5.1 LAN-to-LAN Application

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

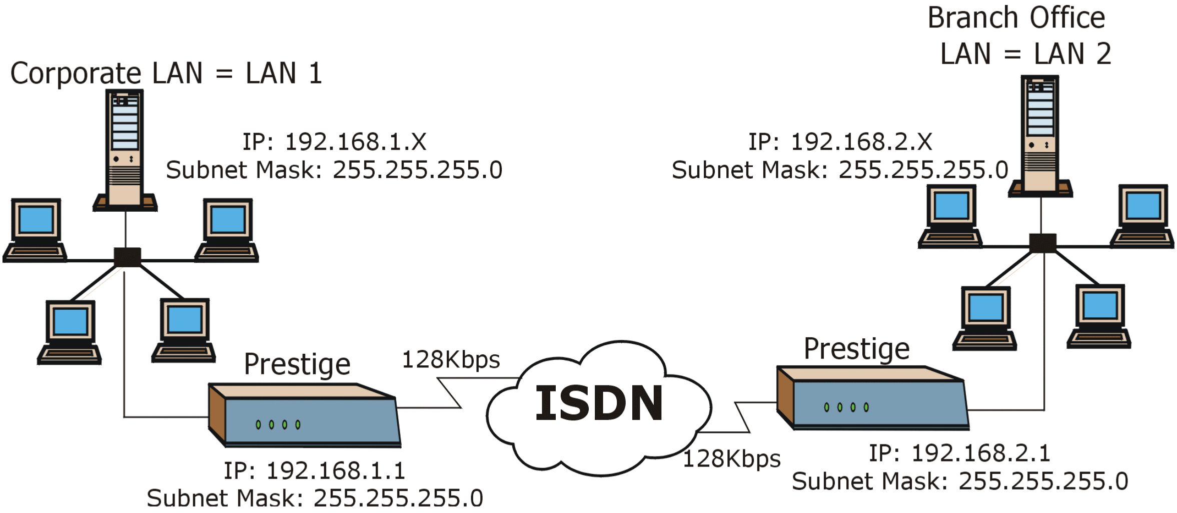
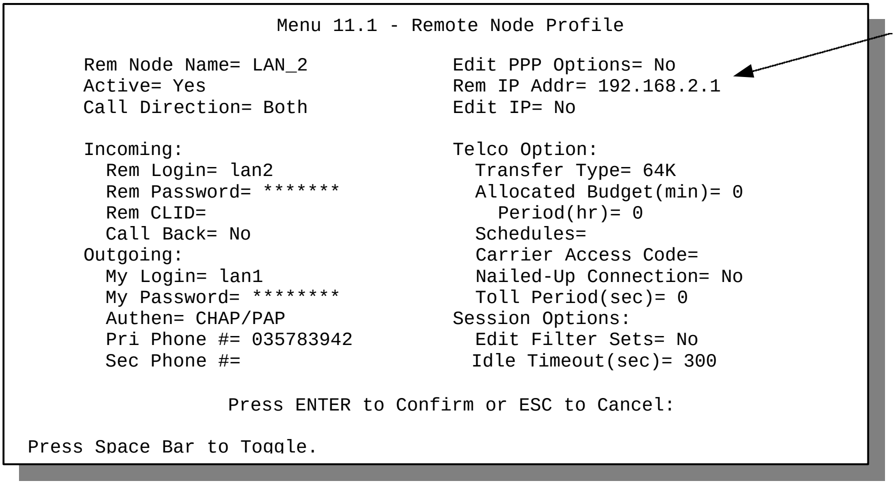


Figure 5-1 TCP/IP LAN-to-LAN Application

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

LAN 1 Setup

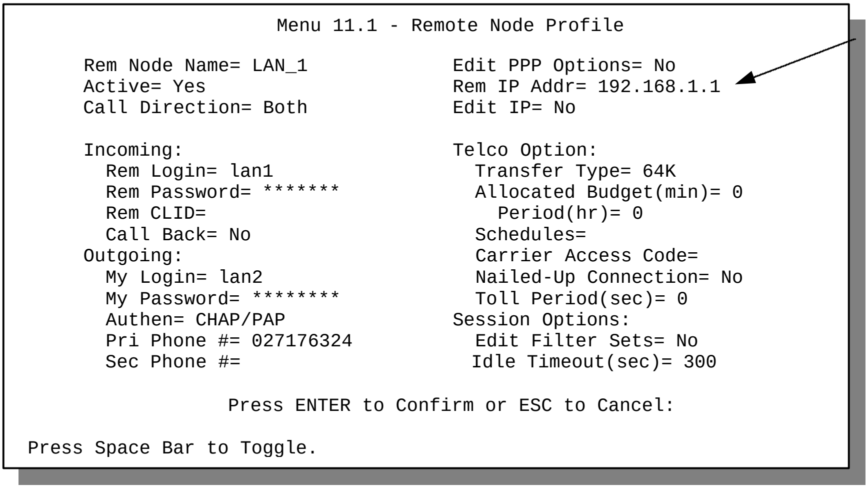


```
                        Menu 11.1 - Remote Node Profile

       Rem Node Name= LAN_2                Edit PPP Options= No
       Active= Yes                         Rem IP Addr= 192.168.2.1
       Call Direction= Both                Edit IP= No

       Incoming:                           Telco Option:
         Rem Login= lan2                     Transfer Type= 64K
         Rem Password= *******               Allocated Budget(min)= 0
         Rem CLID=                             Period(hr)= 0
         Call Back= No                       Schedules=
       Outgoing:                             Carrier Access Code=
         My Login= lan1                      Nailed-Up Connection= No
         My Password= ********               Toll Period(sec)= 0
         Authen= CHAP/PAP                  Session Options:
         Pri Phone #= 035783942              Edit Filter Sets= No
         Sec Phone #=                       Idle Timeout(sec)= 300

                    Press ENTER to Confirm or ESC to Cancel:

  Press Space Bar to Toggle.
```

IP address of the Prestige on LAN 2

Figure 5-2 LAN 1 Setup

LAN 2 Setup



```
                        Menu 11.1 - Remote Node Profile

       Rem Node Name= LAN_1                Edit PPP Options= No
       Active= Yes                         Rem IP Addr= 192.168.1.1
       Call Direction= Both                Edit IP= No

       Incoming:                           Telco Option:
         Rem Login= lan1                     Transfer Type= 64K
         Rem Password= *******               Allocated Budget(min)= 0
         Rem CLID=                             Period(hr)= 0
         Call Back= No                       Schedules=
       Outgoing:                             Carrier Access Code=
         My Login= lan2                      Nailed-Up Connection= No
         My Password= ********               Toll Period(sec)= 0
         Authen= CHAP/PAP                  Session Options:
         Pri Phone #= 027176324              Edit Filter Sets= No
         Sec Phone #=                       Idle Timeout(sec)= 300

                    Press ENTER to Confirm or ESC to Cancel:

  Press Space Bar to Toggle.
```

IP address of the Prestige on LAN 1

Figure 5-3 LAN 2 Setup

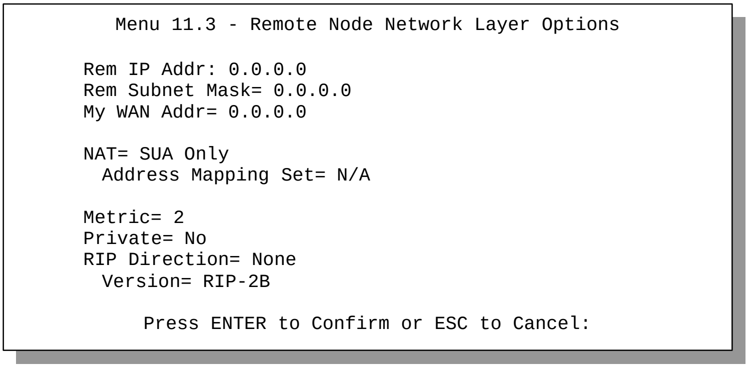
Additionally, you may also need to define static routes if some services reside beyond the immediate remote LAN.

5.2 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 next.

Move the cursor to the **Edit IP** field in **Menu 11** – **Remote Node Profile**, then press [space bar] to toggle and set the value to **Yes**. Press [Enter] to open **Menu 11.3** – **Network Layer Options**.



```
          Menu 11.3 - Remote Node Network Layer Options

       Rem IP Addr: 0.0.0.0
       Rem Subnet Mask= 0.0.0.0
       My WAN Addr= 0.0.0.0

       NAT= SUA Only
         Address Mapping Set= N/A

       Metric= 2
       Private= No
       RIP Direction= None
         Version= RIP-2B

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

Figure 5-4 Menu 11.3 – Remote Node TCP/IP Options

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

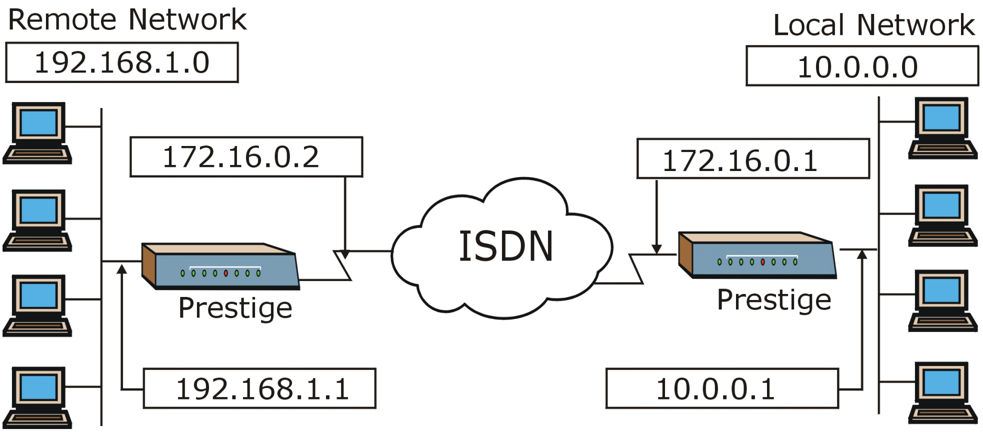


Figure 5-5 Sample IP Addresses for a TCPI/IP LAN-to-LAN Connection

To configure the TCP/IP parameters of a remote node, first configure the three fields in **Menu 11.1 – Remote Node Profile**, as shown in the following table. For more details on the IP Option fields, refer to *Chapter 3 – Internet Access Application.*

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

FIELD	DESCRIPTION	OPTION
Rem IP Addr	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 IP Addr** settings in **Menu 4**. For example, 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 Add** field. If the remote WAN IP is 0.0.0.0, then enter 192.168.1.1(the remote router's LAN IP) in the **Rem IP Addr** field).	
Edit IP	Press [space bar] to 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 5-2 TCP/IP Remote Node Configuration

FIELD	DESCRIPTION	OPTION
Rem IP Addr	This will show the IP address you entered for this remote node in the previous menu.	
Rem Subnet Mask	Enter the subnet mask for the remote network.	
My WAN Addr	Some implementations, especially the UNIX derivatives, require the ISDN 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 ISDN port of your Prestige. **NOTE**: This is the address assigned to your local Prestige WAN, not the remote router. If the remote router is a Prestige, then this entry determines the local Prestige **Rem IP Addr** in Menu 11.1.	
NAT	Choose from **None**, **Full Feature**, or **SUA Only**. See other sections for a full discussion of this new feature.	**Full Feature/ SUA Only/None**
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 for SUA only.	
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	**1** to **15**
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.	**Yes/No**
RIP Direction	Press [space bar] to select from **Both**/**In Only**/**Out Only/None**.	**None** (default)
Version	Press [space bar] to select the RIP version from **RIP-1/ RIP-2B/RIP-2M.**	**RIP-2B** (default)

FIELD	DESCRIPTION	OPTION
Once you have completed filling in the Remote Node Network Layer Options menu, press [Enter] to return to Menu 11.1. Press [Enter] at the message [Press ENTER to Confirm . . .] to save your configuration, or press [Esc] at any time to cancel.		

5.2.1 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 does not 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.

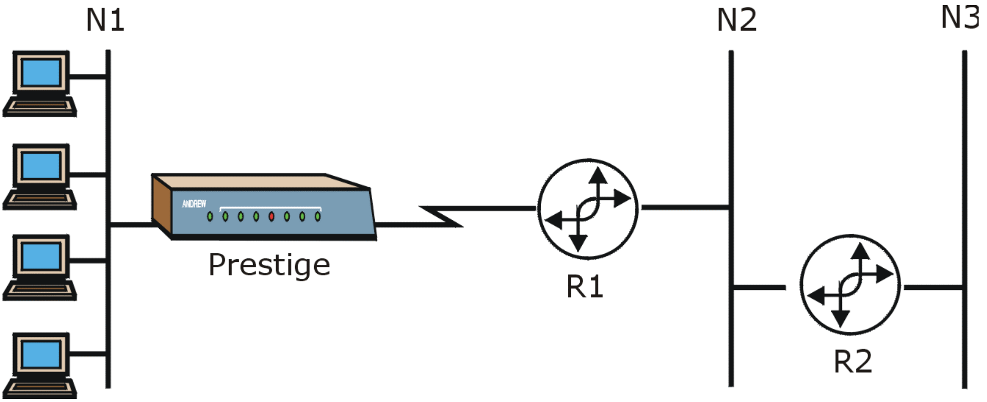
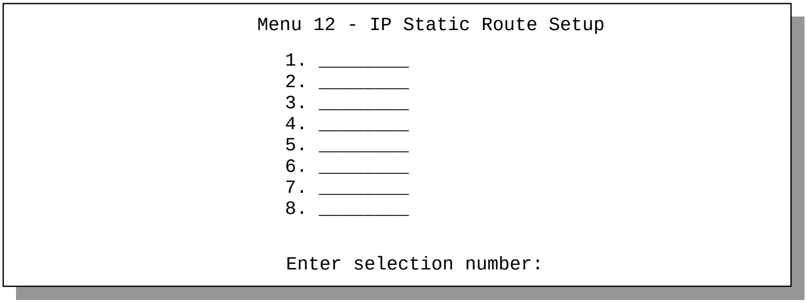


Figure 5-6 Sample Static Routing Topology

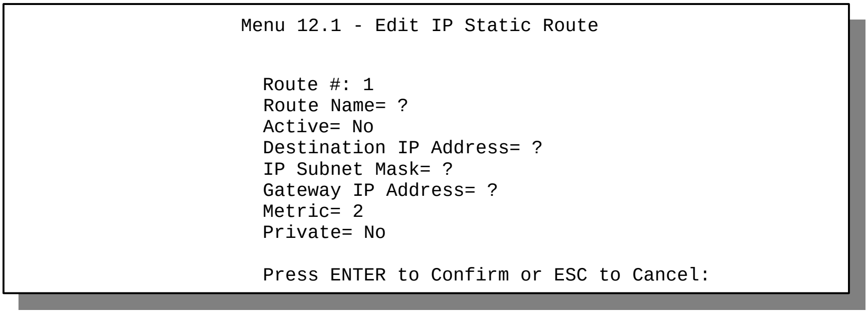
To configure an IP static route, use **Menu 12 – IP Static Route Setup**, as displayed next.



```
                    Menu 12 - IP Static Route Setup

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


                      Enter selection number:
```

Figure 5-7 Menu 12 – IP Static Route Setup

From Menu 12, select one of the available IP static routes to open **Menu 12.1 – Edit IP Static Route**, as shown next.



```
                    Menu 12.1 - Edit IP Static Route


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

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

Figure 5-8 Edit IP Static Route

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

Table 5-3 Edit IP Static Route Menu Fields

FIELD	DESCRIPTION
Route 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

FIELD	DESCRIPTION
	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	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and is not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.

Chapter 6
Dial-in Server Configuration

This chapter shows you how to 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 next table.

Table 6-1 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 User Setup (Menu 13).	Each remote node can have its own set of parameters such as Bandwidth On Demand, Protocol, Security, etc.

The following sections give two examples of how your Prestige can be configured as a dial-in server.

6.1 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 User Setup to set the operational parameters for all dial-in users.

An example of remote access server for telecommuters is shown next.

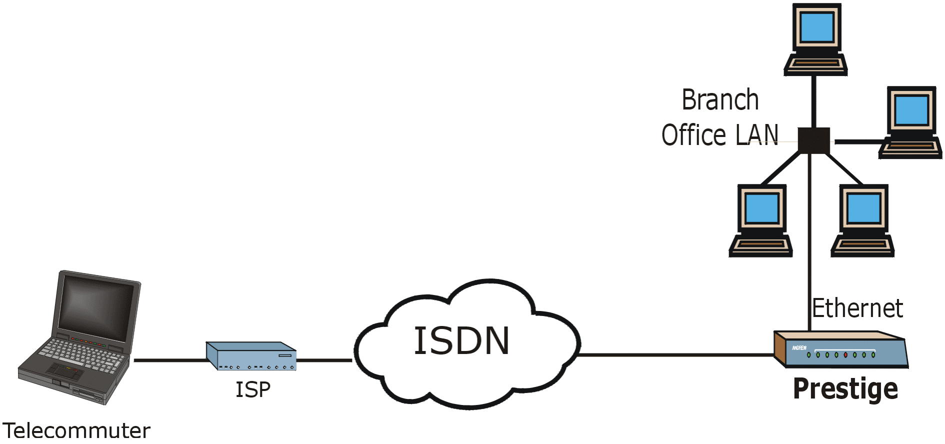


Figure 6-1 Example of Telecommuting

6.2 LAN-to-LAN Server Application

Your Prestige can also be used as a dial-in server for LAN-to-LAN application to provide access for the workstations on a remote network. For your Prestige to be set up as a LAN-to-LAN server, you need to configure the Default Dial-in User 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 4 – Remote Node Configuration*). An example of your Prestige being used as a LAN-to-LAN server is shown as follows.

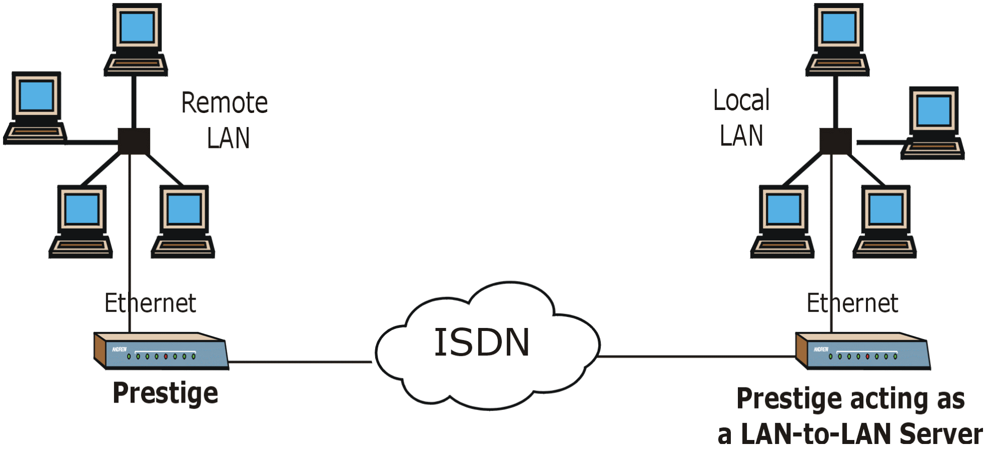


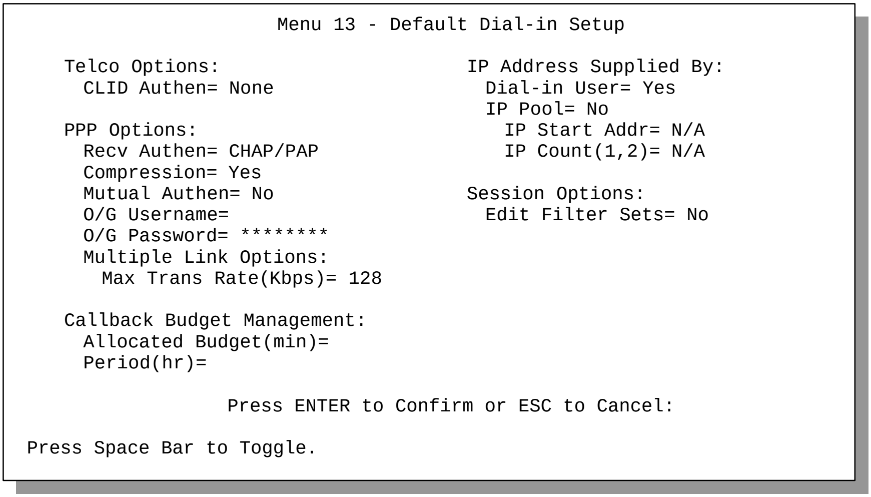
Figure 6-2 Example of a LAN-to-LAN Server Application

6.3 Default Dial-in User 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 the parameters from that particular remote node.

6.3.1 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 Username** 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 the callback feature.



```
                         Menu 13 - Default Dial-in Setup

    Telco Options:                          IP Address Supplied By:
      CLID Authen= None                       Dial-in User= Yes
                                              IP Pool= No
    PPP Options:                                IP Start Addr= N/A
      Recv Authen= CHAP/PAP                     IP Count(1,2)= N/A
      Compression= Yes
      Mutual Authen= No                     Session Options:
      O/G Username=                           Edit Filter Sets= No
      O/G Password= ********
      Multiple Link Options:
        Max Trans Rate(Kbps)= 128

    Callback Budget Management:
      Allocated Budget(min)=
      Period(hr)=

                     Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 6-3 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 following table describes and contains information on how to configure each parameter in **Menu 13 – Default Dial-in Setup**.

Table 6-2 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 **No**.	**Yes/No**
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 Username	Enter in the login name to be used to respond to the peer's authentication request.	

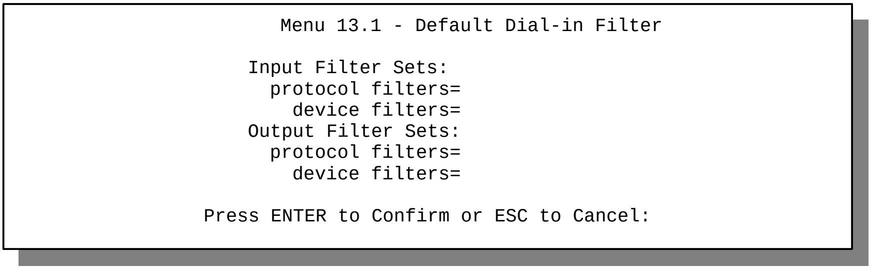
FIELD	DESCRIPTION	OPTIONS
O/G Password	Enter in the outgoing password to be used to respond to the peer's authentication request.	
Multiple Link Options:		
Max Trans Rate(Kbps)	Enter the maximum data transfer rate between your Prestige and the remote dial-in user. **64** – At most, one B channel is used. **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.	**0** (default)
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.	**Yes** (default)
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)
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. The IP start address is the start of a series of consecutive IP addresses.	
	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	

FIELD	DESCRIPTION	OPTIONS
IP Count (1, 2)	192.68.135.5 and 192.68.135.6. The IP count is the number of consecutive IP addresses allowed.	**1, 2**
Session Options: Edit Filter Sets	Select **Yes,** then press [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:** Spaces and [–] symbol are accepted in this field. For more information on customizing your filter sets, *see Chapter 9 – Filter Configuration*. The default is blank, i.e., no filters.	**No** (default)
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.		

6.3.2 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.*



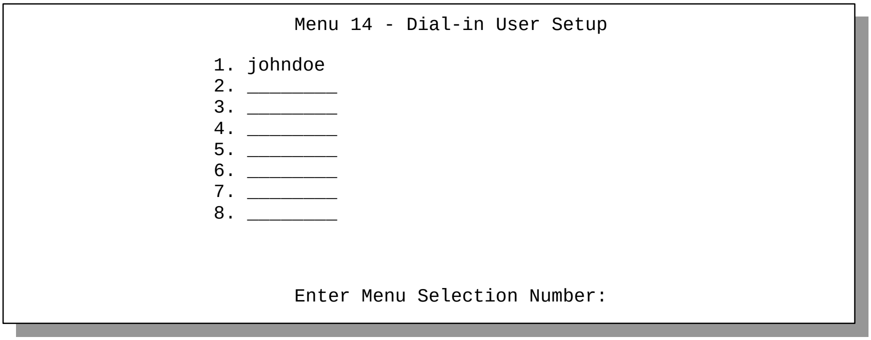
```
                Menu 13.1 - Default Dial-in Filter

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

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

Figure 6-4 Default Dial-in Filter

6.4 Dial-In Users Setup

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

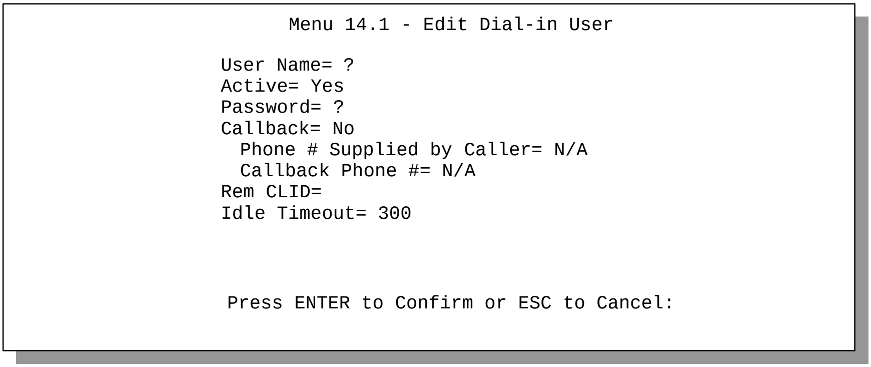
Step 1. From the Main Menu, enter 14 to go to **Menu 14** – **Dial-in User Setup**, as shown in the next figure.



```
                    Menu 14 - Dial-in User Setup

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



                    Enter Menu Selection Number:
```

Figure 6-5 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 next.



```
                    Menu 14.1 - Edit Dial-in User

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



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

Figure 6-6 Edit Dial-in User

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

Table 6-3 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.	

FIELD	DESCRIPTION	OPTION
	Inactive users are displayed with a [–] (minus sign) at the beginning of the name in Menu 14.	**Yes/No**
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 ahead). ● **No** – The default is no callback. ● **Optional** – The user can choose to disable callback. ● **Mandatory** – The user cannot disable callback.	**No** (default) **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.	**No** (default) **Yes**
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.	
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).	300 seconds (default)
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.		

6.4.1 Remote Access Under Windows®

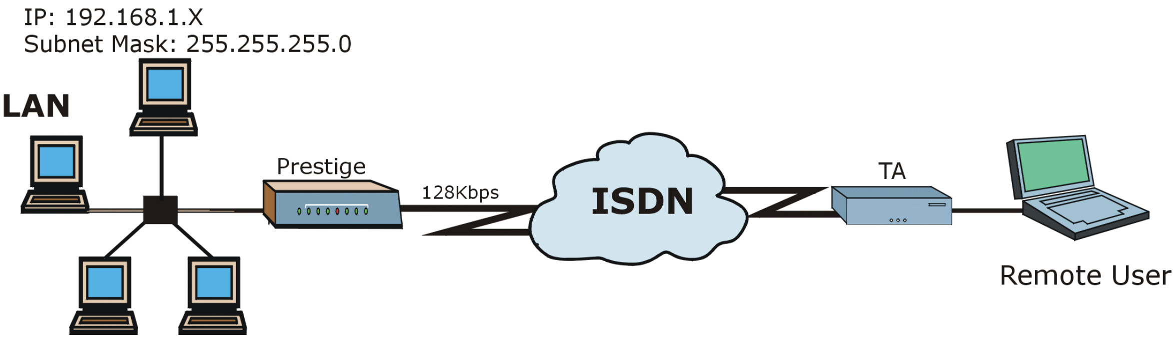
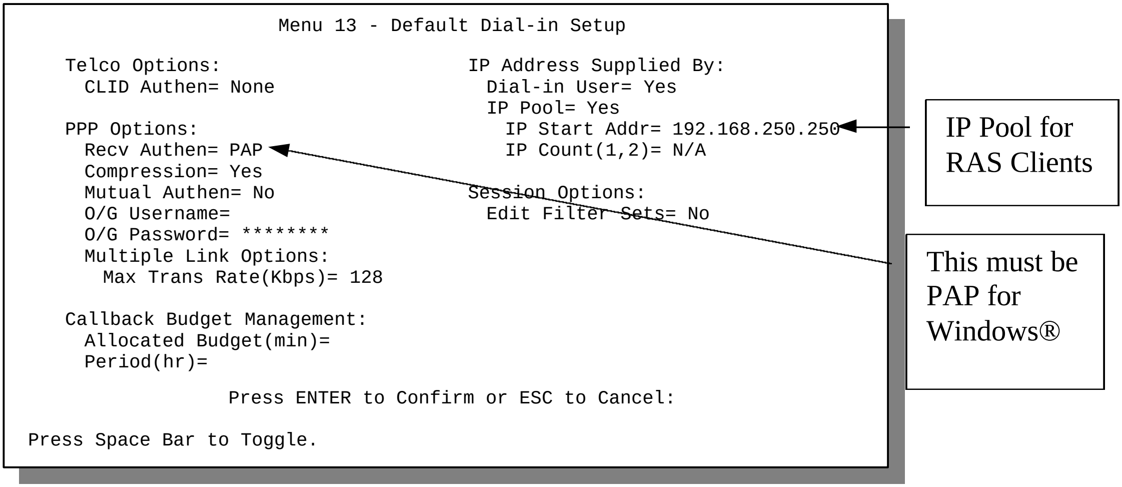


Figure 6-7 Sample Remote Access

Configuring Your Prestige

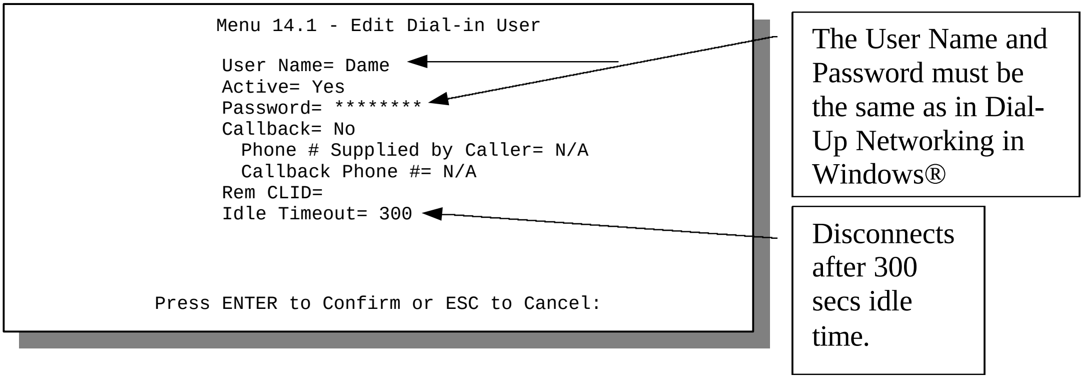


```
                         Menu 13 - Default Dial-in Setup

     Telco Options:                           IP Address Supplied By:
       CLID Authen= None                        Dial-in User= Yes
                                                IP Pool= Yes
     PPP Options:                                 IP Start Addr= 192.168.250.250
       Recv Authen= PAP                           IP Count(1,2)= N/A
       Compression= Yes
       Mutual Authen= No                      Session Options:
       O/G Username=                            Edit Filter Sets= No
       O/G Password= ********
       Multiple Link Options:
         Max Trans Rate(Kbps)= 128

     Callback Budget Management:
       Allocated Budget(min)=
       Period(hr)=

                    Press ENTER to Confirm or ESC to Cancel:

  Press Space Bar to Toggle.
```

IP Pool for RAS Clients

This must be PAP for Windows®

Figure 6-8 Configuring Menu 13 for Remote Access



```
                   Menu 14.1 - Edit Dial-in User

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



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

The User Name and Password must be the same as in Dial-Up Networking in Windows®

Disconnects after 300 secs idle time.

Figure 6-9 Edit Dial-in-User for RAS

NOTE: The caller always controls Idle Timeout, so this field does not apply when there is callback.

6.4.2 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.

6.4.3 Callback

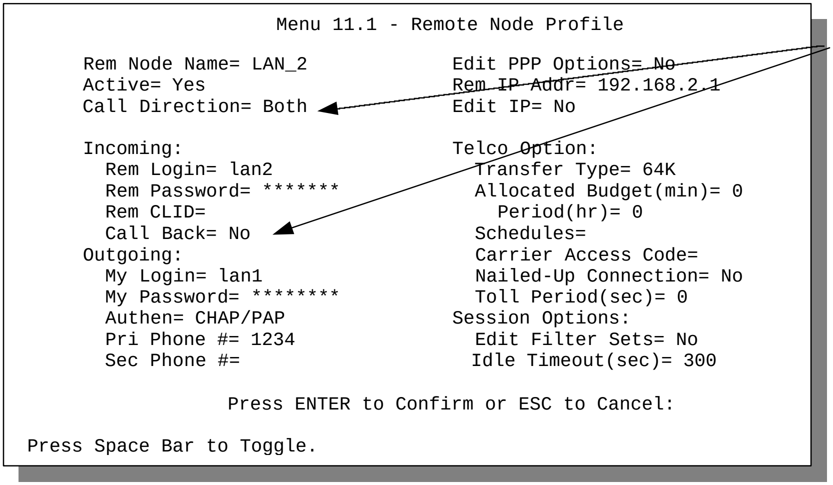
Callback serves two purposes. One is security. When set to callback to a fixed number, an intruder will not gain access to your network even if he/she stole the password from your user, because the Prestige always calls back to the pre-configured number.

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.

Configuring the Prestige for Callback

In this scenario, LAN 1 first calls LAN 2, then LAN 2 calls back to LAN 1. These are the respective SMT menus.

LAN 1

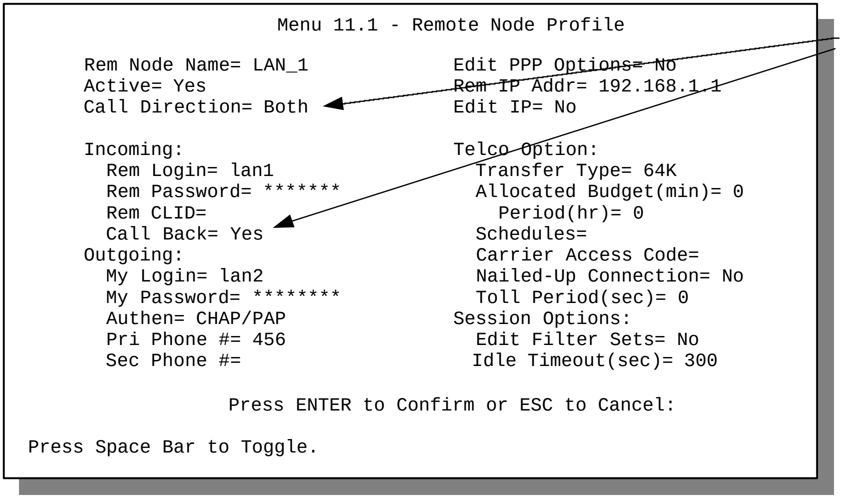


```
                        Menu 11.1 - Remote Node Profile

       Rem Node Name= LAN_2                Edit PPP Options= No
       Active= Yes                         Rem IP Addr= 192.168.2.1
       Call Direction= Both                Edit IP= No

       Incoming:                           Telco Option:
         Rem Login= lan2                     Transfer Type= 64K
         Rem Password= *******               Allocated Budget(min)= 0
         Rem CLID=                             Period(hr)= 0
         Call Back= No                       Schedules=
       Outgoing:                             Carrier Access Code=
         My Login= lan1                      Nailed-Up Connection= No
         My Password= ********               Toll Period(sec)= 0
         Authen= CHAP/PAP                  Session Options:
         Pri Phone #= 1234                   Edit Filter Sets= No
         Sec Phone #=                       Idle Timeout(sec)= 300

                    Press ENTER to Confirm or ESC to Cancel:

  Press Space Bar to Toggle.
```

Set **Call Direction** and **Call Back** to **Both** and **No** respectively.

Figure 6-10 LAN 1 LAN-to-LAN Application

LAN 2



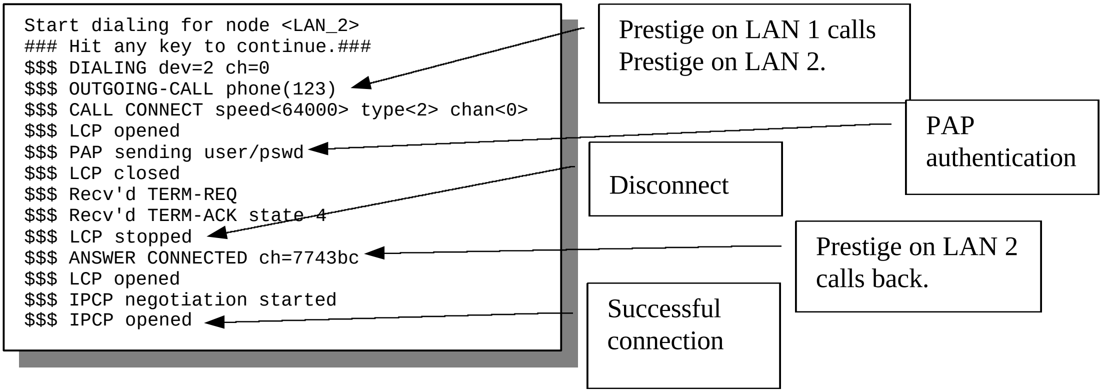
```
                        Menu 11.1 - Remote Node Profile

       Rem Node Name= LAN_1                Edit PPP Options= No
       Active= Yes                         Rem IP Addr= 192.168.1.1
       Call Direction= Both                Edit IP= No

       Incoming:                           Telco Option:
         Rem Login= lan1                     Transfer Type= 64K
         Rem Password= *******               Allocated Budget(min)= 0
         Rem CLID=                             Period(hr)= 0
         Call Back= Yes                      Schedules=
       Outgoing:                             Carrier Access Code=
         My Login= lan2                      Nailed-Up Connection= No
         My Password= ********               Toll Period(sec)= 0
         Authen= CHAP/PAP                  Session Options:
         Pri Phone #= 456                    Edit Filter Sets= No
         Sec Phone #=                       Idle Timeout(sec)= 300

                    Press ENTER to Confirm or ESC to Cancel:

  Press Space Bar to Toggle.
```

Set **Call Direction** and **Call Back** to **Both** and **Yes** respectively.

Figure 6-11 LAN 2 LAN-to-LAN Application

Testing Callback With Your Connection

Go to Menu 24.4.5 of the Prestige on LAN 1 and enter the numbers that correspond to the menu in LAN 1 above.



```
Start dialing for node <LAN_2>
### Hit any key to continue.###
$$$ DIALING dev=2 ch=0
$$$ OUTGOING-CALL phone(123)
$$$ CALL CONNECT speed<64000> type<2> chan<0>
$$$ LCP opened
$$$ PAP sending user/pswd
$$$ LCP closed
$$$ Recv'd TERM-REQ
$$$ Recv'd TERM-ACK state 4
$$$ LCP stopped
$$$ ANSWER CONNECTED ch=7743bc
$$$ LCP opened
$$$ IPCP negotiation started
$$$ IPCP opened
```

Prestige on LAN 1 calls Prestige on LAN 2.

PAP authentication

Disconnect

Prestige on LAN 2 calls back.

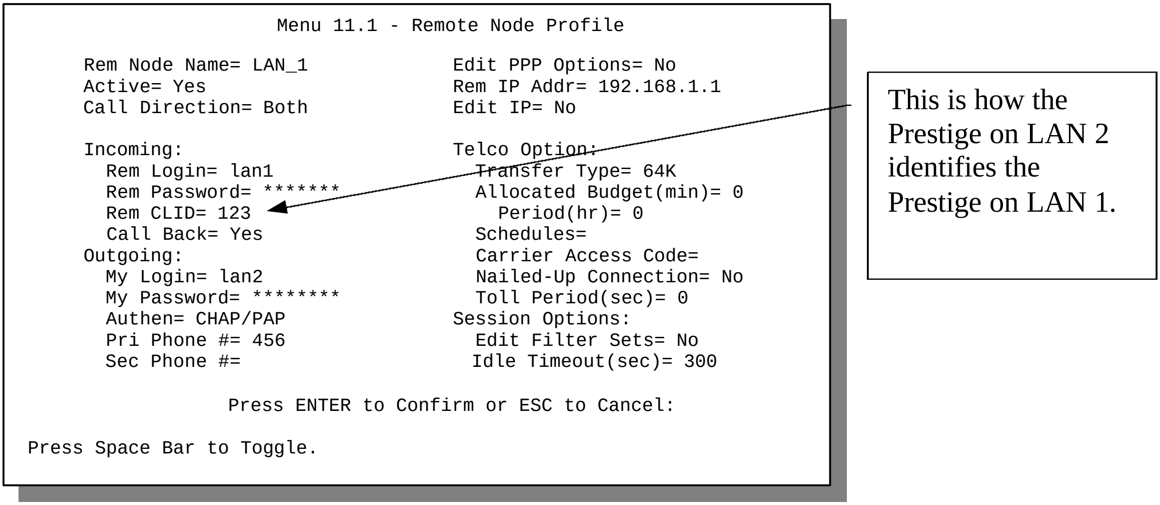
Successful connection

Figure 6-12 Testing Callback With Your Connection

6.4.4 Configuring the Prestige for Callback With CLID

The only difference between callback with CLID (Calling Line Identification) and callback described above is that you do not pay for the first call, i.e., when the Prestige on LAN 1 calls the Prestige on LAN 2. The Prestige (LAN 2) looks at the ISDN D-channel and verifies that the calling number corresponds with that configured in Menu 11. If they do, the Prestige (LAN 2) hangs up and calls the Prestige on LAN 1 back.

Prestige on LAN 2

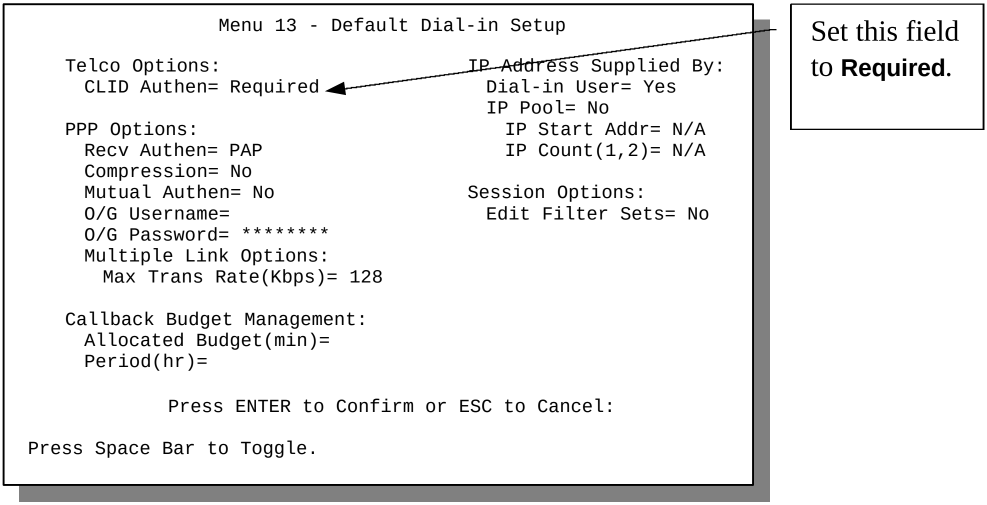


```
                      Menu 11.1 - Remote Node Profile

     Rem Node Name= LAN_1              Edit PPP Options= No
     Active= Yes                       Rem IP Addr= 192.168.1.1
     Call Direction= Both              Edit IP= No

     Incoming:                         Telco Option:
       Rem Login= lan1                   Transfer Type= 64K
       Rem Password= *******             Allocated Budget(min)= 0
       Rem CLID= 123                       Period(hr)= 0
       Call Back= Yes                    Schedules=
     Outgoing:                           Carrier Access Code=
       My Login= lan2                    Nailed-Up Connection= No
       My Password= ********             Toll Period(sec)= 0
       Authen= CHAP/PAP                Session Options:
       Pri Phone #= 456                  Edit Filter Sets= No
       Sec Phone #=                     Idle Timeout(sec)= 300

                  Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

This is how the Prestige on LAN 2 identifies the Prestige on LAN 1.

Figure 6-13 Callback With CLID Configuration

Menu 13



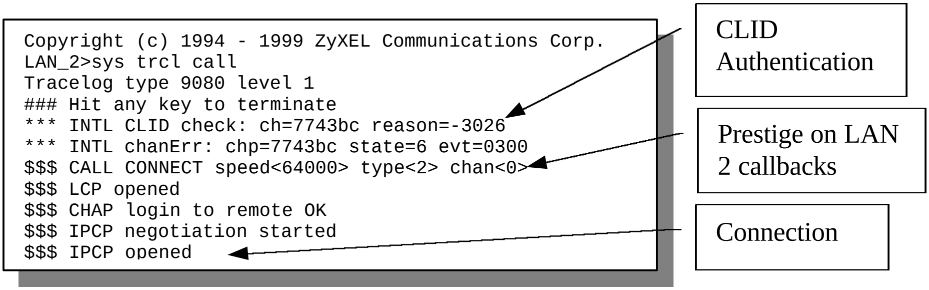
```
                   Menu 13 - Default Dial-in Setup

     Telco Options:                         IP Address Supplied By:
       CLID Authen= Required                  Dial-in User= Yes
                                              IP Pool= No
     PPP Options:                               IP Start Addr= N/A
       Recv Authen= PAP                         IP Count(1,2)= N/A
       Compression= No
       Mutual Authen= No                    Session Options:
       O/G Username=                          Edit Filter Sets= No
       O/G Password= ********
       Multiple Link Options:
         Max Trans Rate(Kbps)= 128

     Callback Budget Management:
       Allocated Budget(min)=
       Period(hr)=

              Press ENTER to Confirm or ESC to Cancel:

  Press Space Bar to Toggle.
```

Set this field to **Required.**

Figure 6-14 Configuring CLID With Callback

Testing Your Connection With Callback and CLID

Go to Menu 24.8 (Prestige on LAN 2) and type "sys trcl call". The Prestige displays all communication traces as shown in the next figure. If CLID authentication fails, this means that the calling number does not match the **Rem CLID** number in Menu 11.1.



```
Copyright (c) 1994 - 1999 ZyXEL Communications Corp.
LAN_2>sys trcl call
Tracelog type 9080 level 1
### Hit any key to terminate
*** INTL CLID check: ch=7743bc reason=-3026
*** INTL chanErr: chp=7743bc state=6 evt=0300
$$$ CALL CONNECT speed<64000> type<2> chan<0>
$$$ LCP opened
$$$ CHAP login to remote OK
$$$ IPCP negotiation started
$$$ IPCP opened
```

CLID Authentication

Prestige on LAN 2 callbacks

Connection

Figure 6-15 Callback and CLID Connection Test

Chapter 7
NAT (Network Address Translation)

This chapter discusses how to configure NAT on the Prestige.

7.1 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 as 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 ahead), 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).*

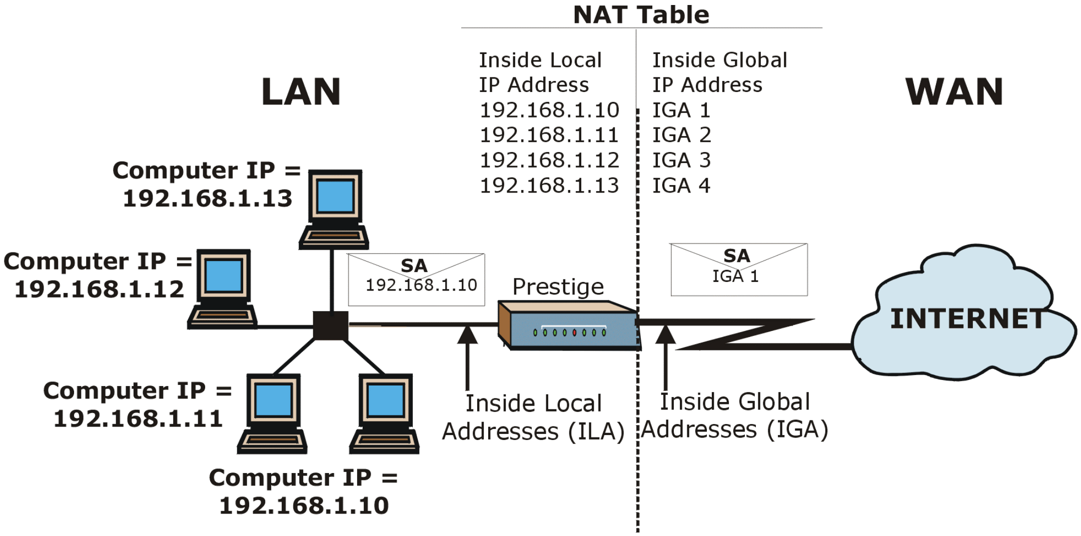
7.1.1 Advantages of NAT

- 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.

7.1.2 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.



NAT Table

Inside Local IP Address	Inside Global IP Address
192.168.1.10	IGA 1
192.168.1.11	IGA 2
192.168.1.12	IGA 3
192.168.1.13	IGA 4

LAN
WAN
Computer IP = 192.168.1.13
Computer IP = 192.168.1.12
Computer IP = 192.168.1.11
Computer IP = 192.168.1.10
SA 192.168.1.10
Prestige
SA IGA 1
INTERNET
Inside Local Addresses (ILA)
Inside Global Addresses (IGA)

Figure 7-1 How NAT Works

7.1.3 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 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.

NOTE: 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 7-1 NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION
One-to-One	ILA1←→ IGA1	1:1

Many-to-One (SUA/PAT)	ILA1←→ IGA1
	ILA2←→ IGA1
	…
		M:1

Many-to-Many Overload	ILA1←→ IGA1
	ILA2←→ IGA2
	ILA3←→ IGA1
	ILA4←→ IGA2
	…
		M:M Ov

Many-to-Many No Overload	ILA1←→ IGA1
	ILA2←→ IGA2
	ILA3←→ IGA3
	…
		M:M No Ov

Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1	Server

7.2 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.

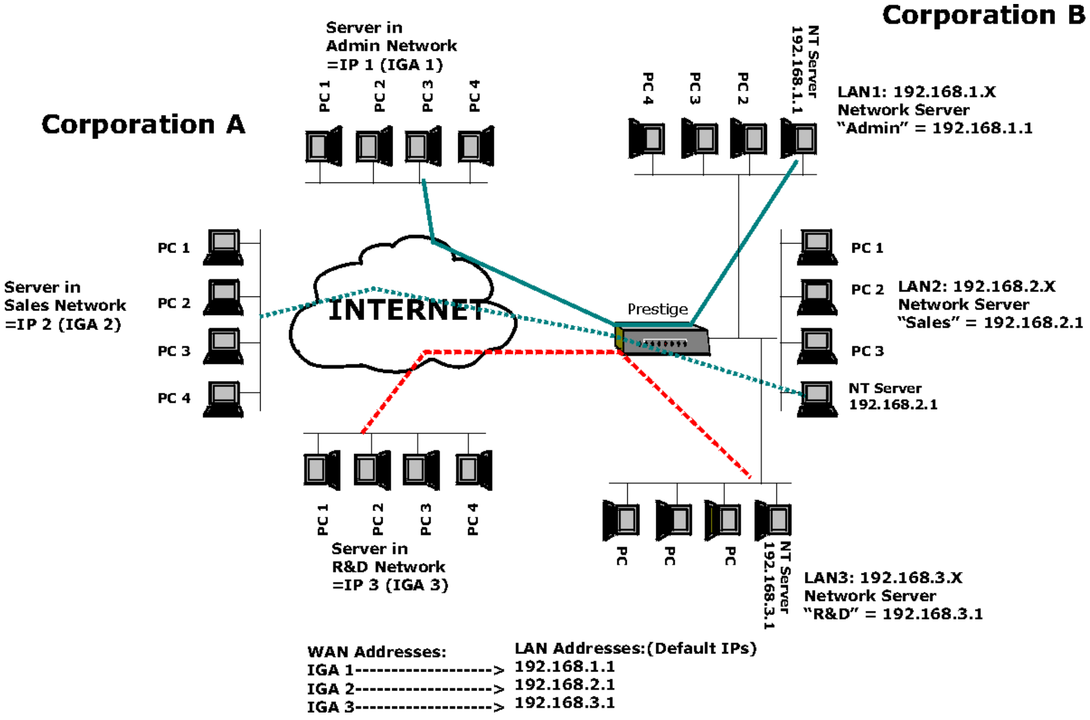


Figure 7-2 NAT Application

7.3 SUA (Single User Account) Versus NAT

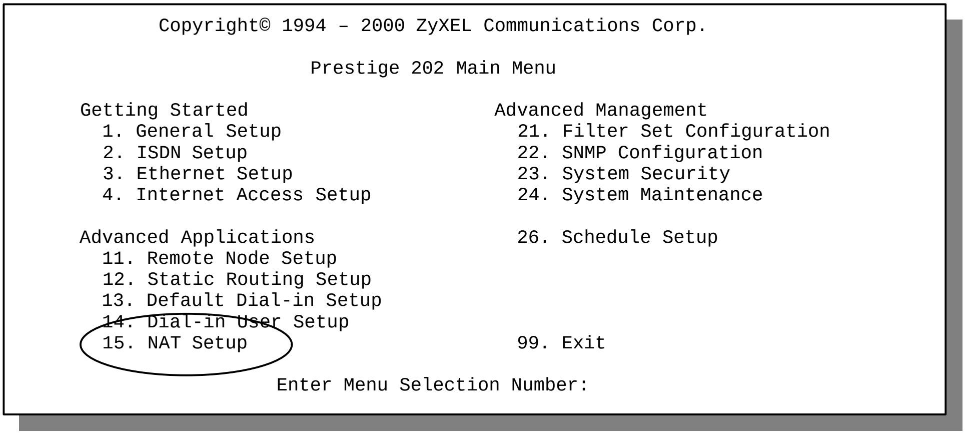
SUA (Single User Account) in previous ZyNOS versions is a NAT set with 2 rules, Many-to-One and Server. See *Section 7.5.1* for a detailed description of the NAT set for SUA. The Prestige now has **Full Feature** NAT support to map global IP addresses to local IP addresses of clients or servers using all mapping types as outlined in *Table 7-1 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-One port mapping set, sufficient for most purposes (*see other section* for some examples) and helpful to people already familiar with SUA in previous ZyNOS versions.

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

7.4 SMT Menus

7.4.1 NAT Setup in the Main Menu

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

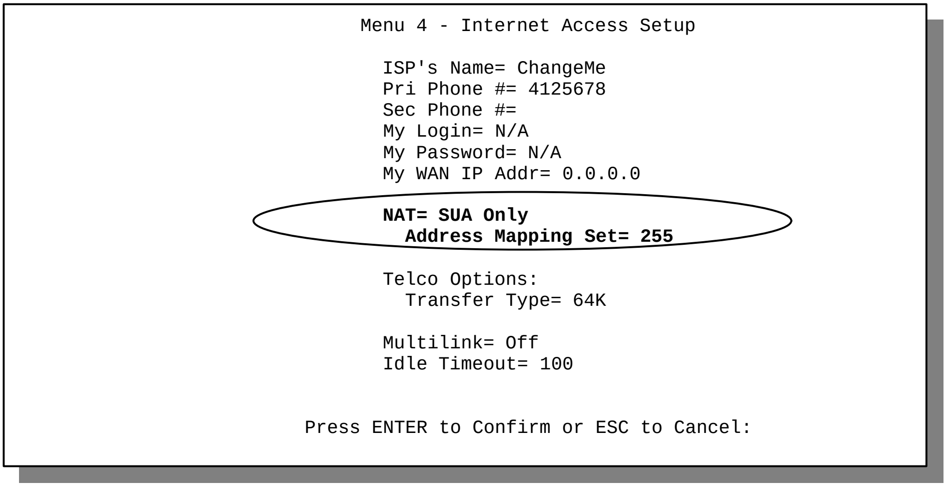


```
           Copyright© 1994 – 2000 ZyXEL Communications Corp.

                          Prestige 202 Main Menu

    Getting Started                       Advanced Management
      1. General Setup                      21. Filter Set Configuration
      2. ISDN Setup                         22. SNMP Configuration
      3. Ethernet Setup                     23. System Security
      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 7-3 NAT in the Main Menu

7.4.2 Applying NAT in the SMT Menus

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



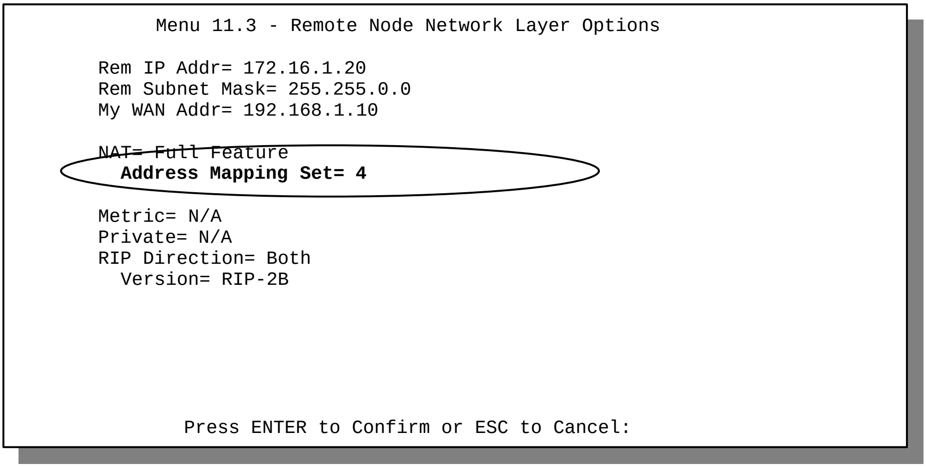
```
                         Menu 4 - Internet Access Setup

                           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

                           Telco Options:
                             Transfer Type= 64K

                           Multilink= Off
                           Idle Timeout= 100


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

Figure 7-4 Applying NAT for Internet Access

This figure shows you how to 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 [space bar] 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 Addr= 172.16.1.20
        Rem 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





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

Figure 7-5 Applying NAT to the Remote Node

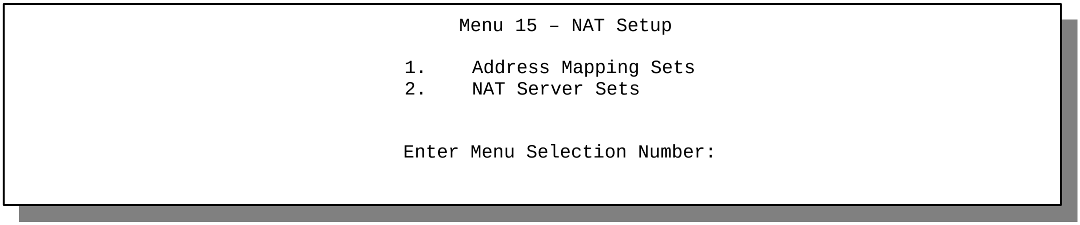
The following table describes the options for Network Address Translation.

Table 7-2 Applying NAT in Menus 4 and 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 7.5.1* for further details). You can configure any of the 5 mapping types described in *Table 7-1 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 7.5.1*). It is a convenient, pre-configured, read only Many-to-One port mapping set, sufficient for most purposes and helpful to people already familiar with SUA in previous ZyNOS versions. **NOTE:** 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 for SUA only.	

7.5 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:
```

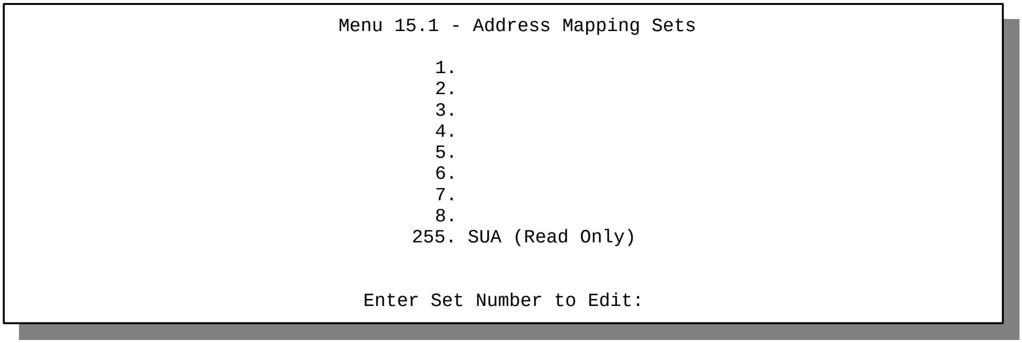
Figure 7-6 Menu 15 NAT Setup

7.5.1 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 7-3*. When you select **SUA Only**, the SMT will use the pre-configured Set 255 (read only) – *see Section 7.2.*

The NAT Server set is a list of LAN side servers mapped to external ports. To use this set, a server rule must be set up inside the NAT Address Mapping set. Please *see Section 7.5.2* for further information on these menus.

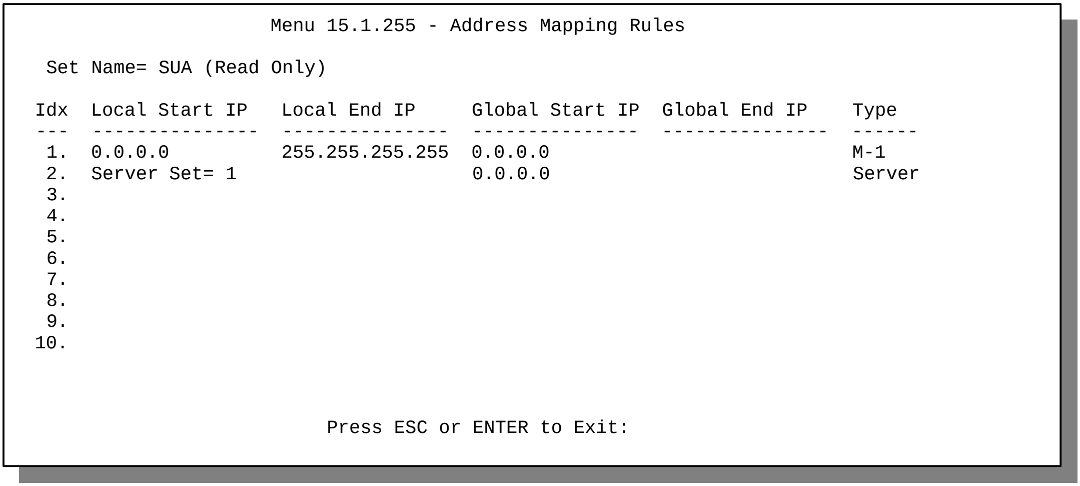
Enter 1 to bring up **Menu 15.1 – Address Mapping Sets**.



```
                    Menu 15.1 - Address Mapping Sets

                                1.
                                2.
                                3.
                                4.
                                5.
                                6.
                                7.
                                8.
                              255. SUA (Read Only)


                      Enter Set Number to Edit:
```

Figure 7-7 Menu 15.1 – Address Mapping Sets

Let us look first at Option 255. Option 255 is equivalent to SUA in previous ZyXEL routers (*see Section 7.2)*. The fields in this menu cannot be changed. Entering 255 brings up this screen.



```
                         Menu 15.1.255 - Address Mapping Rules

   Set Name= SUA (Read Only)

  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 ESC or ENTER to Exit:
```

Figure 7-8 SUA Address Mapping Rules

The following table explains the fields in this screen.

NOTE: 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 7-3 SUA Address Mapping Rules

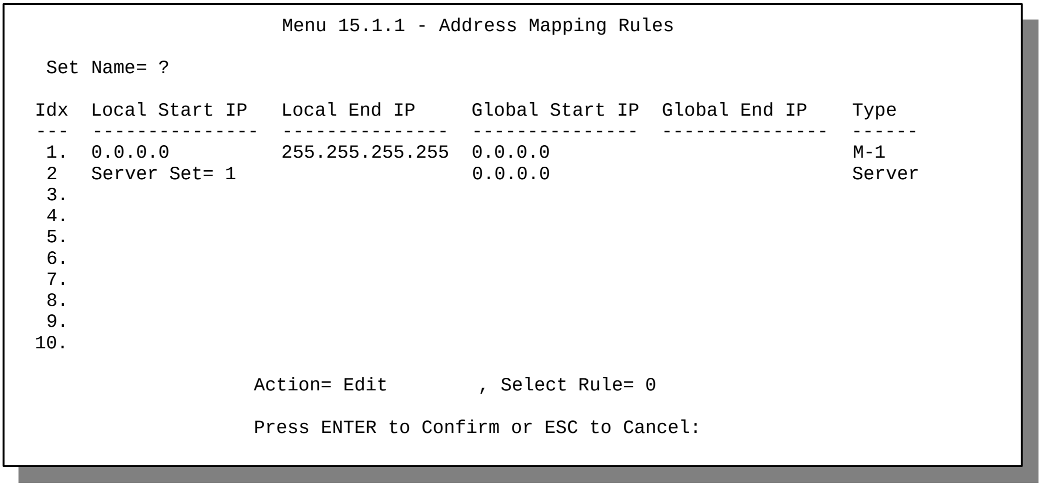
FIELD	DESCRIPTION	OPTIONS/EXAMPLE
Set Name	This is the name of the set you selected in Menu 15.1 or enter the name of a new set you want to create.	**SUA**
Idx	This is the index or rule number.	**1**
Local Start IP	This is the starting local IP address (ILA).	**0.0.0.0**
Local End IP	This is the ending 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	**0.0.0.0**

	Start IP.	
Global End IP	This is the ending global IP address (IGA).	**N/A**
Type	These are the mapping types discussed above (*see Table 7-1*). Type **Server** allows us to specify multiple servers of different types behind NAT to this machine. *See other sections* 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 us look at Option 1 in Menu 15.1. Enter 1 to bring up this menu. We will 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.

NOTE: If the Set Name field is left blank, the entire set will be deleted.



```
                      Menu 15.1.1 - Address Mapping Rules

 Set Name= ?

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.

                    Action= Edit        , Select Rule= 0

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

Figure 7-9 First Set in Menu 15.1.1

NOTE: 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

Ordering your rules is important. 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.

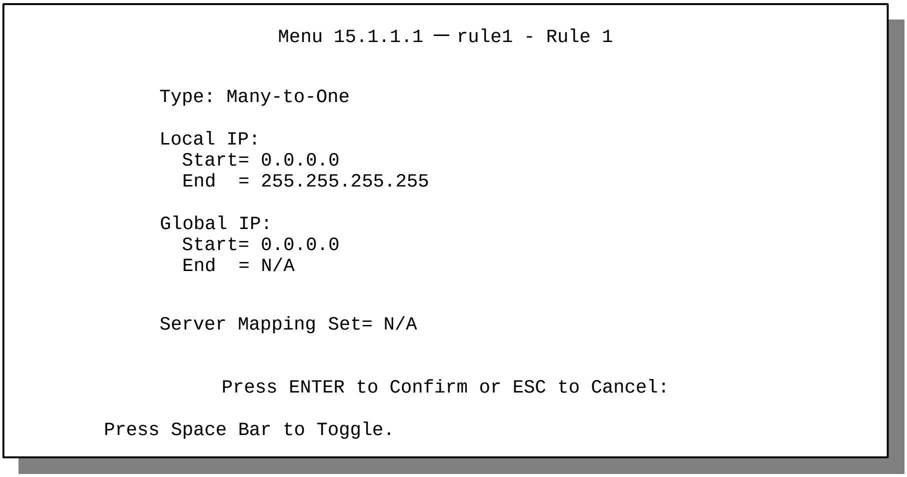
Table 7-4 Menu 15.1.1

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.	**E.g., rule1**
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 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).	**Edit/ Insert Before/ Delete/ Save Set**
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**

IMPORTANT: "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.

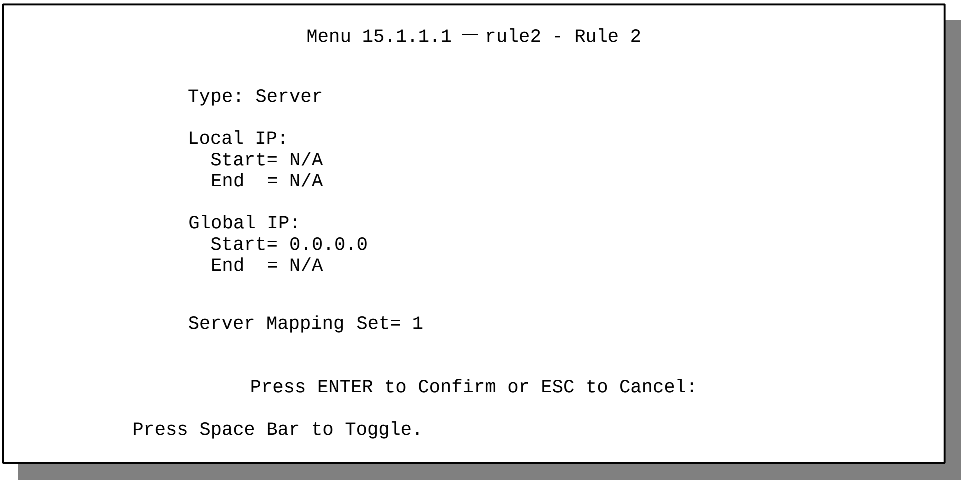
Be careful when ordering your rules as each rule is executed in turn beginning from rule 1.

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 — rule1 - 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 7-10 Editing the First Rule in a Set



```
                           Menu 15.1.1.1 — rule2 - 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:

           Press Space Bar to Toggle.
```

Figure 7-11 Editing the Second Rule in a Set

The following table describes the fields in these screens.

Table 7-5 Menu 15.1.1.1 – Configuring an Individual Rule

FIELD	DESCRIPTION	OPTION/EXAMPLE
Type	Press [space bar] to toggle through a total of 5 types. These are the mapping types discussed above (*see Table 7-1*). Type **Server** allows us to specify multiple servers of different types behind NAT to this machine. *See other section* for some examples.	**One-to-One/Many-to-One/ Many-to-Many Overload/ Many-to-Many No Overload/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	

FIELD	DESCRIPTION	OPTION/EXAMPLE
	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). This field is **N/A** for **One-to-One, Many-to-One** and **Server** types.	**172.16.23.55**
Server Mapping Set	This field is only available when the **Type** field is set at **Server**. Enter a single-digit number from **0** to **9** to refer to a particular server mapping set.	**0** to **9**

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.

7.5.2 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). If you are using Ethernet Encapsulation with either RR-Manager or RR-Toshiba Service Type port 12 set to 1025 (non-editable) as displayed in Figure 7-14.

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 at 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.

NOTE: 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.

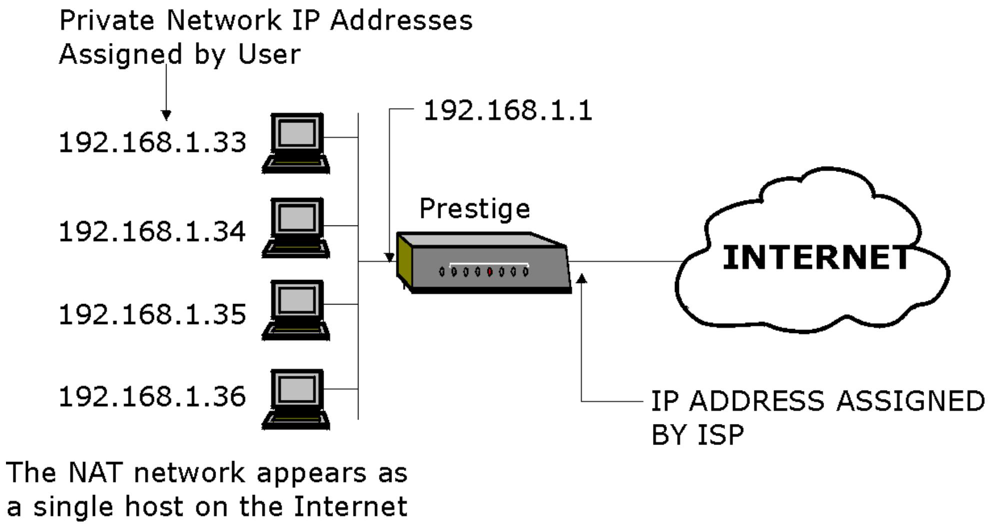


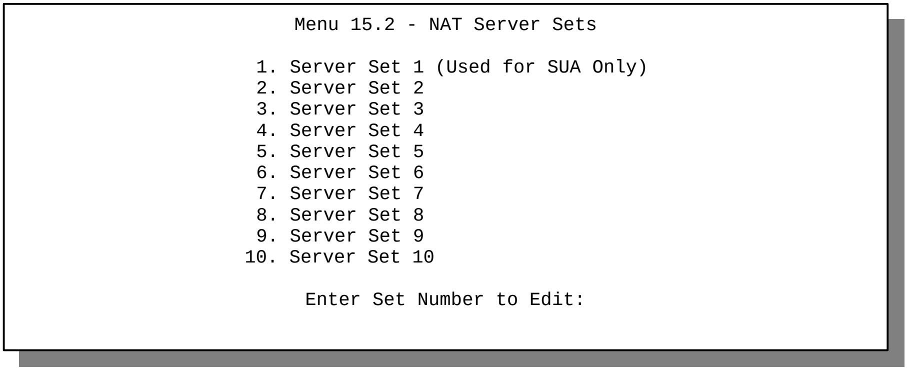
Figure 7-12 Multiple Servers Behind NAT

Configuring a Server Behind NAT

Perform the following steps 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**.

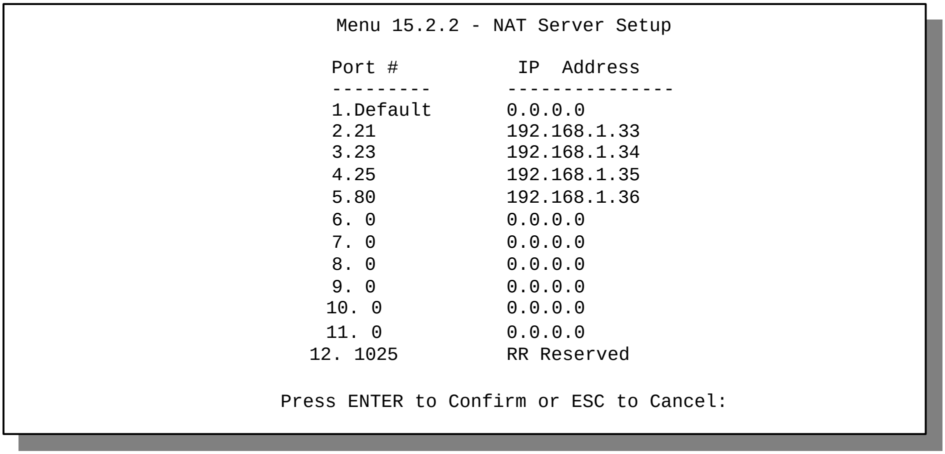


```
                    Menu 15.2 - NAT Server Sets

                  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 7-13 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 - NAT Server Setup

                  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. 1025          RR Reserved

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

Figure 7-14 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 7-6 Services and 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

7.6 Examples

7.6.1 Sample 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.

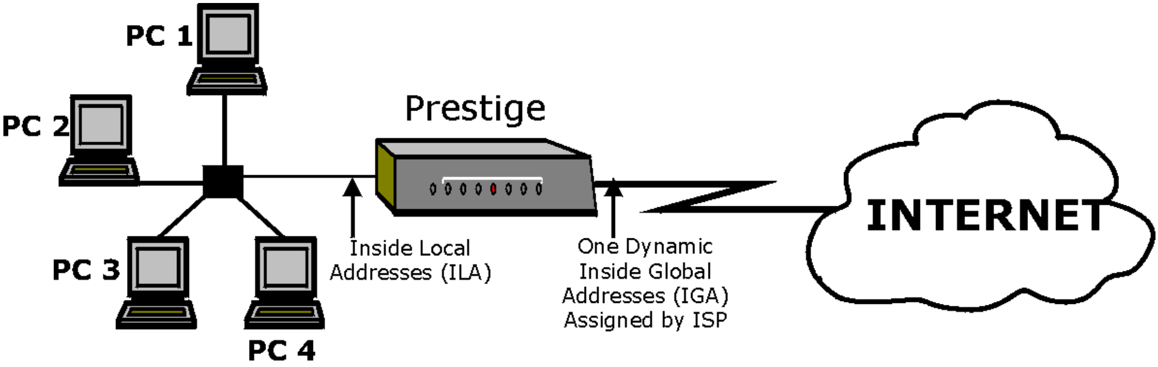
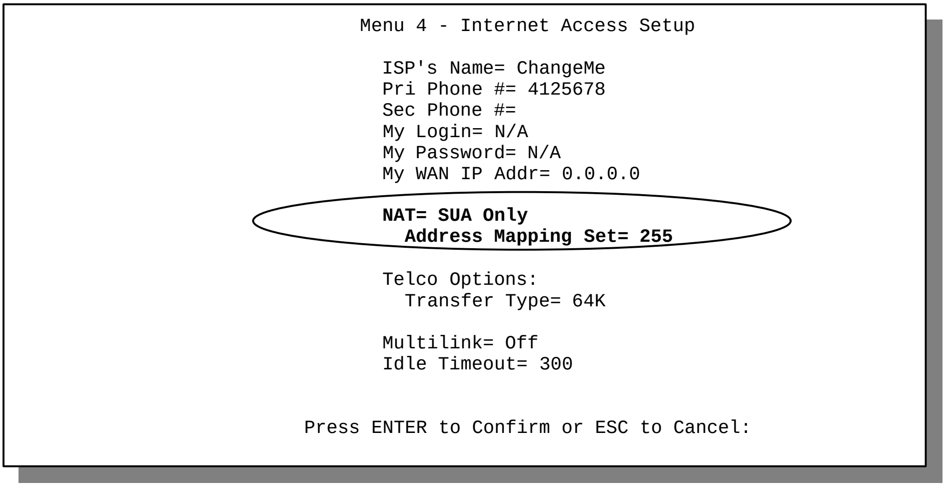

PC 1
PC 2
PC 3
PC 4
Prestige
Inside Local Addresses (ILA)
One Dynamic Inside Global Addresses (IGA) Assigned by ISP
INTERNET

Figure 7-15 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

                           Telco Options:
                             Transfer Type= 64K

                           Multilink= Off
                           Idle Timeout= 300


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

Figure 7-16 Internet Access and 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 7.1.3.* 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.

7.6.2 Example 2 – Internet Access With an Inside Server

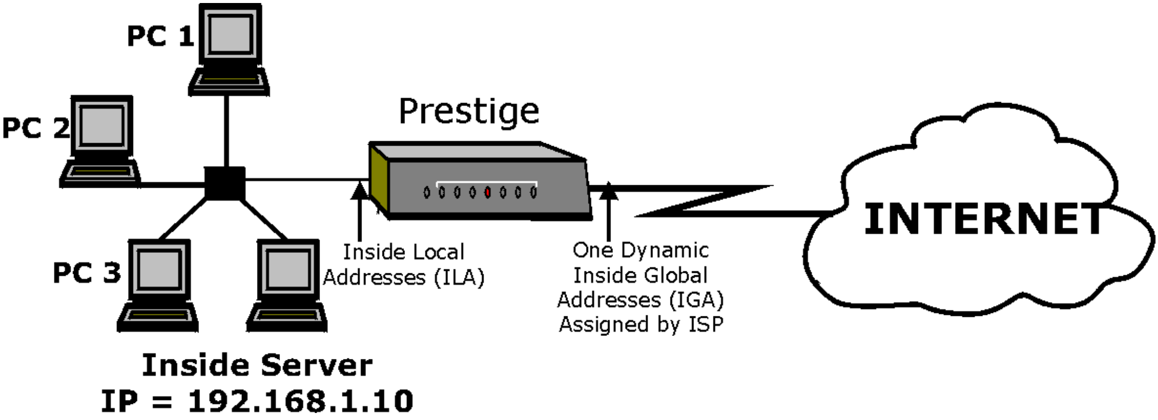
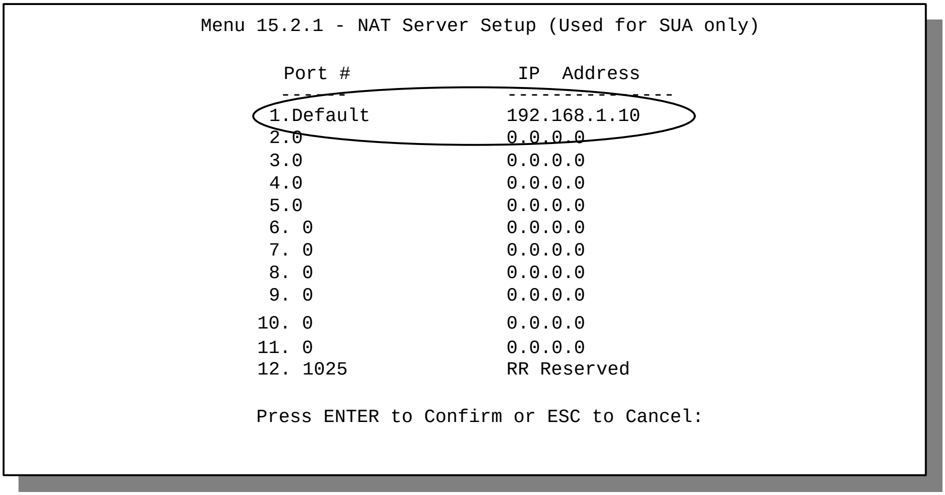

PC 1
PC 2
PC 3
Prestige
INTERNET
Inside Local Addresses (ILA)
One Dynamic Inside Global Addresses (IGA) Assigned by ISP
Inside Server
IP = 192.168.1.10

Figure 7-17 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.



```
                Menu 15.2.1 - NAT Server Setup (Used for SUA only)

                       Port #              IP  Address
                       ------              ---------------
                      1.Default           192.168.1.10
                      2.0                 0.0.0.0
                      3.0                 0.0.0.0
                      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 Confirm or ESC to Cancel:
```

Figure 7-18 Specifying an Inside Server

7.6.3 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 a third IGA to an inside web server and mail server. We need to configure 4 rules, 2 bi-directional and 2 mono-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:

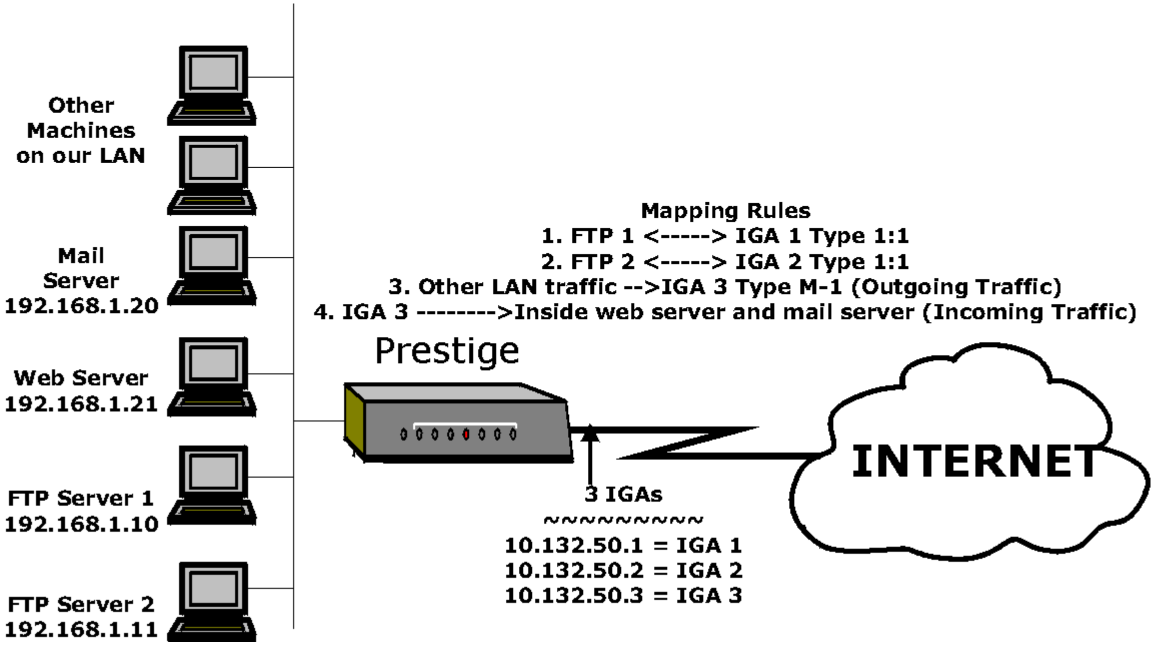

Other Machines on our LAN
Mail Server 192.168.1.20
Web Server 192.168.1.21
FTP Server 1 192.168.1.10
FTP Server 2 192.168.1.11
Mapping Rules
1. FTP 1 <-----> IGA 1 Type 1:1
2. FTP 2 <-----> IGA 2 Type 1:1
3. Other LAN traffic -->IGA 3 Type M-1 (Outgoing Traffic)
4. IGA 3 -------->Inside web server and mail server (Incoming Traffic)
Prestige
INTERNET
3 IGAs
~~~~~~~~~~
10.132.50.1 = IGA 1
10.132.50.2 = IGA 2
10.132.50.3 = IGA 3

Figure 7-19 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 can configure later.

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

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

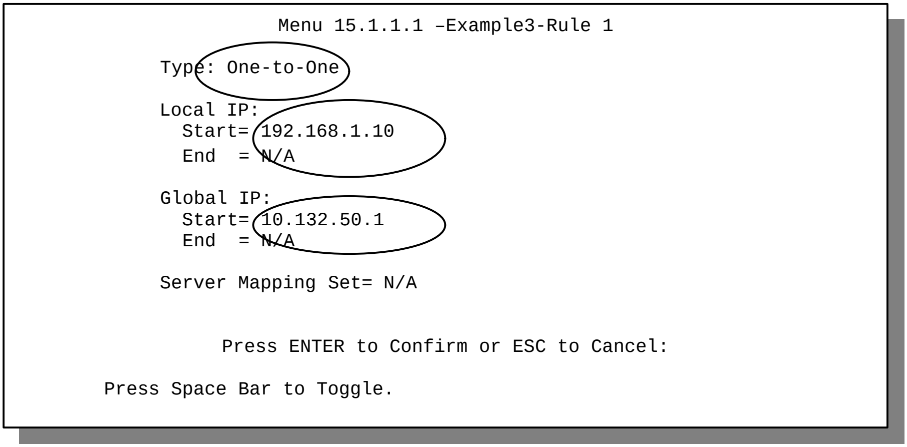
Step 3. Choose 1 to begin configuring this new set. Enter a **Set Name**, choose the **Edit Action** and then select **1** from **Select Rule** field. Press [Enter] to confirm.

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 7-20.)*

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 that shown in *Figure 7-21*.

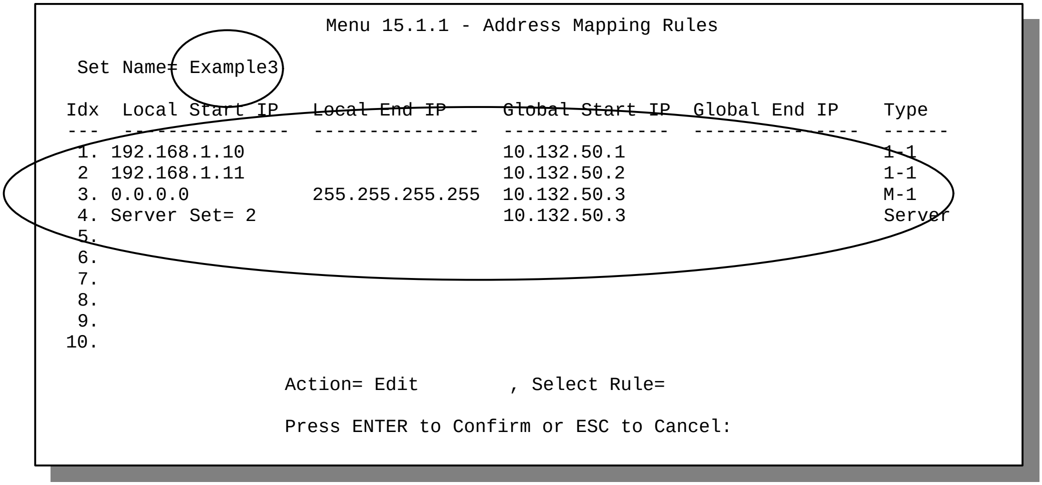
The following figure shows how to configure the first rule.



```
                Menu 15.1.1.1 –Example3-Rule 1

     Type: One-to-One

     Local IP:
       Start= 192.168.1.10
       End  = N/A

     Global IP:
       Start= 10.132.50.1
       End  = N/A

     Server Mapping Set= N/A


           Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 7-20 Example 3 – Menu 15.1.1.1

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



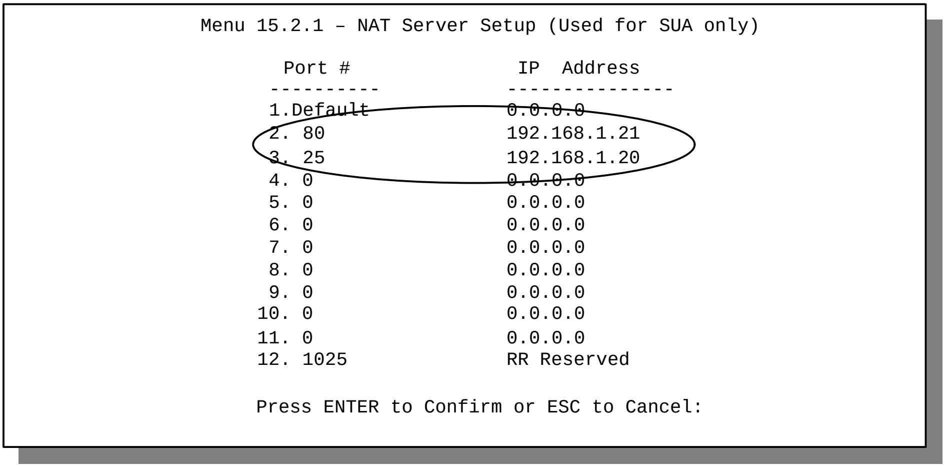
```
                       Menu 15.1.1 - Address Mapping Rules

 Set Name= Example3

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ------
 1. 192.168.1.10                       10.132.50.1                       1-1
 2  192.168.1.11                       10.132.50.2                       1-1
 3. 0.0.0.0           255.255.255.255  10.132.50.3                       M-1
 4. Server Set= 2                      10.132.50.3                       Server
 5.
 6.
 7.
 8.
 9.
10.

                    Action= Edit        , Select Rule=

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

Figure 7-21 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 7-22*.



```
                 Menu 15.2.1 – NAT Server Setup (Used for SUA only)

                          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 Confirm or ESC to Cancel:
```

Figure 7-22 Example 3 – Menu 15.2

7.6.4 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.

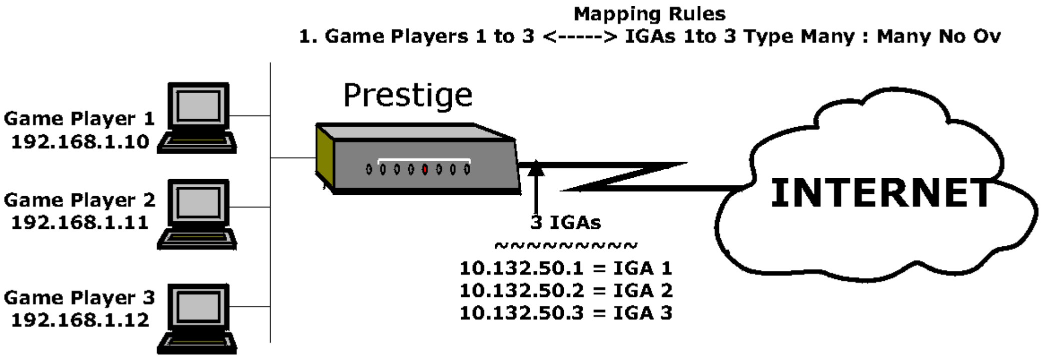
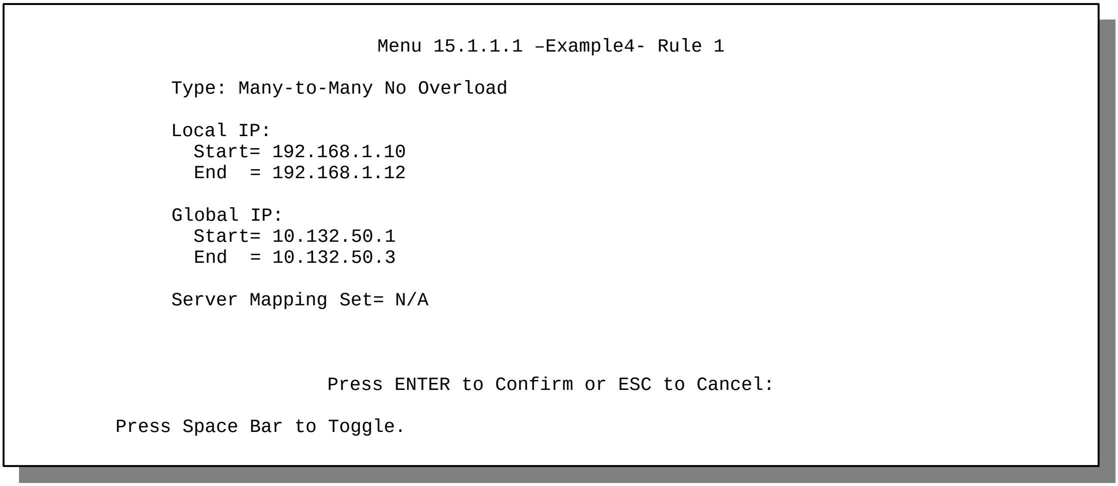


Figure 7-23 NAT Example 4

NOTE: Some applications still will not work through NAT even when using types One-to-One and Many-to-Many No Overload mapping types.

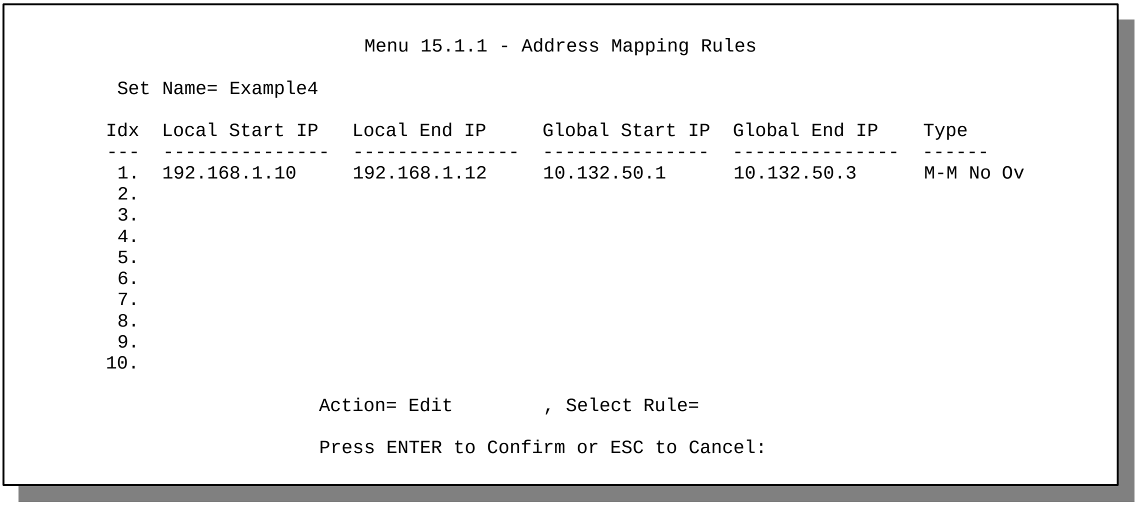
Follow the steps outlined in example 3 above to configure these two menus as follows.



```
                         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

              Server Mapping Set= N/A



                            Press ENTER to Confirm or ESC to Cancel:

         Press Space Bar to Toggle.
```

Figure 7-24 Example 4 – Menu 15.1.1.1

After you have 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 7-25 Example 4 – Menu 15.1.1 – Address Mapping Rules

Chapter 8
Advanced Phone Services

This chapter discusses the European and North American ISDN supplemental services.

The Prestige supports 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 they offer.

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
Multiple Subscriber Number (MSN) / Subaddress	
Terminal Portability: Suspend Resume	
	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. These features vary slightly between different Central Office switch types. 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 effect. However, using the flash key is preferred since the timing is much more precise. With manual 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).

Placing the Current Call on Hold

To place the current call on hold and answer the incoming call, press the flash key after hearing a call waiting indicator tone.

Dropping the Current Call to Switch to an Incoming/Holding Call

After hearing a Call Waiting indicator tone, simply hang up the telephone and wait for it 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 is busy or if they do not 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 of activating 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 8-2 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).

8.9 Multiple Subscriber Number (MSN)

In Europe you can subscribe (for a fee) more than one number for your ISDN line from your telephone company. You can then 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. On the other hand, the telephone company may give you only one number, but allow you to assign your own sub-addresses to different ports, e.g., sub-address 1 to data calls and 2 to A/B adapter 1.

If you choose **MSN** to determine routing for all incoming calls, the Prestige will compare the incoming call's **Called Party Number** or **Subaddress** to the number you set and route the incoming call to the destination that matches the number set. This feature is useful for those who connect a fax machine to one analog port while connecting a telephone set to the other analog port.

8.9.1 Using MSN

Go to SMT **Menu 2 – ISDN Setup**. Select **Multiple Subscriber Number (MSN)** or **Called Party Subaddress** in the **Incoming Phone Number Matching** field. Assign MSN/Subaddress numbers to the data/POTS ports. Then the data port or POTS port will answer incoming calls if and only if the called numbers match the MSN/Subaddress numbers assigned.

8.10 Terminal Portability (Suspend/Resume)

The Terminal Portability service allows you to suspend a phone call temporarily. You can then resume this call later, at another location if you so wish.

8.10.1 How to Suspend/Resume a Phone Call:

To suspend an active phone call

- Press the flash key twice.
- Dial ***3n*#**, where n is any number from 1 to 9.

To resume your phone call

- Reconnect at a(n) (ISDN) telephone that is linked to the same S/T interface (Network Terminator-1, NT1) where you suspended the call.
- Pick up the handset and press the flash key.
- Dial **#3n#**, where n is any number from 1 to 9, but should be identical to that used above.

Part III:

ADVANCED MANAGEMENT

Chapters 9 to 13 provide information on Prestige Filtering, SNMP, Telnet Configuration and Capabilities, System Maintenance, and Call Scheduling.

Chapter 9
Filter Configuration

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

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 filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens the data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the Ethernet side. Call filtering is used to determine if a packet should be allowed to trigger a call.

Outgoing packets must undergo data filtering before they encounter call filtering. 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 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.

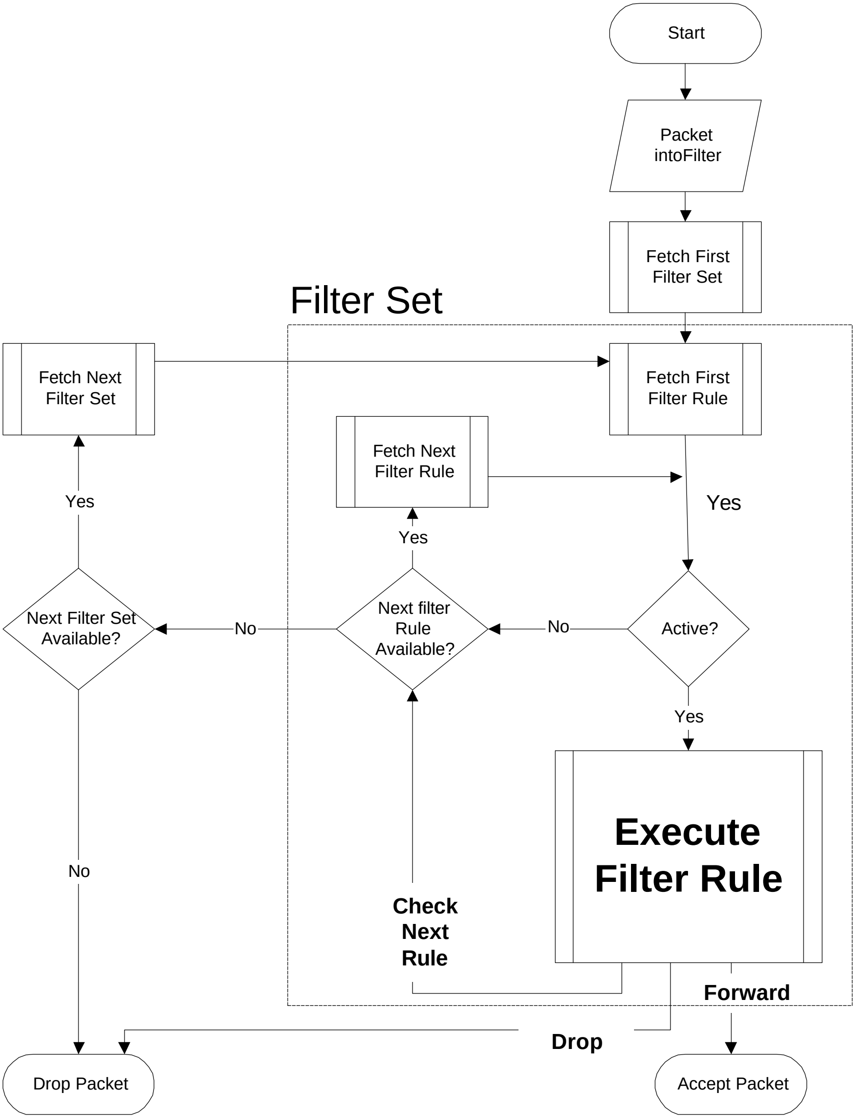


Figure 9-1 Filter Rule Process

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.

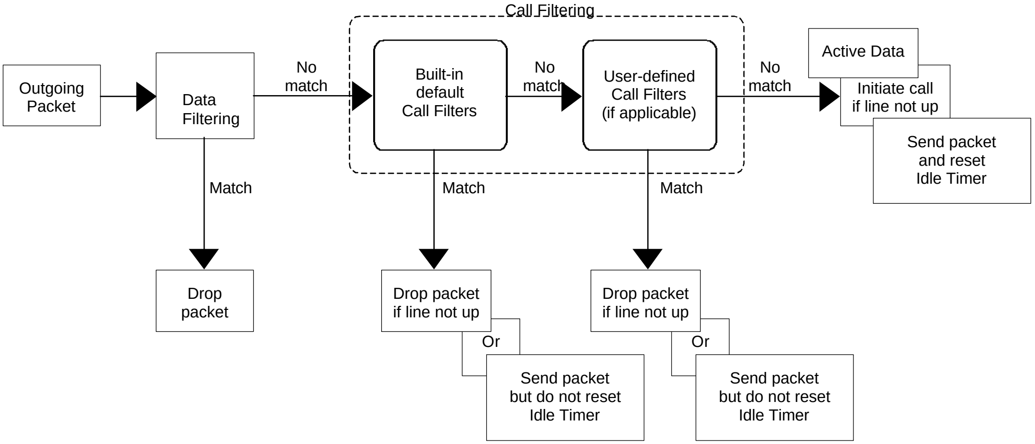

Call Filtering
Outgoing Packet
Data Filtering
No match
Built-in default Call Filters
No match
User-defined Call Filters (if applicable)
No match
Active Data
Initiate call if line not up
Send packet and reset Idle Timer
Match
Match
Match
Drop packet
Drop packet if line not up
Or
Send packet but do not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

Figure 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

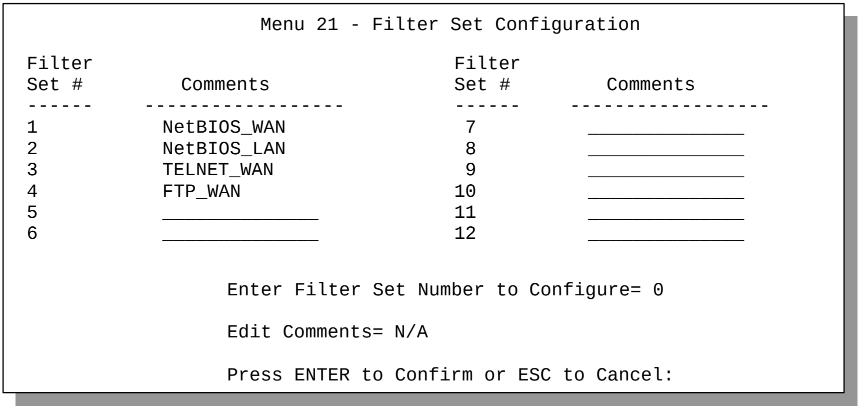
A filter set consists of one or more filter rules. Usually, you would group related rules, e.g., all the rules for NetBIOS, into a single set and give it a descriptive name. The Prestige allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the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

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



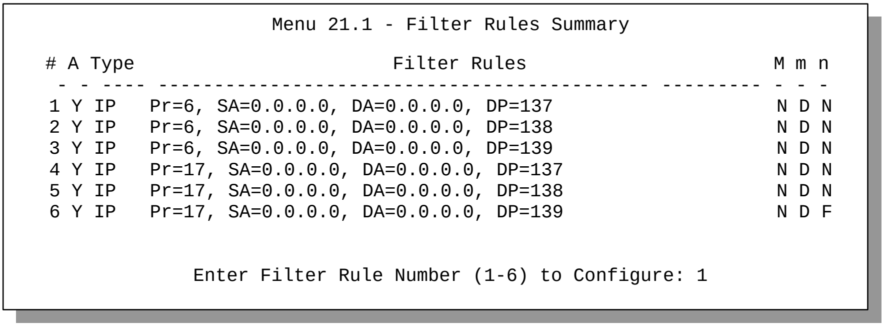
```
                       Menu 21 - Filter Set Configuration

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


                    Enter Filter Set Number to Configure= 0

                    Edit Comments= N/A

                    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 to 12) and press [Enter].

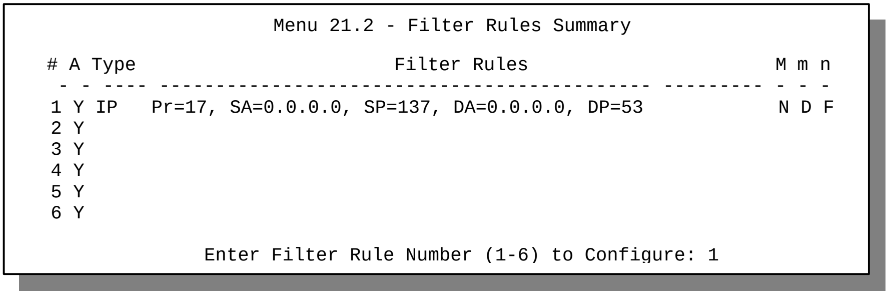
Step 3. Enter a descriptive name or comment in the Edit Comments field and press [Enter].

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 Menus

The preceding screens show summaries of the existing rules in the filter set. The following tables contain a brief description of the abbreviations used in Menu 21.1and Menu 21.2.

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

ABBREVIATIONS	DESCRIPTION	DISPLAY
#	Refers to the filter rule number (1 to 6).	
A	Refers to Active.	[Y] means the filter rule is active. [N] means the filter rule is inactive.
Type	Refers to the type of filter rule. This shows GEN for generic, IP for TCP/IP.	[GEN] for Generic [IP] for TCP/IP
Filter Rules	The filter rule parameters will be displayed here (see ahead).	
M	Refers to More. [Y] means an action cannot 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	[Y] means there are more rules to check. [N] means there are no more rules to check.

	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.**	
m	Refers to Action Matched. [F] means to forward the packet immediately and skip checking of the remaining rules.	[F] means to forward the packet. [D] means to drop the packet. [N] means to check the next rule.
n	Refers to Action Not Matched. [F] means to forward the packet immediately and skip checking of the remaining rules.	[F] means to forward the packet. [D] means to drop the packet. [N] means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

- If the filter type is IP, the 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
SP	Source Port Number
DA	Destination Address
DP	Destination Port Number

- If the filter type is GEN (generic), the 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 [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.

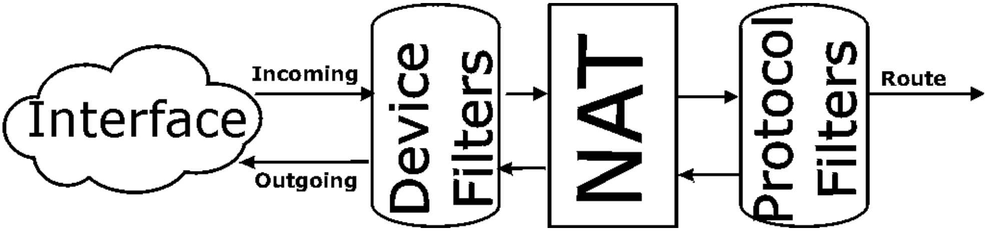


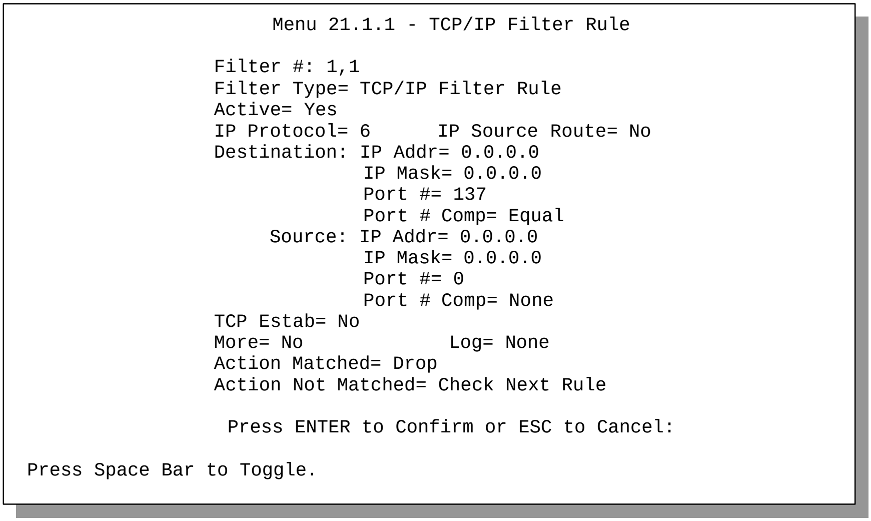
Figure 9-6 Protocol and Device Filter Sets

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



```
                        Menu 21.1.1 - TCP/IP Filter Rule

                   Filter #: 1,1
                   Filter Type= TCP/IP Filter Rule
                   Active= Yes
                   IP Protocol= 6      IP Source Route= No
                   Destination: IP Addr= 0.0.0.0
                                IP Mask= 0.0.0.0
                                Port #= 137
                                Port # Comp= Equal
                        Source: IP Addr= 0.0.0.0
                                IP Mask= 0.0.0.0
                                Port #= 0
                                Port # Comp= None
                   TCP Estab= No
                   More= No             Log= None
                   Action Matched= Drop
                   Action Not Matched= Check Next Rule

                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 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
Filter #	This is the filter set, filter rule coordinates, i.e., 2, 3 refers to the second filter set and the third filter rule of that set.	
Filter Type	Use [space bar] to toggle between types of rules. Parameters displayed for each type will be different.	**TCP/IP Filter Rule/ Generic Filter Rule**
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**	**0** to **255**

FIELD	DESCRIPTION	OPTION
	and **255**.	
IP Source Route	If **Yes**, the rule applies to packet with IP source route option; or else the packet must not have the 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 ignored if it is 0.0.0.0.	IP address
Destination: IP Mask	Enter the IP mask to apply to the Destination: IP Addr.	IP mask
Destination: Port #	Enter the destination port of the packets that you wish to filter. The range of this field is **0** to **65535**. This field is ignored if it is **0**.	**0** to **65535**
Destination: Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in Destination: Port #.	**None/Less/Greater/ Equal/Not Equal**
Source: IP Addr	Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	IP address
Source: IP Mask	Enter the IP mask to apply to the Source: IP Addr.	IP mask
Source: Port #	Enter the source port of the packets that you wish to filter. The range of this field is **0** to **65535**. This field is ignored if it is **0**.	**0** to **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; or 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; or else the packet is disposed of according to the action fields. If More is **Yes**, then Action Matched and Action Not Matched will be **N/A**.	**Yes/No**
Log	Select the logging option from the following: ● **None** – No packets will be logged. ● **Action Matched** – Only packets that match the rule parameters will be logged. ● **Action Not Matched** – Only packets that do not match the rule parameters will be logged. ● **Both** – All packets will be logged.	**None** **Action Matched** **Action Not Matched** **Both**

FIELD	DESCRIPTION	OPTION
Action Matched	Select the action for a matching packet.	**Check Next Rule/ Forward/Drop**
Action Not Matched	Select the action for a packet not matching the rule.	**Check Next Rule/ Forward/Drop**
Once you have completed filling in Menu 21.1.1 – 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.

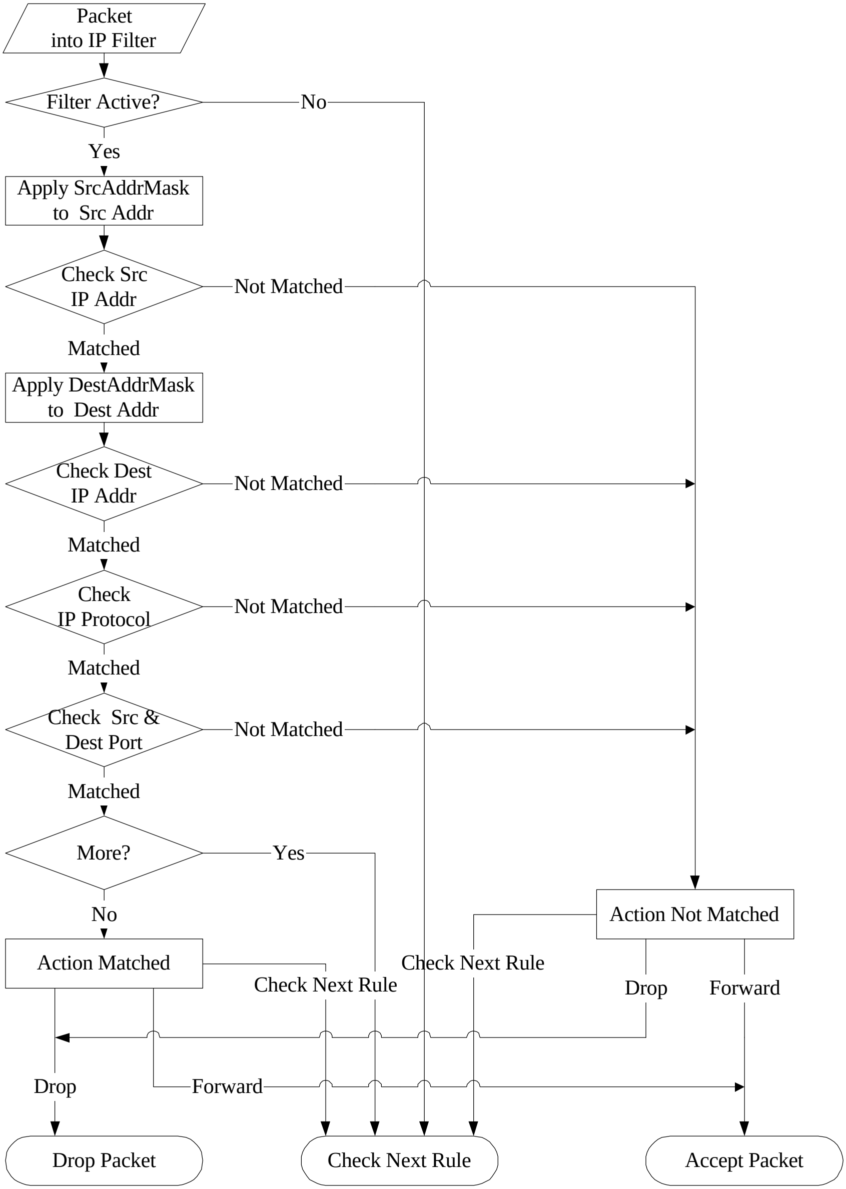


Figure 9-8 Executing an IP Filter

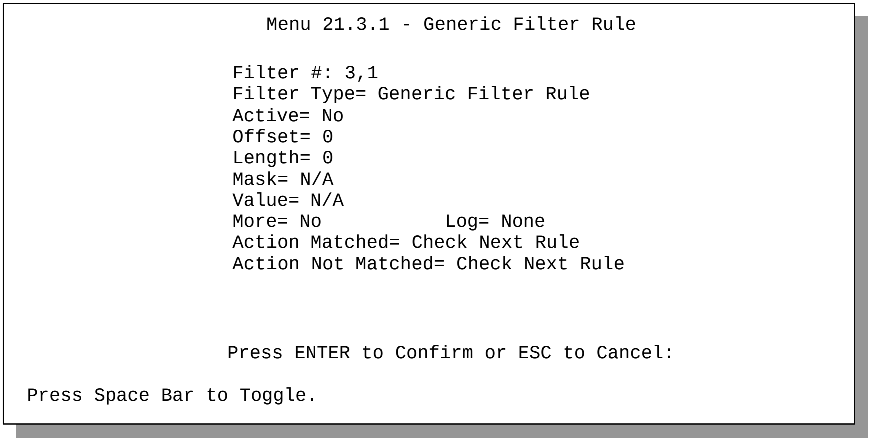
9.3.3 Generic Filter Rule

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: 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 21.3.1 – Generic Filter Rule**, as shown in the following figure.



```
                         Menu 21.3.1 - Generic Filter Rule

                      Filter #: 3,1
                      Filter Type= Generic Filter Rule
                      Active= No
                      Offset= 0
                      Length= 0
                      Mask= N/A
                      Value= N/A
                      More= No           Log= None
                      Action Matched= Check Next Rule
                      Action Not Matched= Check Next Rule



                     Press ENTER to Confirm or ESC to Cancel:

 Press Space Bar to Toggle.
```

Figure 9-9 Menu 21.3.1 – Generic Filter Rule

The next table describes the fields in the Generic Filter Rule menu.

Table 9-5 Generic Filter Rule Menu Fields

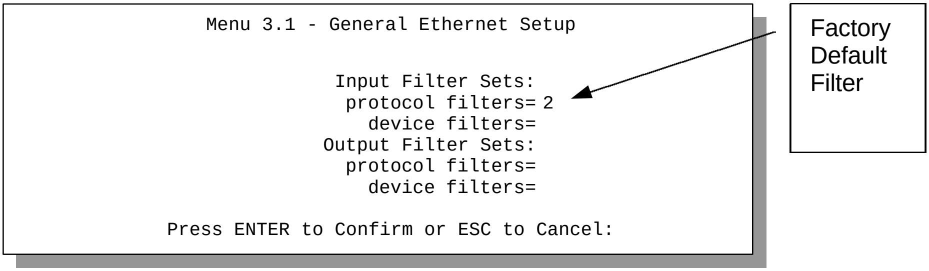
FIELD	DESCRIPTION	OPTION
Filter #	This is the filter set, filter rule coordinates, i.e., 2, 3 refers to the second filter set and the third rule of that set.	
Filter Type	Use [space bar] to toggle between both types of rules. Parameters displayed below each type will be different.	**Generic Filter Rule/ TCP/IP Filter Rule**
Active	Select **Yes** to turn on the filter rule.	**Yes/No**
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from **0** to **255**.	**0** (default)
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is **0** to **8**.	**0** (default)
Mask	Enter the mask (in Hexadecimal) to apply to the data portion before comparison.	
Value	Enter the value (in Hexadecimal) to compare with the data portion.	
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken; or else the packet is disposed of according to the action fields. If More is **Yes**, then Action Matched and Action Not Matched will be **N/A**.	**Yes/No**
Log	Select the logging option from the following: ● **None** – No packets will be logged. ● **Action Matched** – Only packets that match the rule parameters will be logged. ● **Action Not Matched** – Only packets that do not match the rule parameters will be logged. ● **Both** – All packets will be logged.	**None** **Action Matched** **Action Not Matched** **Both**
Action Matched	Select the action for a matching packet.	**Check Next Rule/Forward/ Drop**
Action Not Matched	Select the action for a packet not matching the rule.	**Check Next Rule/Forward/ Drop**
Once you have completed filling in Menu 21.3.1 – Generic Filter Rule, press [Enter] at the message [Press Enter to Confirm] to save your configuration, or press [Esc] to cancel. This data will now be displayed on Menu 21.3 – Filter Rules Summary.		

9.4 Applying Filters 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 9-3 **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 next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. The factory default filter set, NetBIOS_LAN, is inserted in the **protocol filters** field under **Input Filter Sets** in Menu 3.1 in order to prevent local NetBIOS messages from triggering calls to the DNS server.



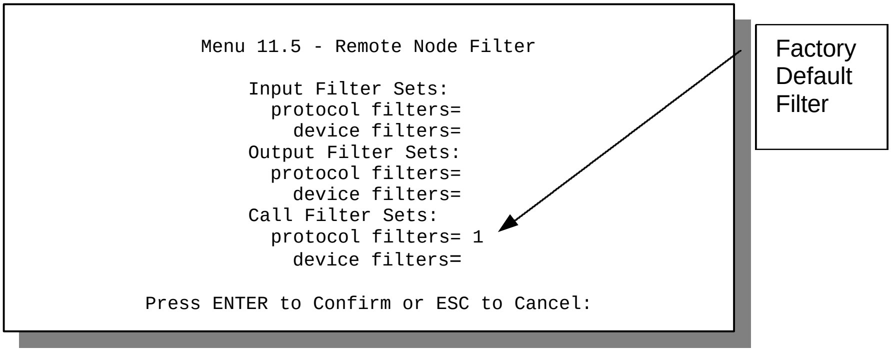
```
       Menu 3.1 - General Ethernet Setup


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

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

Factory Default Filter

Figure 9-10 Filtering Ethernet Traffic

9.4.2 Remote Node Filters

Go to Menu 11.5 (shown next) 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 ISP.



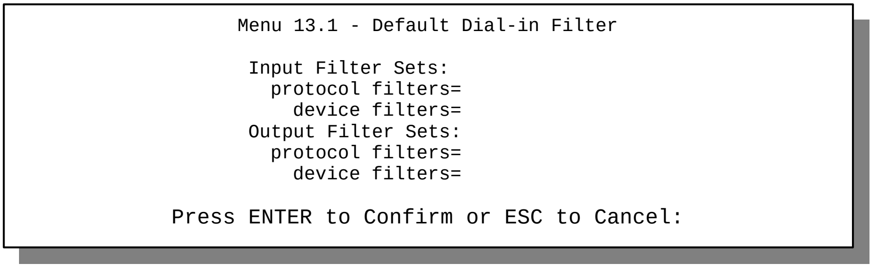
```
                    Menu 11.5 - Remote Node Filter

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

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

Factory Default Filter

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 this 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 a comma, e.g., 1, 5, 9, 12, in each filter field. The default is no filters.



```
                    Menu 13.1 - Default Dial-in Filter

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

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

Figure 9-12 Default Dial-in Filter

9.4.4 Sample FTP_WAN Filter Configuration

Before configuring a filter, you must have the following information:

1. **The inbound packet type (protocol and port number):** In this case, it is the **TCP (06)** protocol going to port **20 or 21**.

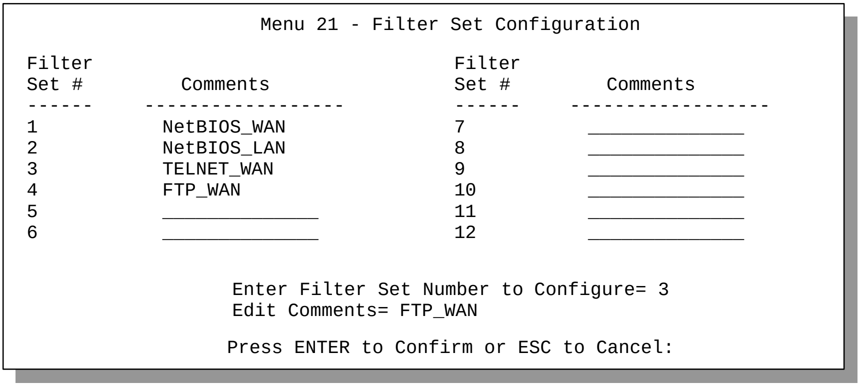
2. **The source IP address:** In this case, as all connections from the outside are blocked, the source IP is **0.0.0.0**.

3. **The destination IP address:** Enter the Prestige's IP address if SUA is disabled and you have a static IP; otherwise enter **0.0.0.0** as the destination IP. Once **0.0.0.0** is set as the destination IP, no FTP connections are allowed to reach neither the Prestige nor the FTP server on the LAN. For a LAN-to-LAN connection, enter the Prestige's LAN IP as **The destination IP address**. After you apply the FTP filter to a remote node, it blocks any FTP connections to the Prestige but continues to permit FTP connections to the local FTP server.

To configure a filter set to block any file uploading attempts from the outside perform the following procedures:

Step 1 Go to **Menu 21 – Filter Set Configuration**.

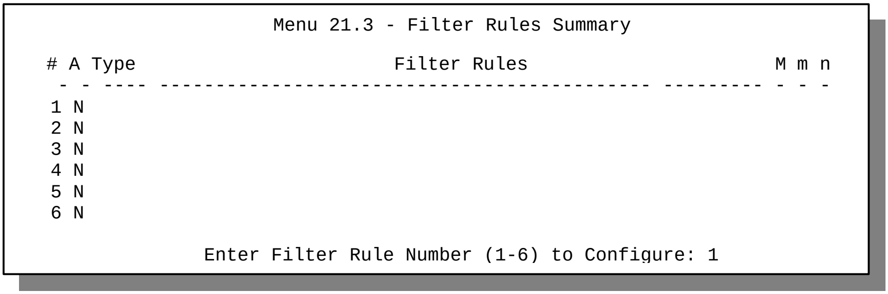
Step 2 Select a filter set and fill its **Edit Comments** field as shown next.



```
                    Menu 21 - Filter Set Configuration

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


                   Enter Filter Set Number to Configure= 3
                   Edit Comments= FTP_WAN

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

Figure 9-13 Menu 21 – Filter Set Configuration

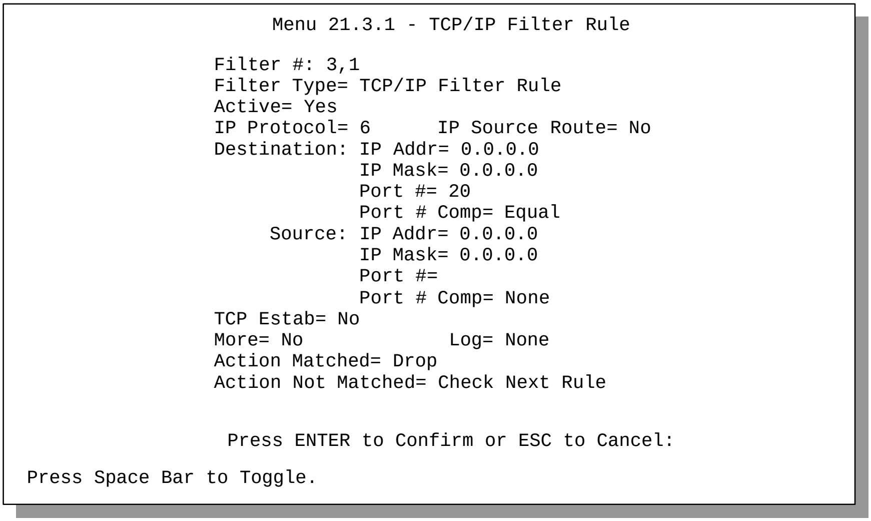
Step 3 Go to Menu 21.3 **–** Filter Rules Summary.



```
                        Menu 21.3 - Filter Rules Summary

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

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

Figure 9-14 Menu 21.3 – Filter Rules Summary

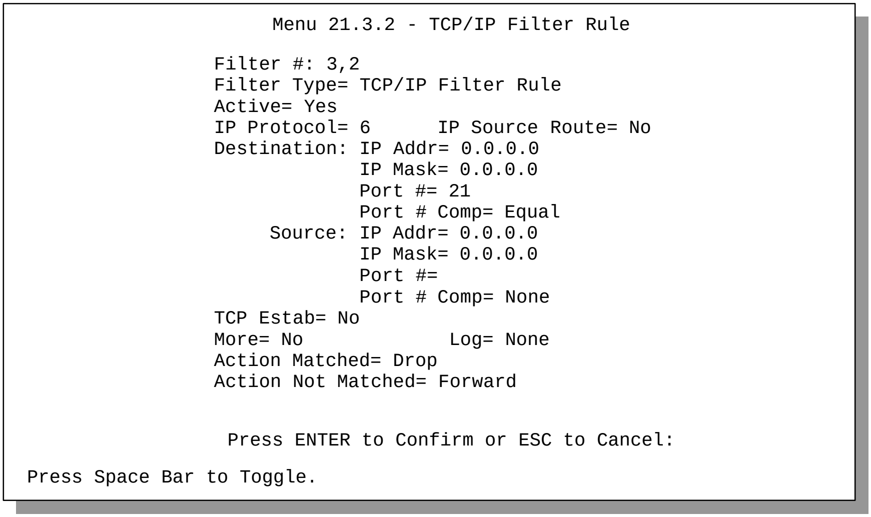
Step 4 Select 1 to configure the first filter rule using **Menu 21.3.1.**



```
                      Menu 21.3.1 - TCP/IP Filter Rule

                 Filter #: 3,1
                 Filter Type= TCP/IP Filter Rule
                 Active= Yes
                 IP Protocol= 6      IP Source Route= No
                 Destination: IP Addr= 0.0.0.0
                              IP Mask= 0.0.0.0
                              Port #= 20
                              Port # Comp= Equal
                      Source: IP Addr= 0.0.0.0
                              IP Mask= 0.0.0.0
                              Port #=
                              Port # Comp= None
                 TCP Estab= No
                 More= No             Log= None
                 Action Matched= Drop
                 Action Not Matched= Check Next Rule


                  Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 9-15 Menu 21.3.1 – TCP/IP Filter Rule

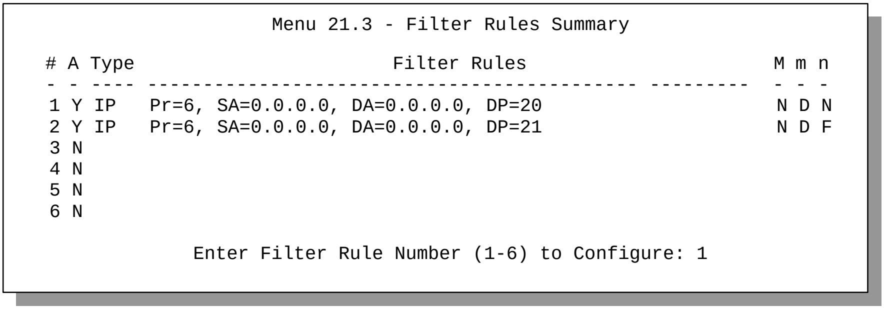
Step 5 Go back to **Menu 21.3** and select 2 to configure the second filter rule using **Menu 21.3.2.**



```
                        Menu 21.3.2 - TCP/IP Filter Rule

                   Filter #: 3,2
                   Filter Type= TCP/IP Filter Rule
                   Active= Yes
                   IP Protocol= 6      IP Source Route= No
                   Destination: IP Addr= 0.0.0.0
                                IP Mask= 0.0.0.0
                                Port #= 21
                                Port # Comp= Equal
                        Source: IP Addr= 0.0.0.0
                                IP Mask= 0.0.0.0
                                Port #=
                                Port # Comp= None
                   TCP Estab= No
                   More= No             Log= None
                   Action Matched= Drop
                   Action Not Matched= Forward


                    Press ENTER to Confirm or ESC to Cancel:

  Press Space Bar to Toggle.
```

Figure 9-16 Menu 21.3.2 – TCP/IP Filter Rule

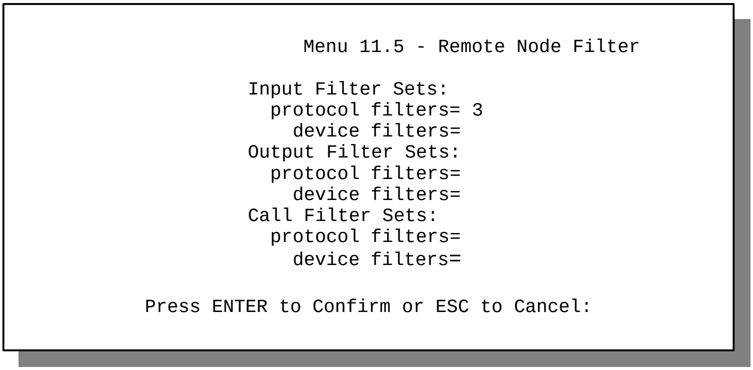
Step 6 Go back to Filter Rules Summary in **Menu 21.3** to check if the filter rule has been configured correctly.



```
                         Menu 21.3 - Filter Rules Summary

    # A Type                       Filter Rules                      M m n
    - - ---- --------------------------------------------- ---------  - - -
    1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=20                      N D N
    2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=21                      N D F
    3 N
    4 N
    5 N
    6 N

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

Figure 9-17 Menu 21.3 – Filter Rules Summary

Step 7 Finally, go to **Menu 11.5 – Remote Node Filter** and enter the protocol filter in every remote node where you want to disable the FTP upload function.



```
                          Menu 11.5 - Remote Node Filter

                     Input Filter Sets:
                       protocol filters= 3
                         device filters=
                     Output Filter Sets:
                       protocol filters=
                         device filters=
                     Call Filter Sets:
                       protocol filters=
                         device filters=

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

Figure 9-18 Menu 11.5 – Remote Node Filter

9.4.5 Sample TELNET_WAN Filter Configuration

Let us look at the third default ZyXEL filter, TELNET_WAN as an example. Please see our PNC Disk for more sample filters. This filter was designed to block outside users telnetting into the Prestige.

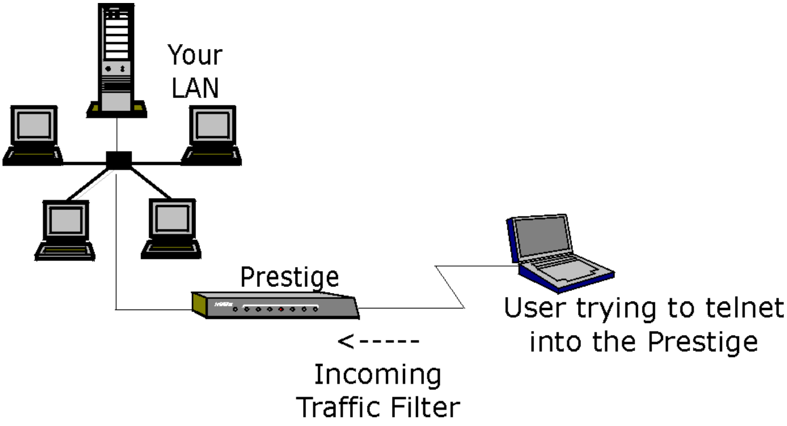


Figure 9-19 Sample Telnet Filter

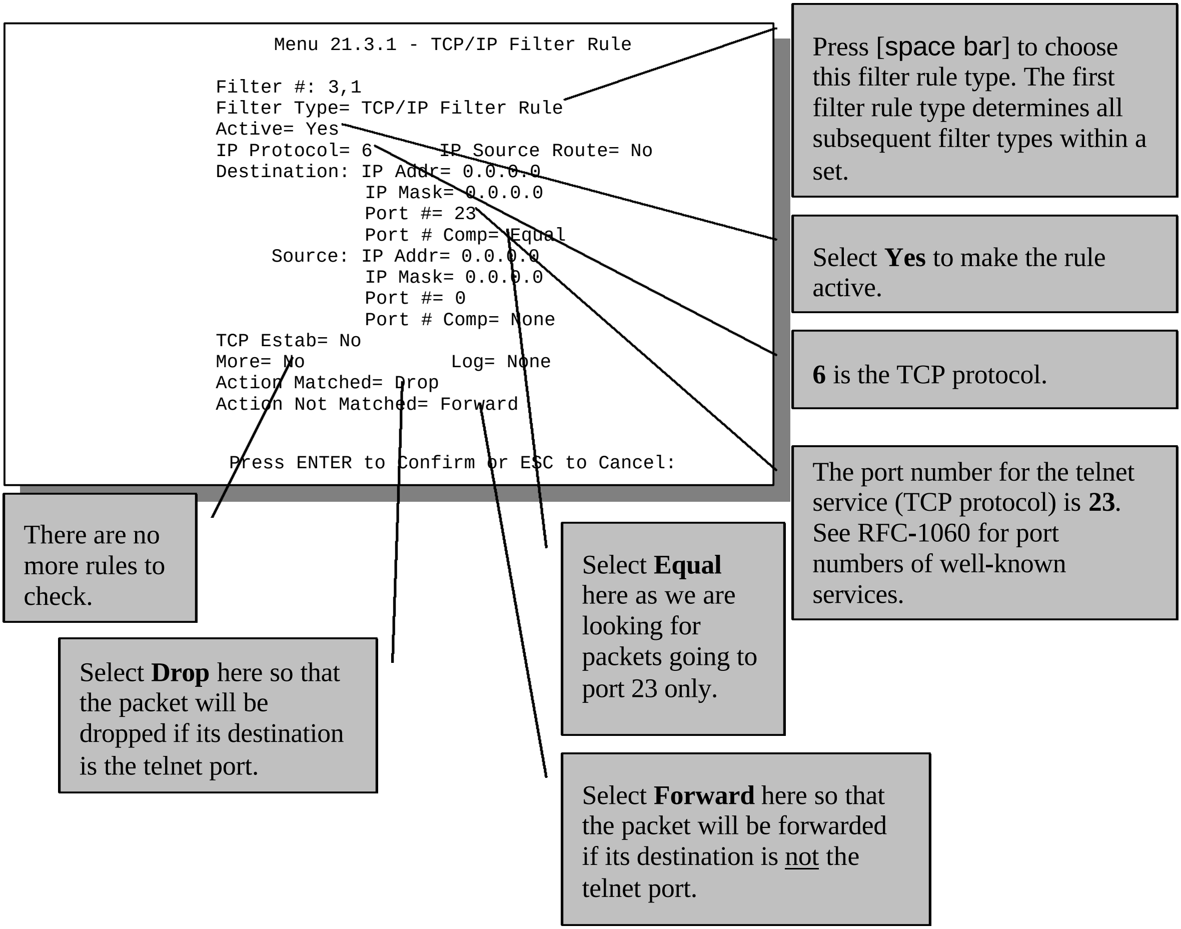
Step 1. Enter **21** from the Main Menu to open **Menu 21 – Filter Set Configuration**.

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

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

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

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



```
                    Menu 21.3.1 - TCP/IP Filter Rule

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


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

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

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

6 is the TCP protocol.

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

There are no more rules to check.

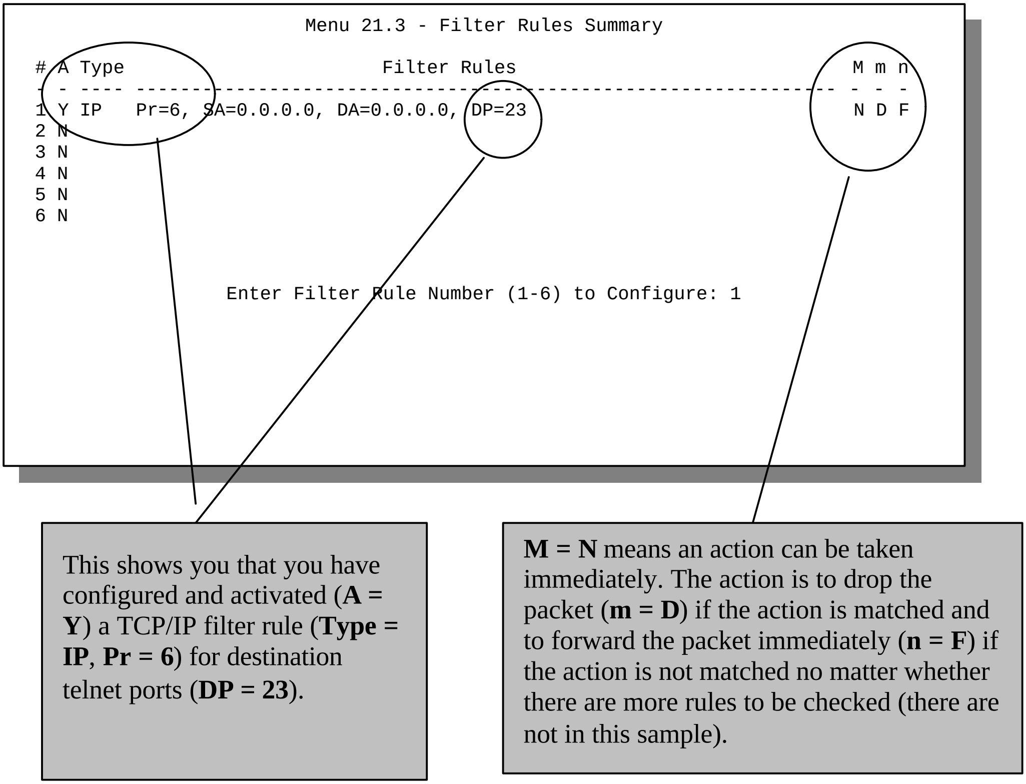
Select **Equal** here as we are looking for packets going to port 23 only.

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

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

Figure 9-20 Sample Filter – Menu 21.3.1

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



```
                         Menu 21.3 - Filter Rules Summary

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



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

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

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

Figure 9-21 Sample Filter Rules Summary – Menu 21.3

After you have created the filter set, you must apply it.

Step 1. Enter **11** from the main menu to go to Menu 11, and enter the remote node number to edit.

Step 2. Go to the **Edit Filter Sets** field, press [space bar] to toggle **No** to **Yes** and press [Enter].

Step 3. This brings you to Menu 11.5. Apply the TELNET_WAN filter set (filter set 3).

Chapter 10

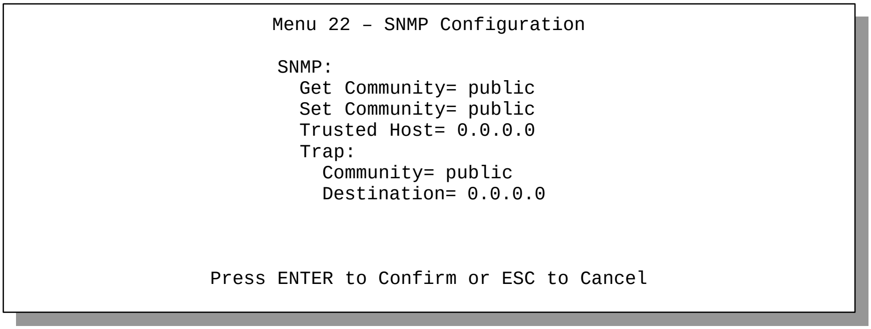
SNMP (Simple Network Management Protocol)

This chapter takes you through SNMP Configuration Menu 22.

The SNMP is a protocol governing network management and the monitoring of network devices and their functions. The Prestige supports the utilization of SNMP to regulate the communication that occurs between the manager station and the agent stations in a network. Basically, your Prestige, when connected to the LAN, acts as an agent station. In this way, the manager station on your LAN can monitor your Prestige as it would another station on the network. Keep in mind that SNMP is only available if TCP/IP is configured.

Configuring Your Prestige For SNMP Support

The following steps describe a simple setup procedure for configuring SNMP management.



```
                         Menu 22 – SNMP Configuration

                          SNMP:
                            Get Community= public
                            Set Community= public
                            Trusted Host= 0.0.0.0
                            Trap:
                              Community= public
                              Destination= 0.0.0.0



                    Press ENTER to Confirm or ESC to Cancel
```

Figure 10-1 Menu 22 – SNMP Configuration

1. From the Main Menu, select option 22. SNMP Configuration. This brings you to Menu 22 – SNMP Configuration.

2. You are prompted to enter the following information. The parameters you have to fill in are indicated in **bold** type.

Table 10-1 Fields in Menu 22 (SNMP Configuration)

FIELD	DESCRIPTION	EXAMPLES
Get Community	You can determine what the Get Community is for your Prestige. The value entered into this field is used to authenticate the community field for the incoming **Get–** and **GetNext –** requests from the management station. The default is **public**.	**Public** (default)
Set Community	Enter the Set Community for your Prestige. The value entered in this field is used to authenticate the community field for the incoming **Set –** requests from the management station. The default is **public**.	**Public** (default)
Trusted Host	Enter the IP address of the trusted host SNMP management station. If this field is configured, then your Prestige only responds to SNMP messages coming from this address. If you leave the field blank (default), then your Prestige responds to all SNMP messages it receives, regardless of origin.	
Trap: Community	Enter the community name that is sent with each trap to the SNMP manager. This should be treated like a password and match what the SNMP manager is expecting. The default is **public**.	**Public** (default)
Trap: Destination	This field contains the IP address of the station that you wish to send your SNMP traps.	

Once you have completed filling in **Menu 22 – SNMP Configuration**, press [Enter] key to confirm your selections or press [Esc] key to cancel your changes. If you are not certain how to configure the fields for the SNMP Configuration, consult your network administrator.

Chapter 11
Telnet Configuration and Capabilities

This chapter discusses using telnet to remotely configure your Prestige.

11.1 About Telnet Configuration

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

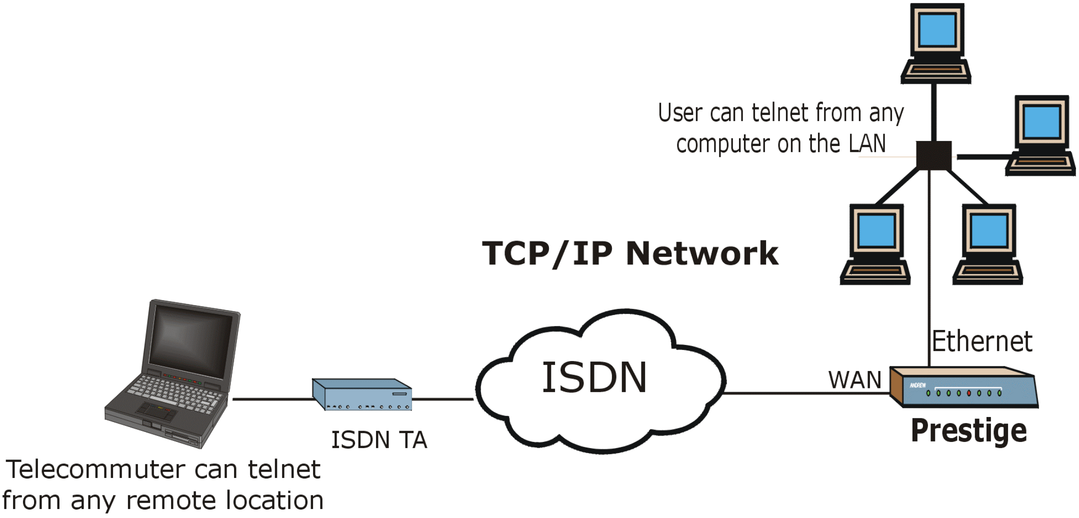

User can telnet from any computer on the LAN
TCP/IP Network
Ethernet
WAN
ISDN
Prestige
ISDN TA
Telecommuter can telnet from any remote location

Figure 11-1 Telnet Configuration on a TCP/IP Network

11.2 Telnet Under NAT

When NAT is enabled and an inside server is specified, telnet connections from the outside will be forwarded to the inside server. So to configure the Prestige via telnet from the outside, you must first telnet to the inside server, and then telnet from the server to the Prestige using its inside LAN IP address. If no inside server is specified, telnetting to the SUA™ ’s IP address connects to the Prestige directly.

11.3 Telnet Capabilities

11.3.1 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.

11.3.2 System Timeout

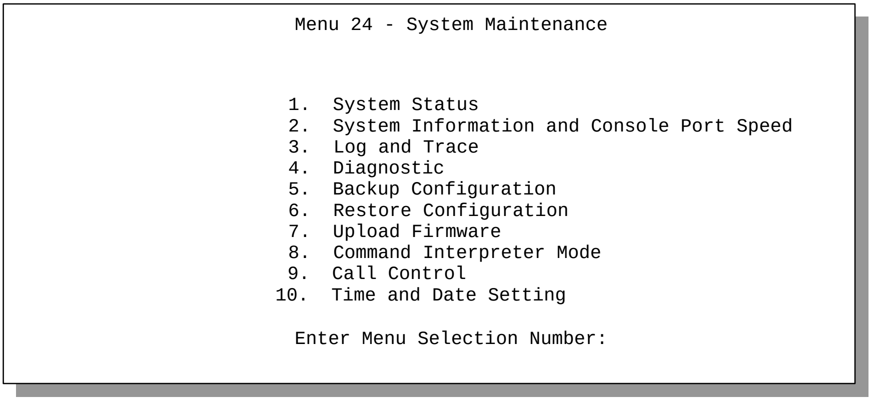
There is a system timeout of 5 minutes (300 seconds) for either the console port or telnet. Your Prestige will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in Menu 24.1.

Chapter 12
System Maintenance

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

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

Select Menu 24 in the main menu to open **Menu 24 – System Maintenance**, as shown in the following figure.



```
                    Menu 24 - System Maintenance



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

                    Enter Menu Selection Number:
```

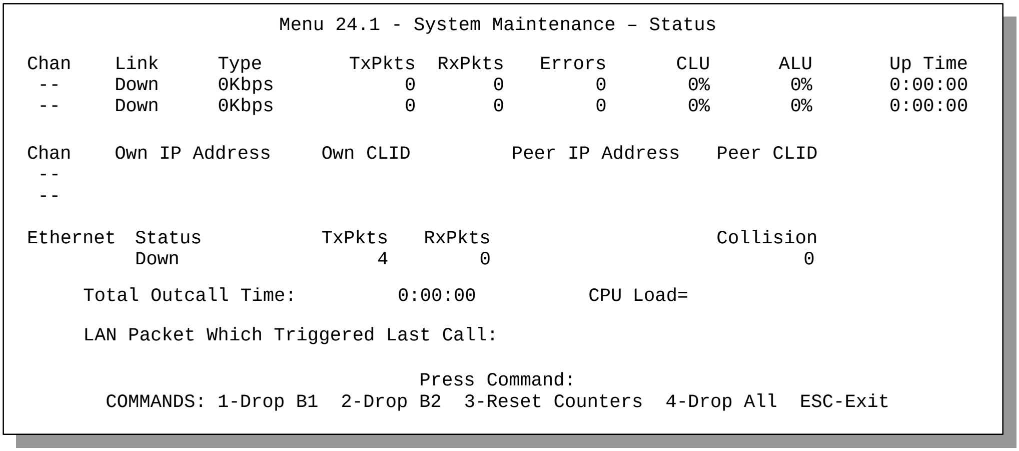
Figure 12-1 Menu 24 – System Maintenance

12.1 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 System Status, enter **24** to go to **Menu 24 – System Maintenance.** From this menu, enter **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 pressing [Esc] takes you back to the previous screen.

The following table 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.



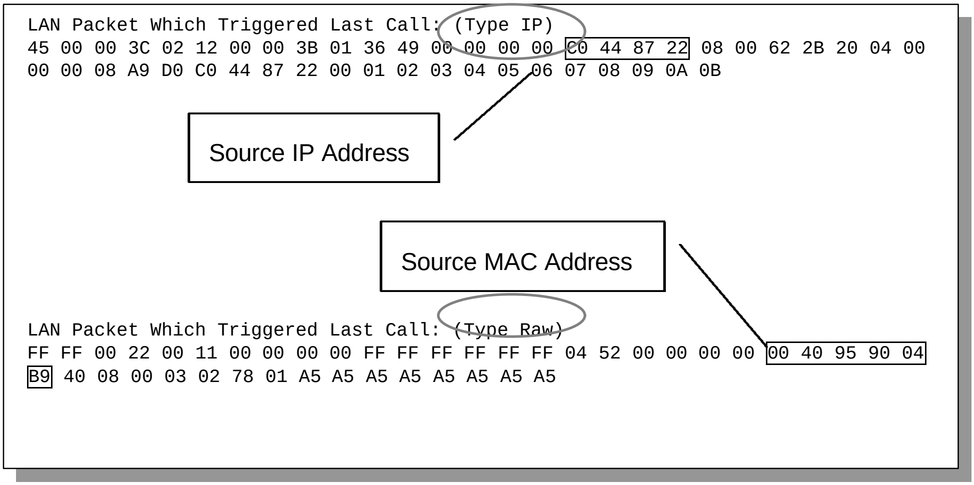
```
                        Menu 24.1 - System Maintenance – Status

 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

 Chan    Own IP Address    Own CLID         Peer IP Address   Peer CLID
  --
  --

 Ethernet  Status           TxPkts   RxPkts                    Collision
           Down                  4        0                            0

      Total Outcall Time:         0:00:00         CPU Load=

      LAN Packet Which Triggered Last Call:

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

Figure 12-2 Menu 24.1 – System Maintenance – Status

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

Table 12-1 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 (e.g., **Down**, **Idle**, **Calling, Answering, NetCAPI,** etc.).
Type	The current connecting speed.
TxPkts	The number of transmitted packets on this channel.
RxPkts	The number of received packets on this channel.
Errors	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 usage for this channel.
Up Time	Time this channel has been connected to the current remote node.
Chan	Shows statistics for **B1** and **B2** channels respectively. This is the information displayed for each channel.
Own IP Address	Refers to the IP address of the Prestige.
Own CLID	Shows your Caller ID.
Peer IP Address	Refers to the IP address of the peer.
Peer CLID	Shows the Caller ID of the peer.
Ethernet	Shows statistics for the LAN.
Status	Shows the current status of the LAN.
TxPkts	The number of transmitted packets to the LAN.
RxPkts	The number of received packets from the LAN.
Collision	Number of collisions.
Total Outcall Time	Shows the total outgoing call time for both **B1** and **B2** channels since the system has been powered up.
CPU Load	Specifies the percentage of CPU utilization.
LAN Packet Which Triggered Last Call	Shows the first 48 octets of the LAN packet that triggered the last outgoing call.

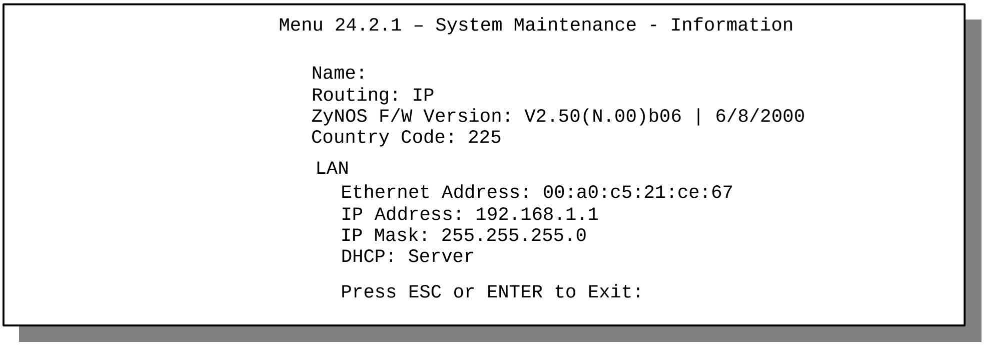


```
LAN Packet Which Triggered Last Call: (Type IP)
45 00 00 3C 02 12 00 00 3B 01 36 49 00 00 00 00 C0 44 87 22 08 00 62 2B 20 04 00
00 00 08 A9 D0 C0 44 87 22 00 01 02 03 04 05 06 07 08 09 0A 0B

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

Figure 12-3 LAN Packet That Triggered Last Call

The figure above shows two samples 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.

12.1.1 System Information



```
                         Menu 24.2.1 – System Maintenance - Information

                            Name:
                            Routing: IP
                            ZyNOS F/W Version: V2.50(N.00)b06 | 6/8/2000
                            Country Code: 225
                            LAN
                               Ethernet Address: 00:a0:c5:21:ce:67
                               IP Address: 192.168.1.1
                               IP Mask: 255.255.255.0
                               DHCP: Server

                               Press ESC or ENTER to Exit:
```

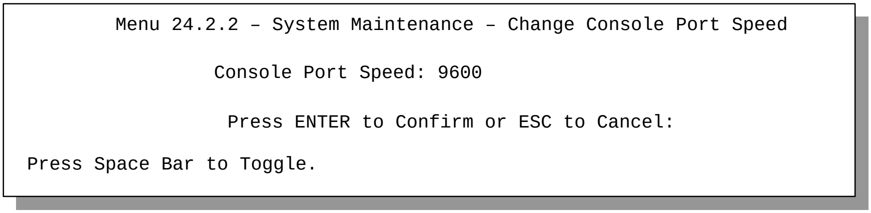
Figure 12-4 System Maintenance – Information

Table 12-2 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.
ZyNOS F/W Version	Refers to the version of the ZyNOS Network Operating System firmware. ZyNOS is a registered trademark of ZyXEL Communications Corp.
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.

12.1.2 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 [space bar] to select the desired speed in Menu 24.2.2, as shown in the following figure.



```
         Menu 24.2.2 – System Maintenance – Change Console Port Speed

                 Console Port Speed: 9600

                  Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 12-5 Menu 24.2.2 – System Maintenance – Change Console Port Speed

12.2 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.

12.2.1 Viewing Error Log

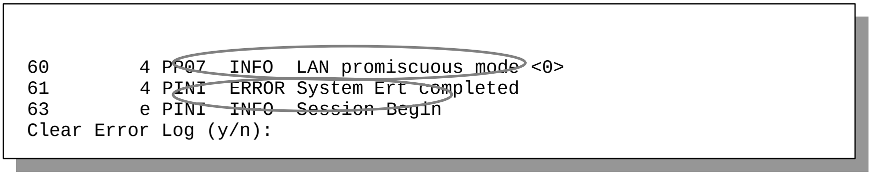
The first place you should look for clues when something goes wrong is the error log. Follow the procedures to view the local error/trace log:

Step 1. Enter 24 from the Main Menu to open **Menu 24** – **System Maintenance**.

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

Step 3. Enter 1 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. Samples of typical error and information messages are presented in the next figure.

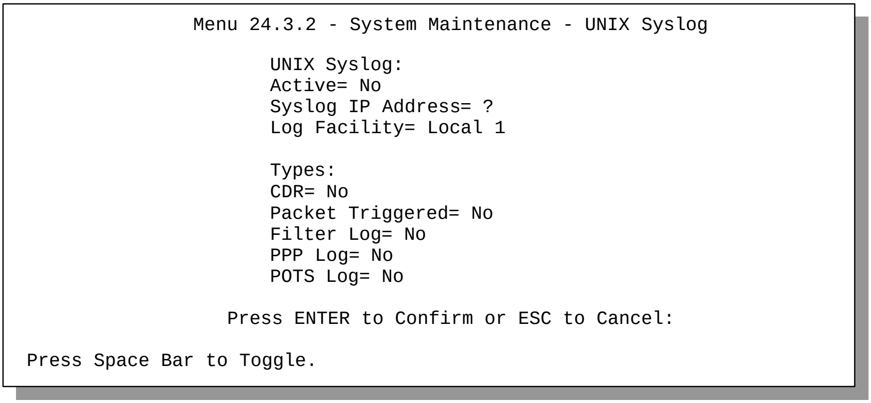


```
60         4 PP07  INFO  LAN promiscuous mode <0>
61         4 PINI  ERROR System Ert completed
63         e PINI  INFO  Session Begin
Clear Error Log (y/n):
```

Figure 12-6 Sample Error and Information Messages

12.2.2 Syslog And Accounting

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



```
                 Menu 24.3.2 - System Maintenance - UNIX Syslog

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

                        Types:
                        CDR= No
                        Packet Triggered= No
                        Filter Log= No
                        PPP Log= No
                        POTS Log= No

                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 12-7 Menu 24.3.2 – System Maintenance – Syslog and Accounting

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

Table 12-3 System Maintenance Menu Syslog Parameters

PARAMETER	DESCRIPTION
UNIX Syslog:	
Active	Use [space bar] to turn on or off syslog.
Syslog IP Address	Enter the IP Address of your syslog server.
Log Facility	Use [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 details.
Types:	
CDR	Call Detail Record (CDR) logs all data phone line activity if set to **Yes.**
Packet Triggered	The first 48 bytes or octets and protocol type of the triggering packet is sent to the UNIX syslog server when this field is set to **Yes.**
Filter Log	No filters are logged when this field is set to **No.** Filters with the individual filter **Log Filter** field set to **Yes** are logged when this field is set to **Yes.**
PPP Log	PPP events are logged when this field is set to **Yes.**
POTS Log	Voice calls are logged when this field is set to **Yes.**

Your Prestige sends five types of syslog messages. Please see Enhanced Syslog in the Appendix for the message format. Some examples of these syslog messages are shown next:

1. CDR

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

C02 CLID call refused
L02 Call Terminated
C02 Call Terminated

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

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

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

2. Packet Triggered

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

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

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

Jul 19 11:29:06 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1,
Data=4500002824014000 1f06ac12c0a86614ca849a7b0427001700195b451d14301350040000776000000
```

3. Filter Log

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

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

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

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

4. PPP Log

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

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

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

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

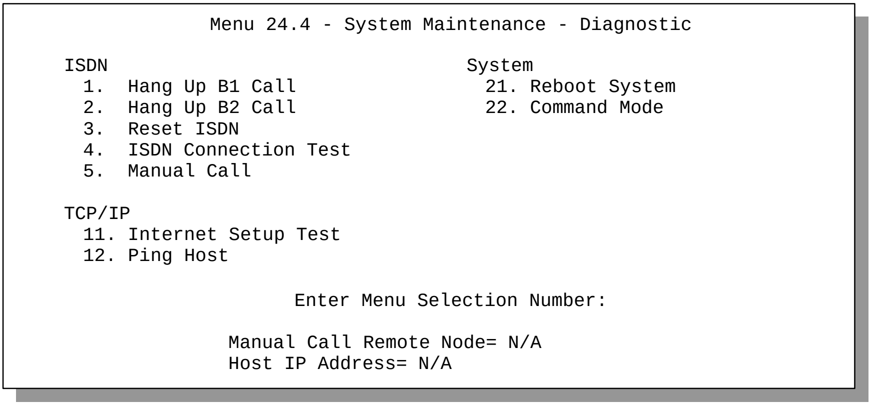
5. POTS Log

POTS Log
SdcmdSyslogSend (SYSLOG_POTSLOG, SYSLOG_NOTICE, String);
String = Call Connect / Disconnect: Dir = xx Remote Call= xxxxx Local Call= xxxxx
Dir = Call Direction 1: Incoming call 2: Outgoing call
Remote Call = a string type which represents as the remote call number
Local Call = a string type which represents as the my (local) call number

```
Jul 19 12:08:25 192.168.102.2 ZyXEL Communications Corp.: Call Connect: Dir=2 Remote
Call=40002 Local Call=1

Jul 19 12:08:29 192.168.102.2 ZyXEL Communications Corp.: Call Disconnect: Dir=2 Remote
Call=40002 Local Call=1

Jul 19 12:08:34 192.168.102.2 ZyXEL Communications Corp.: Call Connect: Dir=2 Remote
Call=40001 Local Call=2
```

12.3 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 in the following figure.



```
                     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 12-8 Menu 24.4 – System Maintenance – Diagnostic

Follow the procedure next 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**.

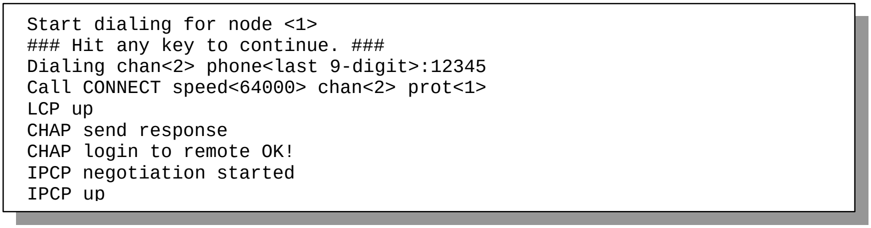
The following table describes the diagnostic tests available in Menu 24.4 for your Prestige and the connections.

Table 12-4 System Maintenance Menu Diagnostic

FIELD	DESCRIPTION
Hang Up B1 Call	This tool hangs up the B1 channel. It is only applicable if the B1 channel is currently in use.
Hang Up B2 Call	This tool hangs up the B2 channel. It 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. The following 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. It allows you to diagnose and test your Prestige using a specified set of commands.
Manual Call Remote Node	If you entered **5** above, then enter the remote node number (with reference to the remote node listing on Menu 11 – Remote Node Setup) you wish to call.
Host IP Address	If you entered **12** above, then enter the IP address of the machine you want to ping in this field.

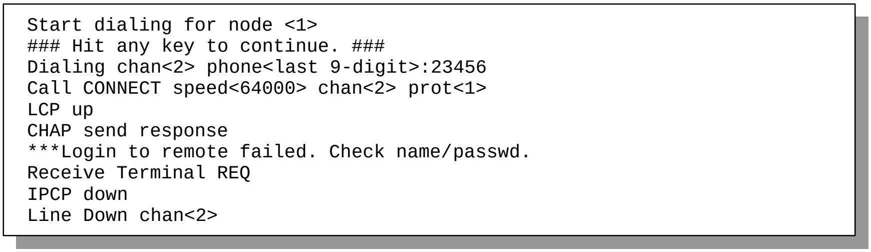
The following figure shows an example of a successful connection after selecting option **Manual Call** in Menu 24.4.



```
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 12-9 Display for a Successful Manual Call

This figure shows an example where authentication failed.



```
Start 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 12-10 Display for a Failed Authentication

12.4 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., P202.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., P202.bin. Rename the configuration filename to “rom-0” and the firmware filename to “ras” when transferring files to the Prestige (i.e., the internal filenames on the Prestige). Renaming the files is not necessary when you transfer files to the Prestige using the XMODEM protocol.

The following table is a summary. Please note that the internal filename refers to the filename on the Prestige and the external filename refers to the filename not on the Prestige, i.e., on your workstation, local network, or ftp site and so the name (but not the extension) will vary. The AT command is the command you enter after you press “Y” when prompted in the SMT menu to go into debug mode. After uploading the new firmware see the **ZyNOS F/W Version** field in **Menu 24.2.1** to check if you have uploaded the correct firmware version.

Table 12-5 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION	AT COMMAND
Configuration File	Rom-0	*.rom	This is the router configuration filename on the Prestige. Uploading the rom-0 file replaces the entire ROM file system, including your Prestige configurations, system-related data (including the speed and default password), the error log and the trace log.	ATLC
Firmware	Ras	*.bin	This is the generic name for the ZyNOS firmware on the Prestige.	ATUR

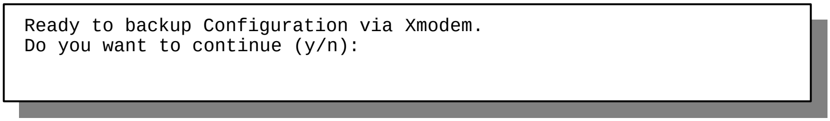
12.5 Backup Configuration

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

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

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

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



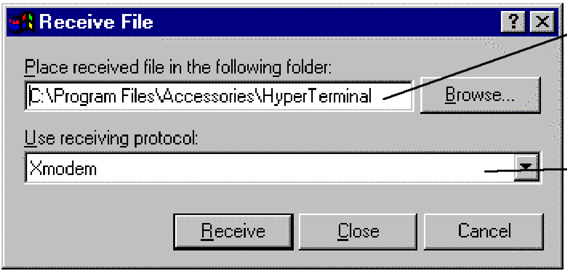
```
Ready to backup Configuration via Xmodem.
Do you want to continue (y/n):
```

Figure 12-11 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.



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

Use receiving protocol: Xmodem

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

Choose the XMODEM Protocol.

Figure 12-12 HyperTerminal Screen

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

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

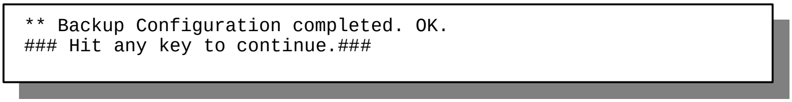

```
** Backup Configuration completed. OK.
### Hit any key to continue.###
```

Figure 12-13 Successful Backup

12.6 Restore Configuration

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

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

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

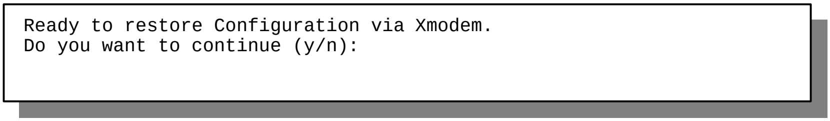
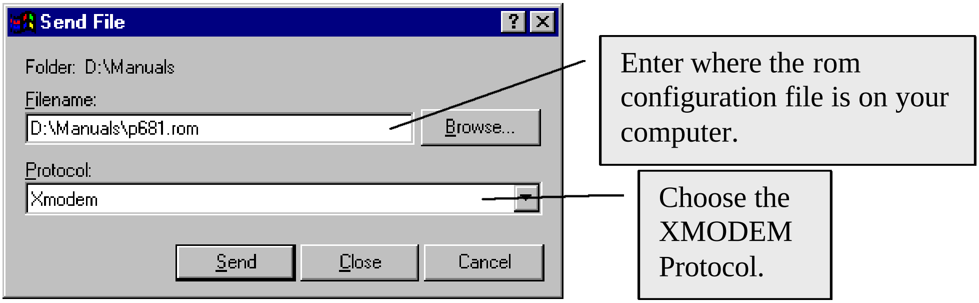

```
Ready to restore Configuration via Xmodem.
Do you want to continue (y/n):
```

Figure 12-14 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.



Folder: D:\Manuals

Filename: D:\Manuals\p681.rom

Protocol: Xmodem

Enter where the rom configuration file is on your computer.

Choose the XMODEM Protocol.

Figure 12-15 HyperTerminal Screen

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

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

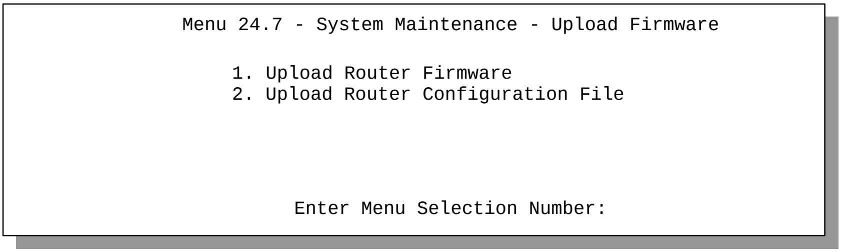
```
Save to ROM
Hit any key to start system reboot.
```

Figure 12-16 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.

12.7 Upload Firmware

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



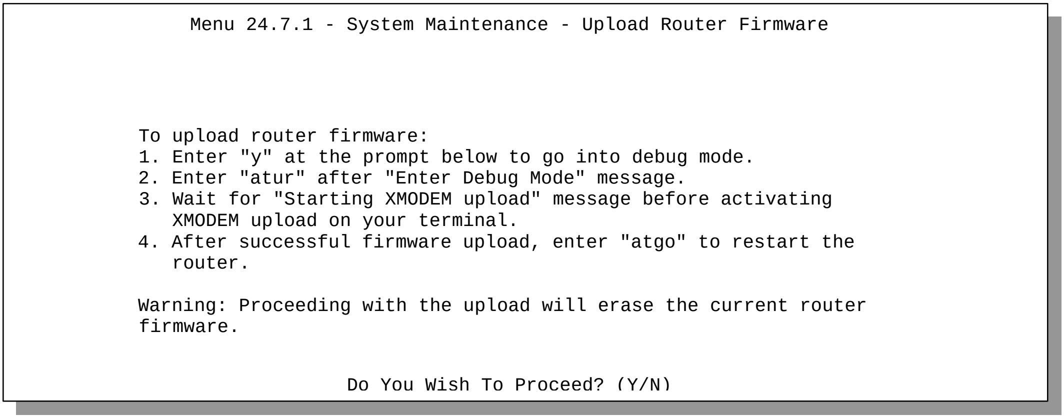
```
                Menu 24.7 - System Maintenance - Upload Firmware

                     1. Upload Router Firmware
                     2. Upload Router Configuration File





                           Enter Menu Selection Number:
```

Figure 12-17 Menu 24.7 – System Maintenance – Upload Firmware

12.7.1 Upload Router Firmware

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

1. Enter “`atur`” after the “`Enter Debug Mode`” message.
2. Wait for the “`Starting XMODEM upload`” message before activating XMODEM upload on your terminal.
3. After successful firmware upload, enter “`atgo`” to restart the Prestige.



```
               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 12-18 Menu 24.7.1 – Uploading Router Firmware

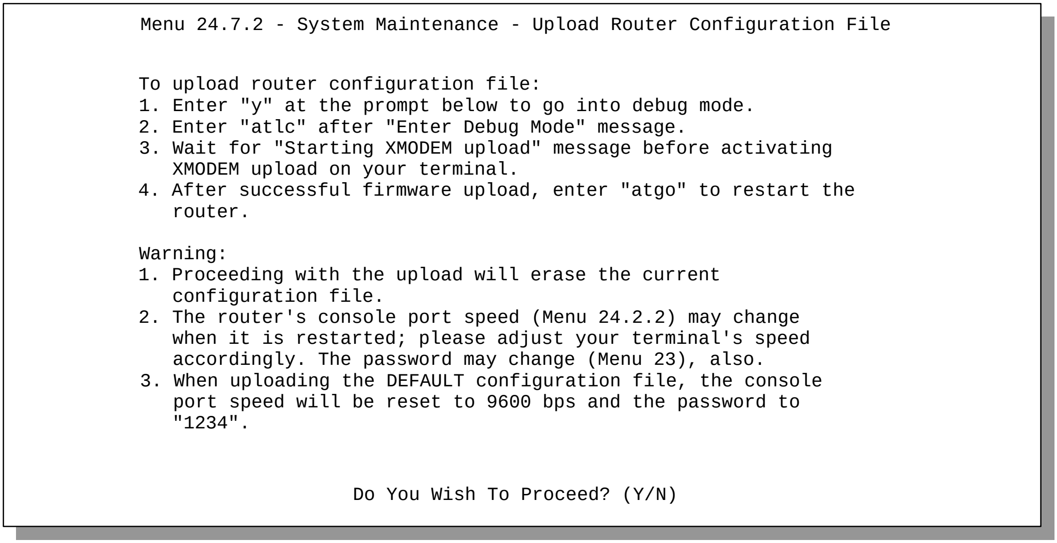
12.7.2 Uploading Router Configuration File

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

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

1. Enter “`atlc`” after the “`Enter Debug Mode`” message.
2. Wait for the “`Starting XMODEM upload`” message before activating XMODEM upload on your terminal.
3. After successful firmware upload, enter “`atgo`” to restart the Prestige.

If you replace the current configuration file with the default configuration file, i.e., p202.rom, you will lose all configurations that you had before and the speed of the console port will be reset to the default of 9600 bps with 8 data bit, no parity, 1 stop bit (8n1) and no Flow Control. You will need to change your serial communications software to the default before you can connect to the Prestige again. The password will be reset to the default of 1234, also.



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


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

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



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

Figure 12-19 Menu 24.7.2 – System Maintenance – Upload Router Configuration File

12.7.3 TFTP Transfer

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

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

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

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

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

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

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

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

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

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

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

ftp> put P202.bin ras
This is a sample ftp session showing the transfer of the PC file "P202.bin" to the Prestige.

ftp> get rom-0 MyP202.cfg
This is a sample ftp session saving the current configuration to the PC file MyP202.cfg.

Using the FTP Command From the DOS Prompt

Step 1. Launch the FTP client on your workstation.

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

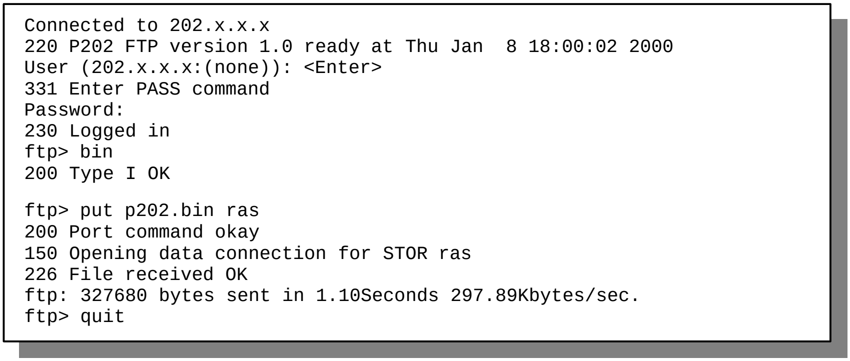
Step 3. You may press [Enter] when prompted for a username.

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

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

Step 6. Use **`put`** to transfer files from the workstation to the Prestige, e.g., **`put p202.bin ras`** transfers the firmware on your computer (p202.bin) to the Prestige and renames it "ras". Similarly **`put p202.rom rom`** transfers the configuration file on your computer (p202.rom) to the Prestige and renames it "rom".

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



```
Connected to 202.x.x.x
220 P202 FTP version 1.0 ready at Thu Jan  8 18:00:02 2000
User (202.x.x.x:(none)): <Enter>
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK

ftp> put p202.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 327680 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 12-20 Sample FTP Session

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

Table 12-6 Third Party FTP Clients – General Fields

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

The following is a sample tftp command:

```
TFTP [-i] host put p202.bin ras
```

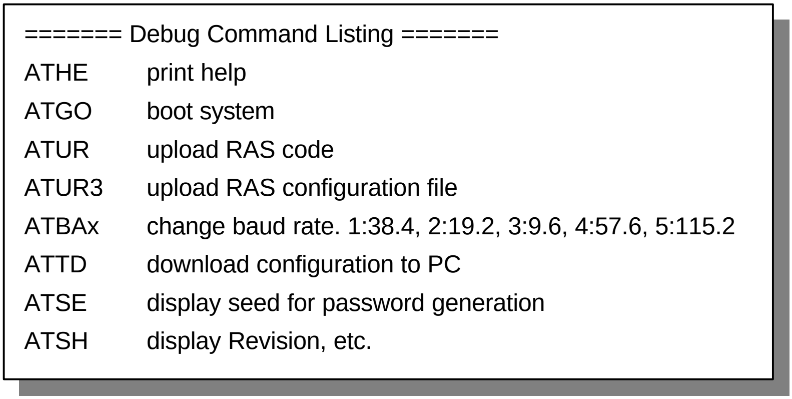
where "**i**" specifies binary image transfer mode (use this mode when transferring binary files), "**host**" is the Prestige IP address, "**put**" transfers the file source on the workstation (p202.bin – name of the firmware on the workstation) to the file destination on the remote host (ras – name of the firmware on the Prestige).

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

Host	Enter the IP address of the Prestige. 192.168.1.1 is the Prestige default IP address when shipped.
Send/Fetch	Press **`Send`** to upload the file to the Prestige and **`Fetch`** to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the Prestige. The filename for the firmware is **`ras`** and for the configuration file, is **`rom-0`**.
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

12.7.4 Boot Module Commands

Prestige boot module commands are shown next. For ATBAx, x denotes the number preceding the colon to give the console port speed following the colon in the list of numbers that follow; 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.

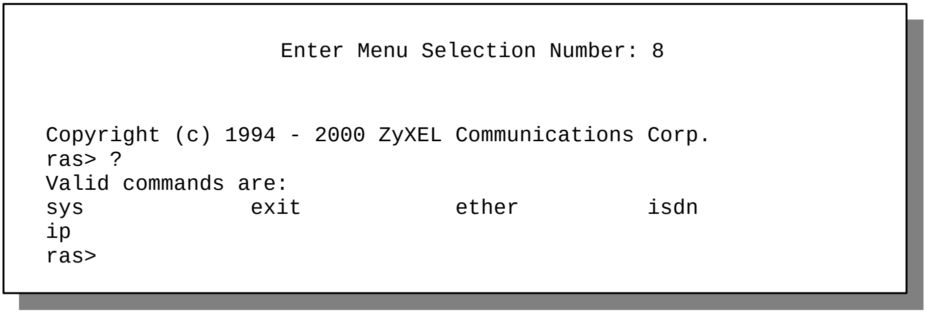


```
======= Debug Command Listing =======
ATHE     print help
ATGO     boot system
ATUR     upload RAS code
ATUR3    upload RAS configuration file
ATBAx    change baud rate. 1:38.4, 2:19.2, 3:9.6, 4:57.6, 5:115.2
ATTD     download configuration to PC
ATSE     display seed for password generation
ATSH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

Figure 12-21 Boot Module Commands

12.8 Command Interpreter Mode

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



```
                      Enter Menu Selection Number: 8


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

Figure 12-22 Command Mode

12.9 Call Control

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

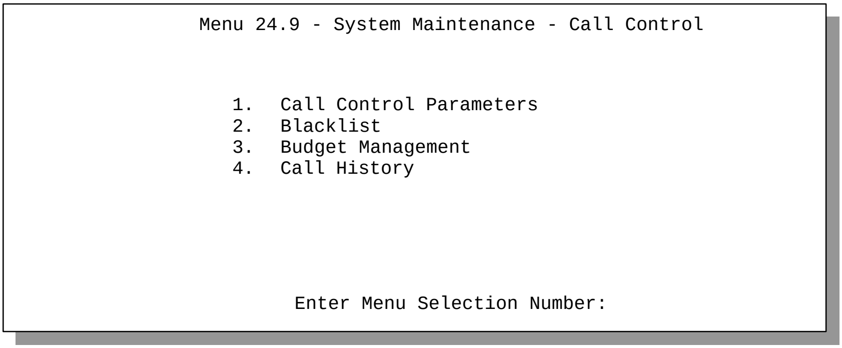
Call control parameters allows you to set a dial out time limit, the number of times a number should be called before it is added to the blacklist and the interim between calls.

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 placed on 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.

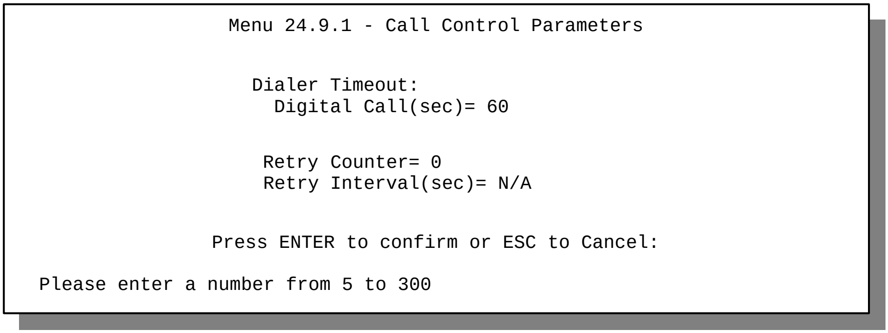
To enter the call control menu, select option **9. Call Control** in Menu 24 to go to Menu 24.9 – System Maintenance – Call Control, as shown in the following figure.



```
                 Menu 24.9 - System Maintenance - Call Control



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






                         Enter Menu Selection Number:
```

Figure 12-23 Menu 24.9 – System Maintenance – Call Control

12.9.1 Call Control Parameters



```
                    Menu 24.9.1 - Call Control Parameters


                      Dialer Timeout:
                        Digital Call(sec)= 60


                       Retry Counter= 0
                       Retry Interval(sec)= N/A


                  Press ENTER to confirm or ESC to Cancel:

   Please enter a number from 5 to 300
```

Figure 12-24 Call Control Parameters

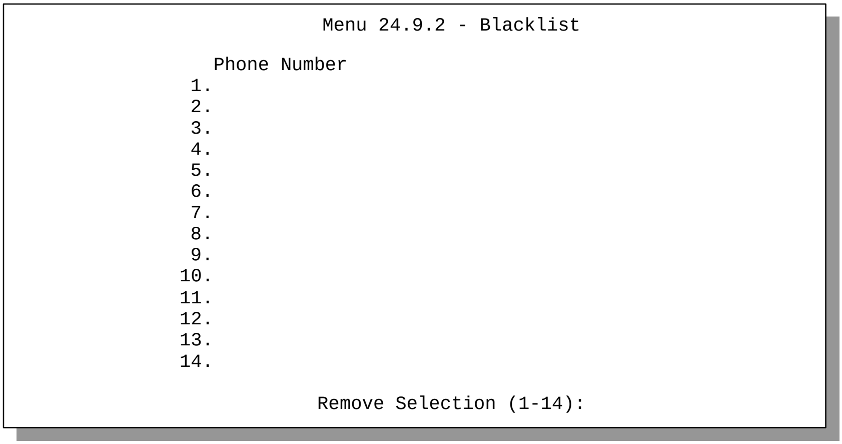
Table 12-7 Call Control Parameters Fields

FIELD	DESCRIPTION
Dialer Timeout: Digital Call (sec)	The Prestige will timeout if it cannot 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.

12.9.2 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 a blank list of telephone numbers that have been blacklisted.

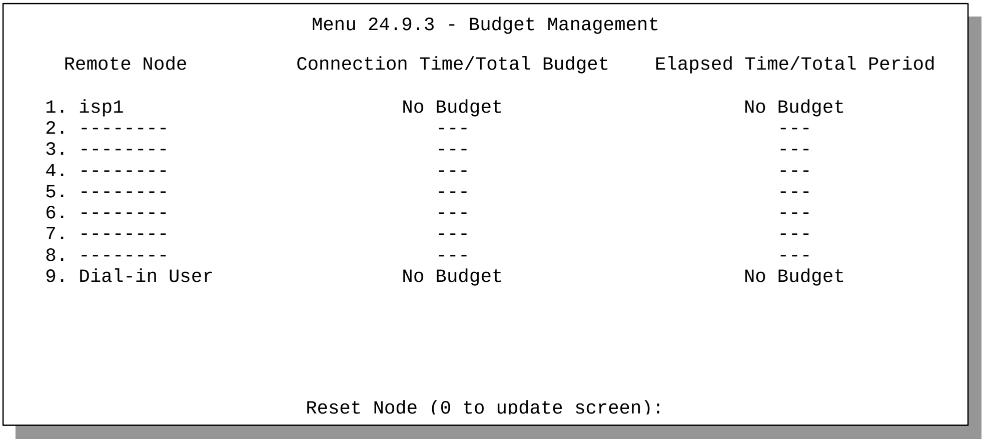


```
                          Menu 24.9.2 - Blacklist

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

                         Remove Selection (1-14):
```

Figure 12-25 Menu 24.9.2 – Blacklist

12.9.3 Budget Management

Menu 24.9.3 shows the budget management statistics for outgoing calls.



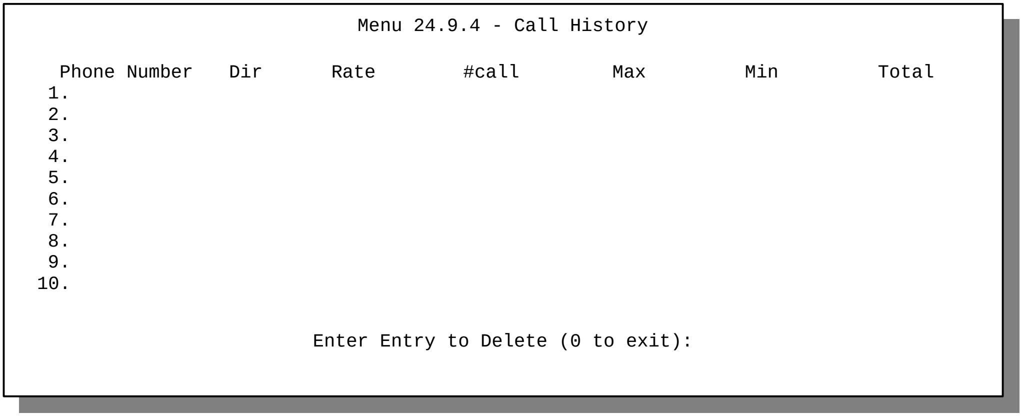
```
                        Menu 24.9.3 - Budget Management

    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 12-26 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 Menu 11 and 13 for a remote node and for the dial-in user, respectively.

12.9.4 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 12-27 Call History

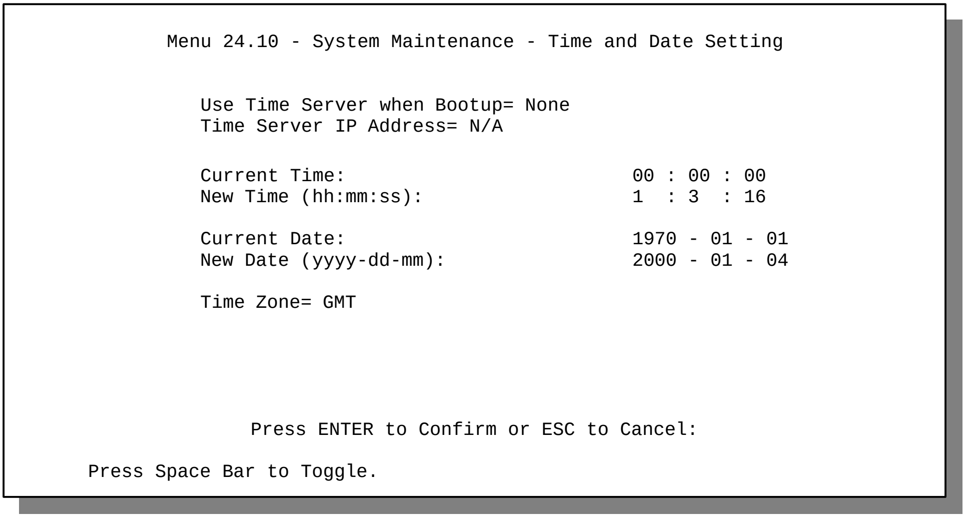
Table 12-8 Call History Fields

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.

12.10 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 we have a software mechanism to get the current time and date from an external server when you power up your Prestige. **Menu 24.10** does just that – it allows you to update the time and date settings of your Prestige. The real time is then displayed in the Prestige error logs. If you do not choose a time service protocol that your time server will send when the Prestige powers up you can enter the time manually but each time the system is booted, the time and date will be reset to **1970/1/1 0:0:0**.



```
              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 (yyyy-dd-mm):                2000 - 01 - 04

                 Time Zone= GMT




                     Press ENTER to Confirm or ESC to Cancel:

       Press Space Bar to Toggle.
```

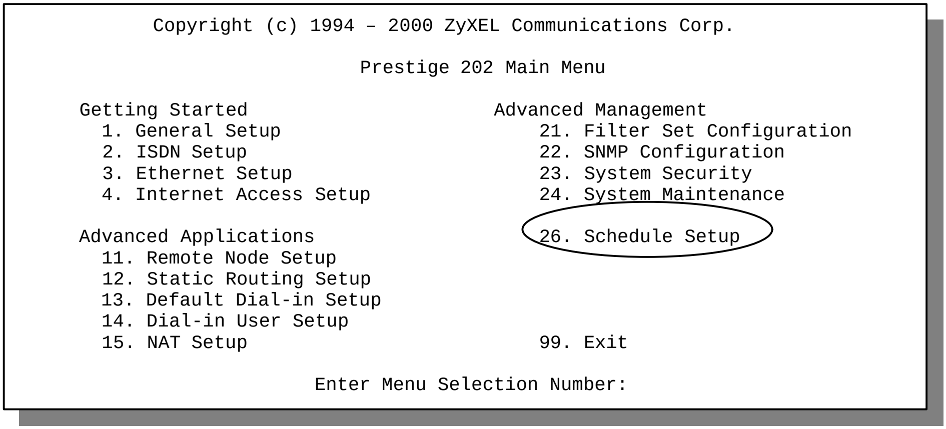
Figure 12-28 System Maintenance – Time and Date Setting

Table 12-9 Time and Date Setting Fields

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

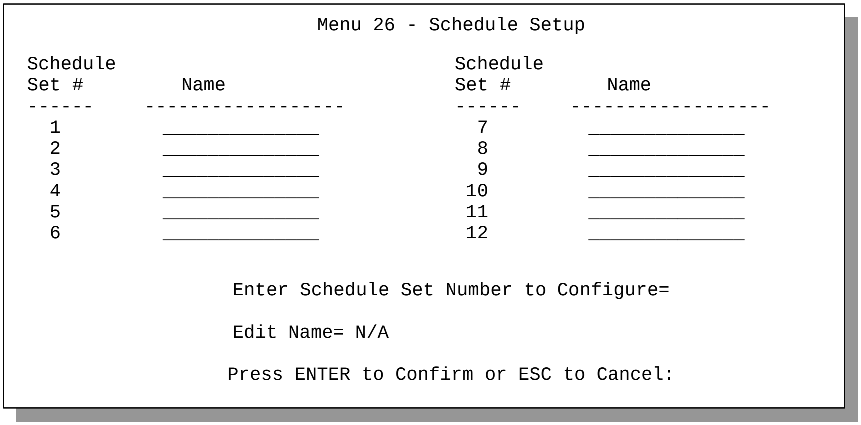
Chapter 13
Call Scheduling

The call scheduling feature allows the Prestige to manage a remote node and dictate when a remote node should be called and for how long. This feature is 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 – 2000 ZyXEL Communications Corp.

                              Prestige 202 Main Menu

    Getting Started                        Advanced Management
      1. General Setup                         21. Filter Set Configuration
      2. ISDN Setup                            22. SNMP Configuration
      3. Ethernet Setup                        23. System Security
      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 13-1 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= N/A

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

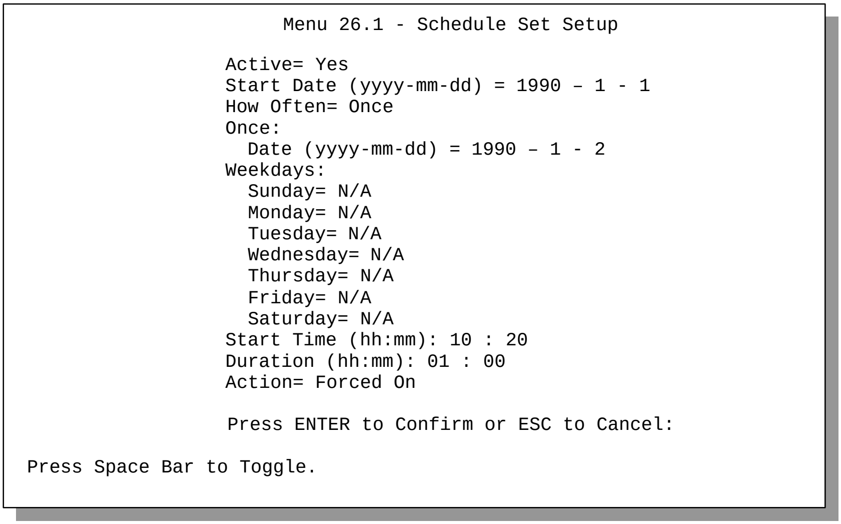
Figure 13-2 Schedule Setup

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.

NOTE: To delete a schedule set, enter the set number and press [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 to 12) and press [Enter] to see **Menu 26.1 – Schedule Set Setup** as shown next.



```
                         Menu 26.1 - Schedule Set Setup

                    Active= Yes
                    Start Date (yyyy-mm-dd) = 1990 – 1 - 1
                    How Often= Once
                    Once:
                      Date (yyyy-mm-dd) = 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:

Press Space Bar to Toggle.
```

Figure 13-3 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.

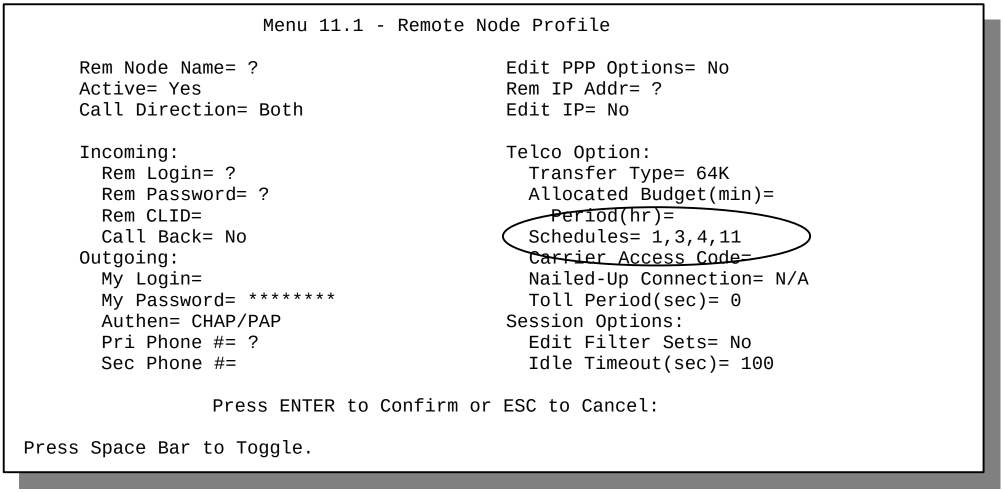
Once the connection is dropped manually or it times out, then that remote node cannot be triggered up until the end of the **Duration**.

Table 13-1 Schedule Set Setup Fields

FIELD	DESCRIPTION	OPTION
Active	Press [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 [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.	
Weekdays: 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 [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 [space bar] to toggle between these options. Choose one and then press [Enter].	**Forced On/ Forced Down/ Enable Dial-On-Demand/Disable Dial-On-Demand.**

13.1.1 Applying a Schedule Set

After you have 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.



```
                       Menu 11.1 - Remote Node Profile

      Rem Node Name= ?                      Edit PPP Options= No
      Active= Yes                           Rem IP Addr= ?
      Call Direction= Both                  Edit IP= No

      Incoming:                             Telco Option:
        Rem Login= ?                          Transfer Type= 64K
        Rem Password= ?                       Allocated Budget(min)=
        Rem CLID=                               Period(hr)=
        Call Back= No                         Schedules= 1,3,4,11
      Outgoing:                               Carrier Access Code=
        My Login=                             Nailed-Up Connection= N/A
        My Password= ********                 Toll Period(sec)= 0
        Authen= CHAP/PAP                    Session Options:
        Pri Phone #= ?                        Edit Filter Sets= No
        Sec Phone #=                          Idle Timeout(sec)= 100

                  Press ENTER to Confirm or ESC to Cancel:

 Press Space Bar to Toggle.
```

Figure 13-4 Applying Schedule Set(s) to a Remote Node

Part IV:

TROUBLESHOOTING

Chapter 14 provides information about solving common problems, some Appendices, Acronyms and Abbreviations, as well as an Index.

Chapter 14
Troubleshooting

This chapter covers the potential problems you may run into and the possible remedies.

After each problem description, some instructions are provided to help you diagnose and solve it.

14.1 Problems Starting Up the Prestige

Table 14-1 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 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. It should be configured as follows:</td><td>VT100 terminal emulation.</td></tr>
<tr><td>9600 bps is the default speed of the Prestige upon leaving the factory. Try other speeds in case it has been changed.</td></tr>
<tr><td>No parity, 8 Data bits, 1 Stop bit, No Flow Control.</td></tr>
</table>

14.2 Problems With the ISDN Line

Table 14-2 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 **2**, there is an SPID error (North America only). Check the SPID numbers again in Menu 2 and if they are correct, re-initialize them from Menu 24.4.3. If the code is **3**, this indicates a general failure. Verify the provisioning information for your switch by contacting your telephone company.
	Check your SPID numbers if the ISDN LED is blinking slowly as this indicates that SPID negotiation has failed (North America only).
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 second 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.

14.3 Problems With the LAN Interface

Table 14-3 Troubleshooting the LAN Interface

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

14.4 Problems Connecting to a Remote Node or ISP

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

PROBLEM	CORRECTIVE ACTION
Cannot connect to a remote node or ISP.	Check Menu 24.1 to verify the line status. If it indicates [down], then refer to the section on the line problems.
	In Menu 24.4.5, do a manual call to that remote node. Observe the messages and take appropriate actions.

14.5 Problems for Remote User to Dial-in

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

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

Appendix A
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	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
SPID	Service Profile Identifier
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

Appendix B Enhanced Syslog

The following are the message formats that Syslog sends to the server.

CDR

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

Packet Triggered

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

Filter Log

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

PPP Log

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

POTS Log

```
SdcmdSyslogSend (SYSLOG_POTSLOG, SYSLOG_NOTICE, String);
String = Call Connect / Disconnect: Dir = xx Remote Call= xxxxx Local Call= xxxxx
Dir = Call Direction 1: Incoming call 2: Outgoing call
Remote Call = a string type which represents as the remote call number
Local Call = a string type which represents as the my (local) call number
```

Appendix C Power Adapter Specifications

AC POWER ADAPTER SPECIFICATIONS
North America
AC Power Adapter model: AD48-1201200DUY Input power: AC 120Volts/60Hz/0.25A Output power: DC 12Volts/1.2A Power consumption: 11W Plug: North American standards Safety standards: UL; CUL (UL 1950, CSA C22.2 No.234-M90)
European Union
AC Power Adapter model: AD-1201200DV Input power: AC 230Volts/50Hz/0.2A Output power: DC 12Volts/1.2A Power consumption: 9.5W Plug: European Union standards Safety standards: TUV, CE (EN 60950)
AC Power Adapter model: JAD-121200E Input power: AC 230Volts/50Hz Output power: DC 12Volts/1.2A Power consumption: 9.5W Plug: European Union standards Safety standards: TUV, CE (EN 60950)

Index