Prestige 1600

Universal Access Concentrator

ZyNOS Version 3.20

Dec. 2000

Configuration and Management Guide

ZyXEL

TOTAL INTERNET ACCESS SOLUTION

Prestige 1600

Universal Access Concentrator

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 patents rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

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

ZyXEL Limited Warranty

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

Note

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

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

Customer Support

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

When Contacting Customer Support Representative

When you contact your customer support representative, have the following information ready:

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

Method Location	E-MAIL - Support/ Sales	Telephone/Fax	Web Site/ FTP Site	Regular Mail
Worldwide	support@zyxel.com.tw support@europe.zyxel.com sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, HsinChu, Taiwan 300, R.O.C.
North America	support@zyxel.com sales@zyxel.com	+1-714-632-0882 800-255-4101 +1-714-632-0858	www.zyxel.com ftp.zyxel.com	ZyXEL Communications Inc., 1650 Miraloma Avenue, Placentia, CA 92870, U.S.A.
Scandinavia	support@zyxel.dk sales@zyxel.dk	+45-3955-0700 +45-3955-0707	www.zyxel.dk ftp.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark.
Austria	support@zyxel.at sales@zyxel.at	+43-1-4948677-0 +43-1-4948678	www.zyxel.at ftp.zyxel.at	ZyXEL Communications Services GmbH. Thaliastrasse 125a/2/2/4 A-1160 Vienna, Austria
Germany	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A4 D-52146 Wuerselen, Germany

Table of Contents

List of Figures

List of Tables

Preface

Congratulations on your purchase of the Prestige 1600 Universal Access Concentrator.

This preface introduces you to your concentrator and discusses the organization and conventions of this user's guide. It also provides information on other related documentation.

About the Prestige

The Prestige 1600 is a scalable access concentration platform, delivering networking services at multiple selectable speeds. It can be deployed at high rise buildings, Telcos, ISPs and System Integrators with various configurations.

Equipped with one 10/100M Ethernet port, three network module Slots, and one WAN interface and one optional five-port 10M/100M LAN switch card, the architecture of the Prestige 1600 allows network modules of different generations to coexist in the same chassis and to inter-operate with the same system module.

Network Modules

IDSL

Each Prestige 1600 IDSL network module (NM) consists of 16 IDSL ports. You can install 2 IDSL NMs in a Prestige, which is equipped with a 10/100M Ethernet that allows you to daisy chain up to five units (giving a maximum of 160 IDSL ports).

ADSL

Each Prestige 1600 ADSL network module (NM) consists of 8 ADSL ports. You can install 3 ADSL NMs in a Prestige, which is equipped with a 10/100M Ethernet that allows you to daisy chain up to five units (giving a maximum of 120 ADSL ports).

SDSL

Each Prestige 1600 SDSL network module (NM) consists of 8 SDSL ports. You can install 3 SDSL NMs in a Prestige, which is equipped with a 10/100M Ethernet that allows you to daisy chain up to five units (giving a maximum of 120 SDSL ports).

Please note that slot 3 may contain an ADSL or SDSL network module type only.

The Prestige can automatically detect the network module type.

Configuring your Prestige

You can use the System Management Terminal (SMT) interface or the CLI (Command Line Interpreter) commands to configure your Prestige. The SMT is a menu-driven interface that you can access from either a VT100 compatible terminal or a terminal emulation program on a computer via the console port or telnet. Use of CLI/CI commands are recommended only for advanced users.

About this Guide

This User's Guide covers all operations of the Prestige 1600 and shows you how to get the best out of the multiple advanced features of your Prestige concentrator. It is designed to help you to configure the Prestige correctly for various applications using the SMT interface via the console port or telnet. For detailed CI commands please refer to the section *Related Documentation*.

Syntax Conventions

"Enter" means for you to type one or more characters and press the carriage return. "Select" or "Choose" means for you to select one from the predefined choices.

The SMT menu titles and labels are in **Bold Times** font. The choices of a menu item are in **Bold Arial** font. A single keystroke is in Arial font and enclosed in square brackets, for instance, [ENTER] means the Enter, or carriage return, key; [ESC] means the Escape key.

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

The Prestige 1600 will also be referred to as the Prestige or the P1600 in this manual.

Related Documentation

Hardware Installation Guide

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 pages at zyxel.com.

ZyXEL Web Page and FTP Server Site

You can access release notes as well as firmware upgrades at ZyXEL web and FTP sites. Refer to the Customer Support page in this User’s Guide for more information.

What is DSL?

DSL stands for Digital Subscriber Line. Local Exchange carriers currently use a single unshielded twisted pair of wire on the local loop (between Central Office and Customer Premises) for transmitting voice, which requires 300-3,400 Hz of bandwidth. The wires are, however, capable of carrying information at much higher rate when modern digital processing techniques are deployed. The same pair of wires are used successfully worldwide to provide ISDN services yielding up to 128 Kbps. The explosive growth in Internet access, remote LAN access and telecommuting demand data rates that are a lot higher than what conventional analog modems can provide over the existing pair of wires.

SDSL (Symmetric DSL)

SDSL operates on a single copper pair. SDSL allows applications that require symmetric data rates. Because only one pair is needed in this arrangement, the capacity of the entire local loop infrastructure is greatly magnified. With this capability, local providers can extract the maximum value from their existing plant, or deploy new capacities both more quickly and at a lower capital expenditure.

SDSL allows for rapid and cost effective deployment of intermediate data rate services. Potential uses for this technology include fractional T1 with a particular advantage in 768 Kbps systems, Work-at-home LAN access, Distance Learning, Internet Access, and Campus or Large Facility LAN to LAN connectivity. Since SDSL can be configured at multiple data rates, it can have different capacity and reach limitations.

This also allows for easy, cost-effective implementation of such services as remote cell site support of PCs, remote LAN access, distance education and training, digital imaging, or any other service, which requires a larger amount of bandwidth.

ADSL (Asymmetric DSL)

Asymmetric Digital Subscriber Line takes its name from the comparatively high bandwidth in one direction, with low bandwidth in the opposite direction. ADSL uses a single phone line for transmission. Many service providers have also come to recognize its potential to support a range of data applications.

Additionally, ADSL’s ability to operate at speeds of up to 8 Mbps positions it to support real-time broadcast services and pre-recorded interactive video services; and to have multiple video and data activities running simultaneously. ADSL supports applications with asymmetric traffic demands such as:

- Web Surfing
- File Downloads
- Distance Learning

IDSL (ISDN DSL)

IDSL stands for ISDN Digital Subscriber Line (IDSL). IDSL uses the 2B1Q line coding standard for ISDN BRI circuits. Used for data-only applications, IDSL operates at 128 Kbps for up to 18,000 feet.

Because IDSL uses the same industry-standard line coding technique as ISDN, customers with ISDN BRI terminal adapters can use their current TAs, routers and bridges for connecting to IDSL lines. Any of the commonly used transport protocols such as PPP, MP, or Frame Relay may be used over the IDSL line, allowing rapid and transparent integration into Internet, remote LAN access and telecommuting.

DSL Comparison Chart

Technology	**Downstream Rate**	**Upstream Rate**	**Wires**	**CO distance**
IDSL	128 Kbps	128 Kbps	1 Copper Pair	18,000 feet
ADSL	256Kbps to 6.1 Mbps	64 Kbps to 512 Kbps	1 Copper Pair	18,000 feet
SDSL	144 Kbps to 2320 Kbps	144 Kbps to 2320 Kbps	1 Copper Pair	11,500 to 22,000 feet

Chart A DSL Comparison Chart

Chapter 1
Getting to Know Your Concentrator

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

The Prestige 1600 is a scalable, high-performance, easy-to-configure access concentrator. It consolidates multiple traffic streams onto a single backbone network. It can be deployed at either the customer's premise (CP) or a service provider's Central Office (CO).

Equipped with one 10/100M Ethernet port, three network module (NM) slots, one WAN interface and one optional five-port 10M/100M LAN switch card, the architecture of the Prestige 1600 allows network modules of different generations to coexist in the same chassis and to inter-operate with the same system module.

With its flexible and scalable architecture, you can start with a single P1600 chassis to address low or medium density network requirements and expand with up to four additional P1600s. With the optional five-port 10/100M Ethernet switch installed, you can connect up to five units.

1.1 Overview of the Prestige 1600

Physical Dimensions

- Chassis: 17.3" (W) x 13.39" (L) x 2.6" (H); 44cm (W) x 34cm (L) x 6.6cm (H)
- DSL network module: 5.3" (W) x 12.2" (L) x 0.94" (H); 13.5cm (W) x 31cm (L) x 2.4cm (H)
- Rack-mounting options: EIA 19" or 23" front or mid-mount central-office style

Power Requirement

- Built-in 100V-240VAC, 50-60 Hz switching power supply

Operating Environment

- Temperature: 0ºC - 50º C
- Humidity: 20 - 95%

IDSL Interface

- Two 16-port IDSL network modules.
- Up to 160 IDSL ports. 32 IDSL ports in each P1600 chassis.
- IDSL Server only

ADSL Interface

- Three 8-port ADSL network modules.
- Up to 120 ADSL ports (112 if using the 5-port Ethernet switch card). 24 ADSL ports in each P1600 chassis.

SDSL Interface

- Three 8-port SDSL network modules.
- Up to 120 SDSL ports (112 if using the 5-port Ethernet switch card). 24 SDSL ports in each P1600 chassis.

Network Address Translation (NAT)

NAT (Network Address Translation - NAT, RFC 1631) allows the translation of an Internet Protocol address used within one network to a different IP address known within another network.

Internet Protocols

- IP routing
- IP packet filtering, including network level and device level filtering
- RIP-1 and RIP-2
- Static IP Route
- MultiNAT for multiple-IP address translation

Ethernet Interface

- Auto-negotiating 10/100M Fast Ethernet port

WAN Interface

- FlexWAN port.

PPP Support

- PPP for WAN connection

Network Management

- Local and remote console management
- SNMP manageable
- Remote secondary management via Telnet using MultiNAT

Security

- CHAP, PAP and RADIUS authentication

Remote Firmware Upgrades

- Console, Telnet, TFTP and FTP Firmware Upgrades

1.2 Key Benefits

- Flexibility, Scalability and High capacity (120 to160 DSL ports with daisy chaining)
- MultiNAT Support
- Mix of DSL types on a single access platform using the existing network infrastructure.
- Reduced network complexity and easy manageability
- Greater bandwidth efficiency
- High speed DSL platform
- Variety of network interfaces and easy upgradability
- Consolidated access to network services over a single carrier
- Cost, space and power efficient solution for Internet access
- SNMP support

- Monitoring of WAN/LAN status and port status
- Diagnostics
- Safety tested and high security

1.3 Detailed Features of the Prestige 1600

Modular Architecture

The P1600 chassis is equipped with three network module slots, one system module and two removable fan modules.

Configuration Types

The Prestige 1600 can be configured via SMT Menu 1 as a primary, secondary or standalone device.

1. **Primary**

The P1600 primary provides concentration, network management, Internet access and routing functions as well as uses the FlexWan port as the interface to the trunk.

2. **Secondary**

The P1600 secondary provides concentration, network management, Internet access and routing functions as well but only through the LAN interface. A secondary needs to work with a primary device because for WAN access, you need to connect to a P1600 primary.

3. **Standalone**

Standalone SMT configurations are the same as a secondary, but in this configuration mode, it does not have to work with a primary. You can connect a router directly to its LAN port.

Network Interfaces

The P1600 has two trunk interfaces: one Ethernet and one WAN port (primary mode only). The WAN port supports RS-232, EIA 530,RS-422, X.21 and V.35 interfaces.

Network Protocol Support

The P1600 supports the following network protocols:

- TCP/IP (Transmission Control Protocol/Internet Protocol) network layer protocol.
- IP Policy Routing
- Routing Information Protocol (RIP-1 and RIP-2)

Full Network Management

Your Prestige 1600 offers you a variety of options for network management. It supports password protected local and remote network management via the console port or a telnet connection. It also supports FTP, TFTP, SNMP (Simple Network Management Protocol) and CI command.

If you cannot telnet to your Prestige, you can configure your Prestige via a modem connected to the console port over a phone line as shown in the next figure.

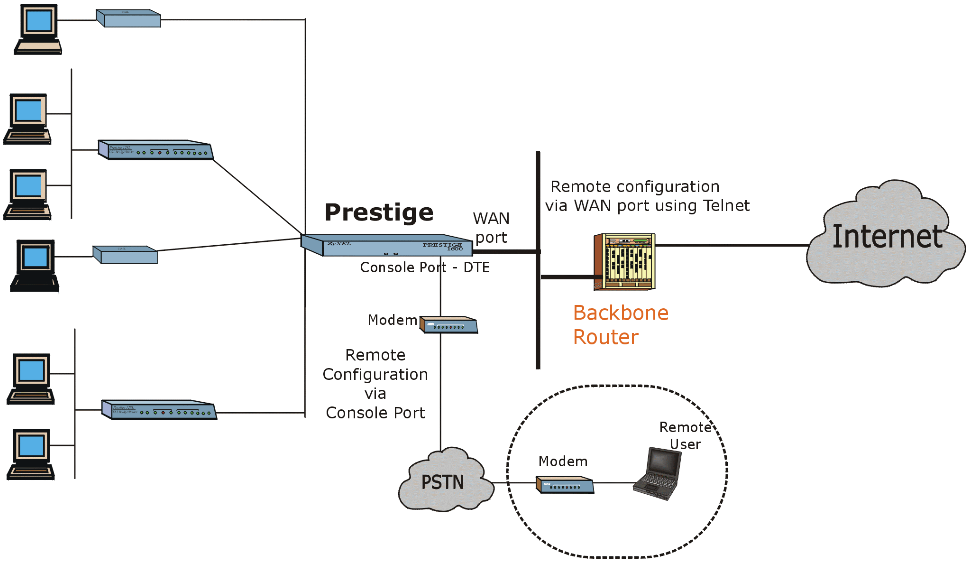

Prestige
WAN port
Console Port - DTE
Remote configuration via WAN port using Telnet
Internet
Backbone Router
Modem
Remote Configuration via Console Port
PSTN
Modem
Remote User

Figure 1-1 Remote Configuration

Please note that for figures in this manual, the "Prestige" refers to the Prestige 1600 and that the Prestige 1600 clients are not labeled - please see the next section.

Robust Security Features

Your Prestige supports CHAP (Challenge Handshake Authentication Protocol), PAP (Password Authentication Protocol) and RADIUS (Remote Authentication Dial in User Service). In addition, the SMT is password protected. You can also configure the LAN, WAN filters to block unwanted incoming and outgoing packets.

Internet Access Sharing

The Prestige 1600 primary support Single User Account (SUA)/Network Address Translation (NAT) which enables multiple subscribers to access the Internet using a single IP address. The ZyXEL Network Operating System (ZyNOS) implementation of SUA/NAT allows NetMeeting, CuSeeMe, ICQ and other multimedia application traffic behind NAT on the client side.

Note that P1600 secondary machine does not support SUA/NAT; only the P1600 primary does on the WAN port. For a P1600 standalone NAT/SUA is supported over LAN when the Ethernet port is connected to a broadband modem.

Remote Software Upgrades

The Prestige 1600 uses FLASH memory technology that enables software upgrades without opening the units. The P1600 can be upgraded via the console port, locally and remotely, as well as via FTP and TFTP.

1.4 Prestige 1600 and Prestige DSL Clients

DSL clients suitable for the Prestige 1600 are shown in the following table.

Table 1-1 P1600 DSL Clients

DSL Network Module	Prestige Client
IDSL	Prestige 100L Omni 128L
ADSL	Prestige 642
SDSL	Prestige 681

Please note that for figures in this manual, the word "Prestige" refers to the Prestige 1600 and that the Prestige 1600 clients are not labeled.

Chapter 2
Prestige 1600 Applications

This chapter shows you some applications of the Prestige 1600.

2.1 Multi Purpose Concentrator

The Prestige 1600 is a highly flexible, high-speed Internet access solution. It is an integrated, cost-effective solution for line concentration, routing and network management. Using the existing infrastructure, service providers (ISPs, Telcos, SIs) and owners of high-rise buildings can take advantage of the DSL technologies using the P1600 concentrator.

2.2 Prestige 1600 Deployment Scenarios

The P1600 concentrator can be deployed at various offices for high-speed Internet Access, campus connectivity and remote access. It can be deployed at an ISP site or at remote sites (MDU, Telcos/CLECs) with various configurations. The P1600 provides two kinds of connection to the ISP: WAN port and Ethernet port. When the P1600 is installed at an ISP site, traffic from the DSL ports is routed to LAN port. When the P1600 is installed at a remote site, traffic is routed to WAN port, then to an ISP.
The P1600 supports RS-232, EIA 530, RS-422, X.21 and V.35 interface types on the WAN port. The P1600 supports Ethernet port interfaces such as a broadband modem. A few P1600 deployment scenarios are shown next.

2.2.1 Deployed at a High-rise for High-Speed Internet Access

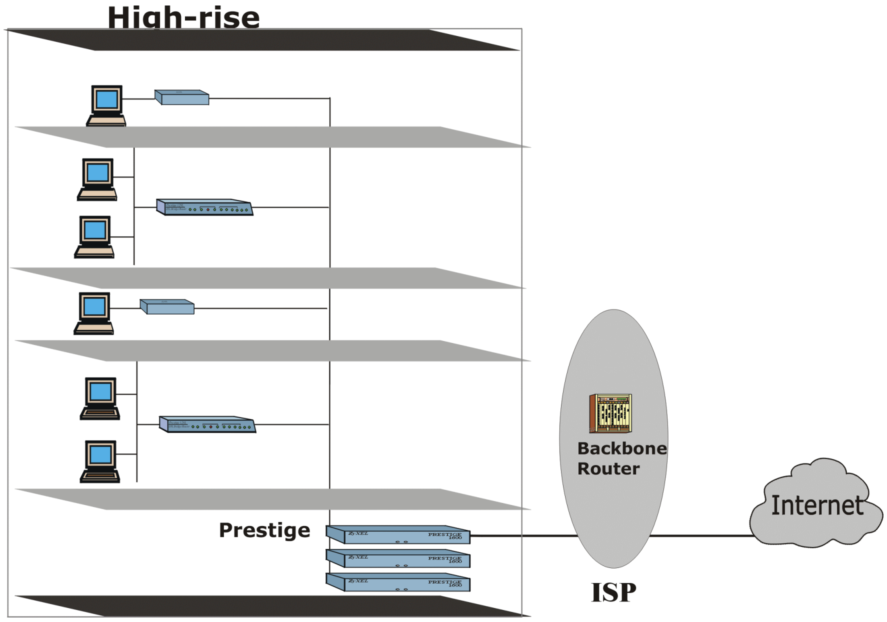


Figure 2-1 Deployed at a High-rise

Property managers or service providers can install the P1600 in Multiple Dwelling Units (MDU) and provide the subscribers with high-speed Internet access and other services.

For Internet access with the P1600 in standalone mode, you can connect a broadband device such as a DSL modem or cable modem to the Ethernet port.

2.2.2 Campus Connectivity

In a campus environment, there are several buildings that need to be interconnected to the computer room. The P1600 offers a long reach and cost effective solution for universities, corporations, etc. to extend networks to multiple buildings spread out over large campuses. It can be deployed at a campus for concentration and high-speed Internet Access, as shown next.

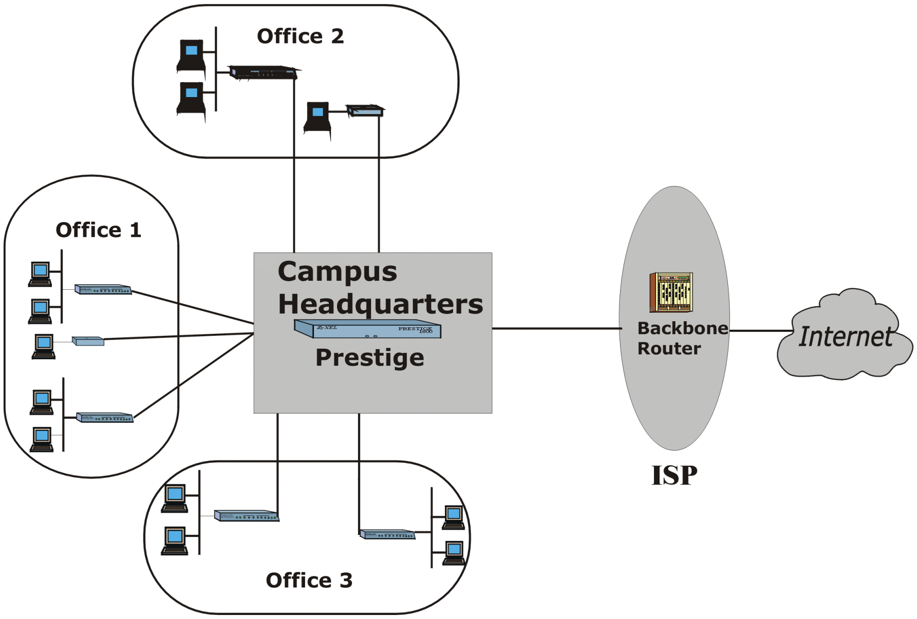


Figure 2-2 Campus Deployment

2.2.3 Deployed at ISPs and Other Service Providers

ISPs and other service providers can offer services to corporate and other customers using the P1600. For example, the P1600 can be connected to the ISP’s internal LAN and users can access the Internet using the ISP’s router as shown next.

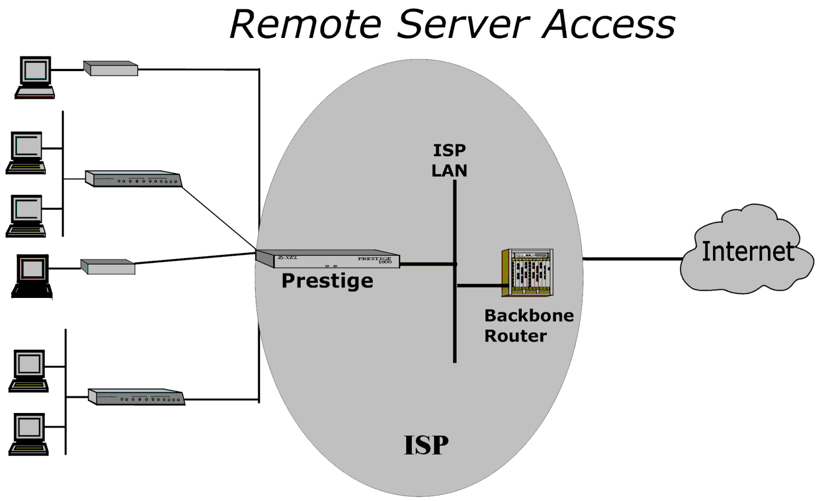


Figure 2-3 Deployed at an ISP

A few examples of possible configurations for these deployments are shown next.

2.2.4 Configuration Example One

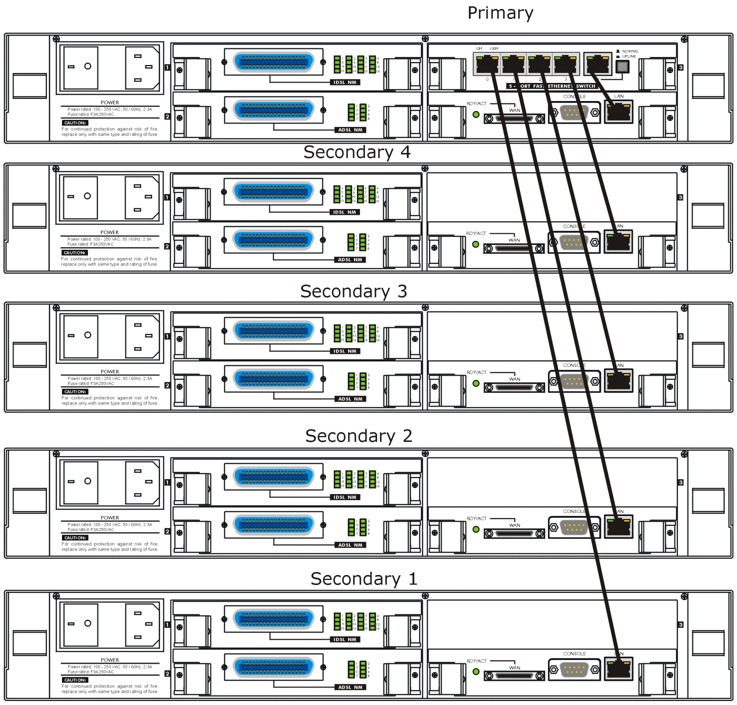


Figure 2-4 A Very High Capacity Concentrator

2.2.5 Configuration Example Two

You can also have any number of P1600 standalones chained to an external Ethernet hub as shown next.

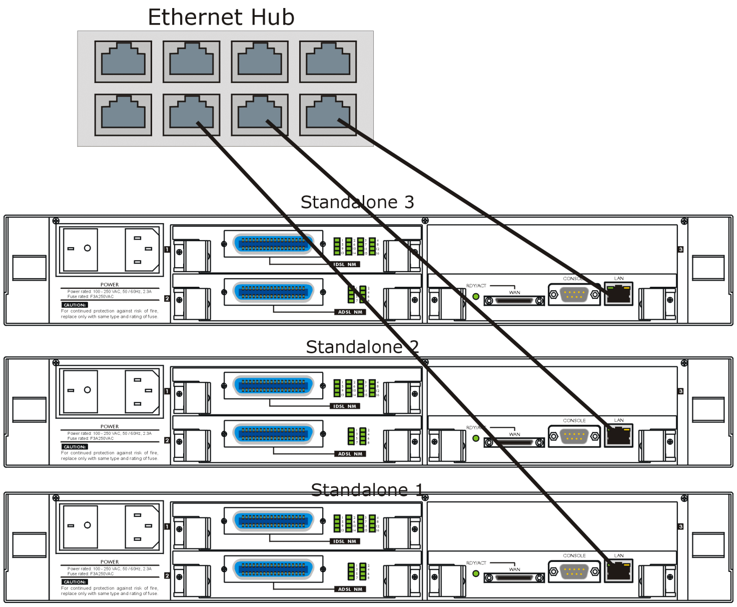


Figure 2-5 High Capacity Concentrator

2.2.6 Configuration Example Three

Depending on your requirement you can vary the number of Prestige 1600 secondaries as shown next.

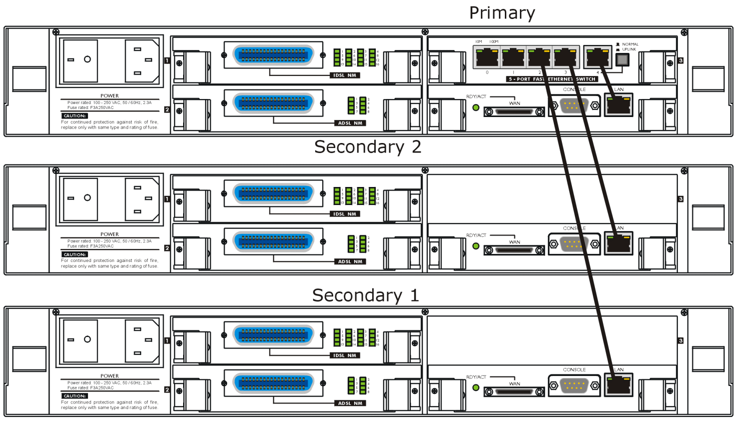


Figure 2-6 Medium Capacity Concentrator

2.2.7 Configuration Example Four

You can also use the P1600 standalone concentrator for Internet Access.

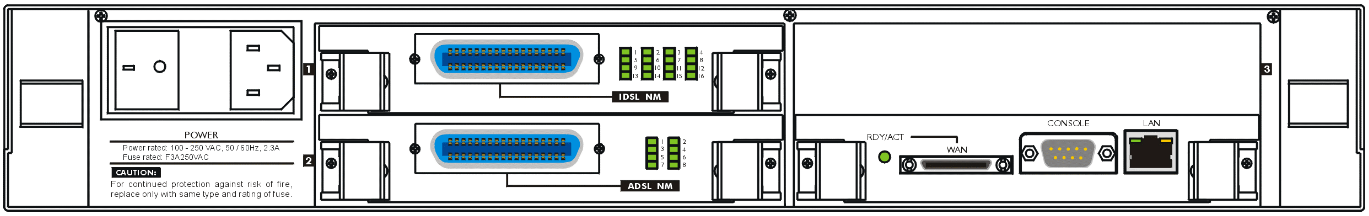

POWER
Power rated: 100 - 250 VAC, 50 / 60Hz, 2.3A
Fuse rated: F3A250VAC
CAUTION:
For continued protection against risk of fire, replace only with same type and rating of fuse.
1
2
3
IDSL NM
ADSL NM
RDY/ACT
WAN
CONSOLE
LAN

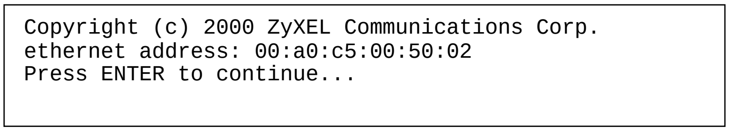
Figure 2-7 Low Capacity Concentrator

Chapter 3
Initial Setup

This chapter shows you how to perform initial setup using the SMT.

3.1 Initial Screen

When you power on your Prestige 1600, the router performs several internal tests and initializes the ports. After the initialization, the Prestige asks you to press [ENTER] to continue, as shown below:



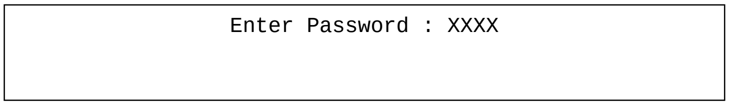
```
Copyright (c) 2000 ZyXEL Communications Corp.
ethernet address: 00:a0:c5:00:50:02
Press ENTER to continue...
```

Figure 3-1 Power-On Display

3.1.1 Password

After you press [ENTER], the Login screen appears prompting you to enter the password, as shown in the next figure.

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



```
Enter Password : XXXX
```

Figure 3-2 Login Screen

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

3.2 Navigating the SMT Interface

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

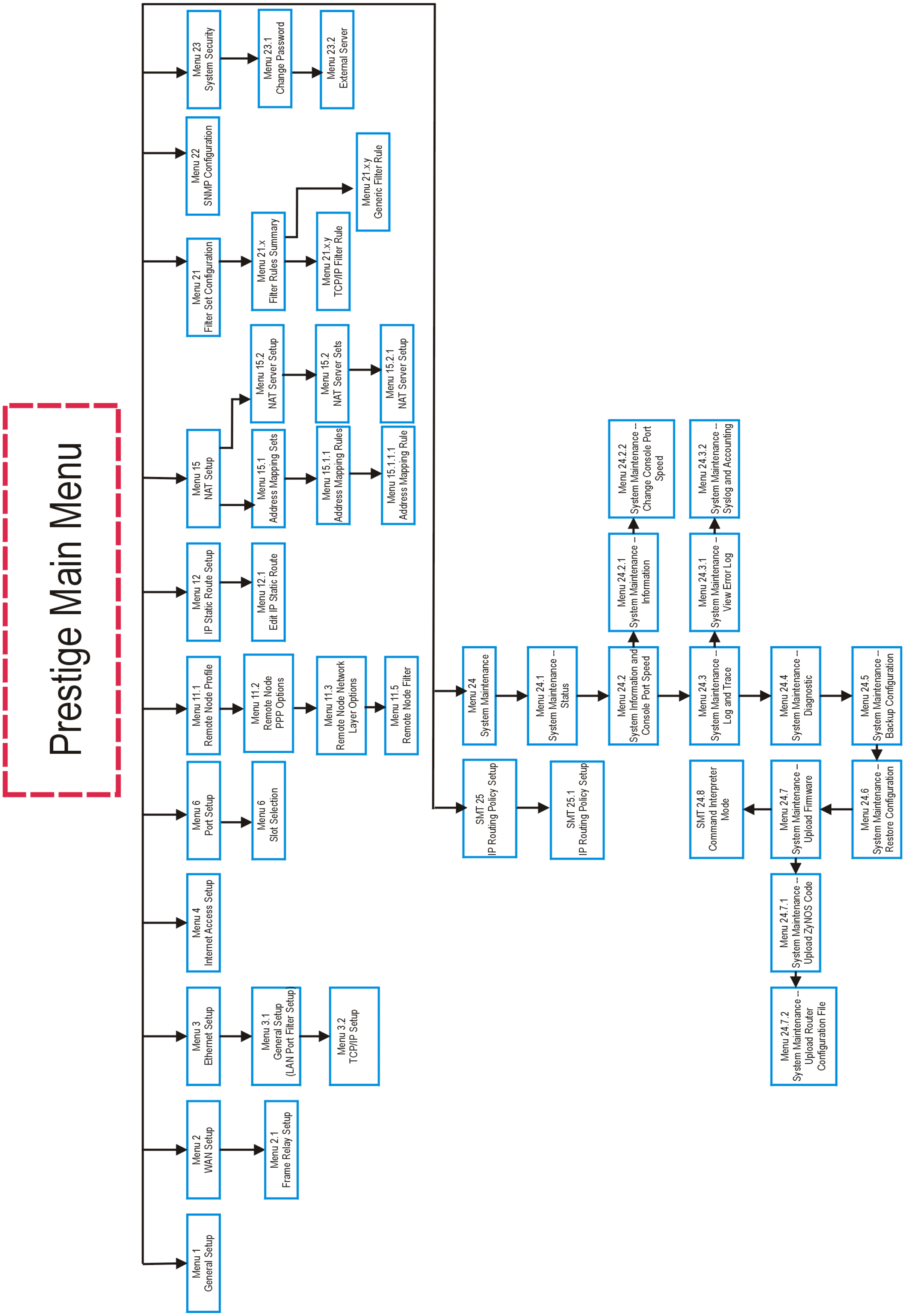
Several operations that you should be familiar with before you attempt to modify the configuration are listed in Table 3-1.

Table 3-1 Navigating the SMT

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

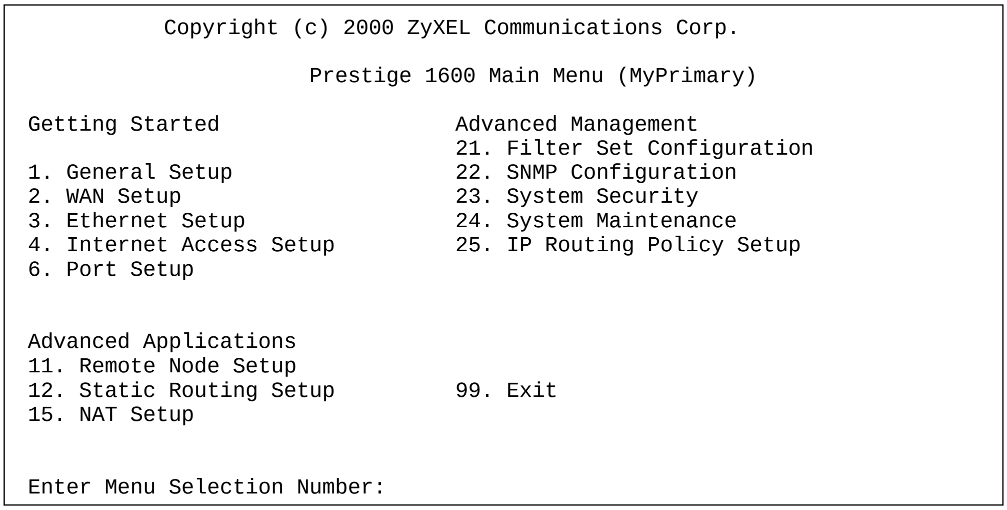
3.3 SMT Menus At A Glance

The following chart is an overall view of how the SMT menus are organized.


Prestige Main Menu
Menu 1 General Setup
Menu 2 WAN Setup
Menu 2.1 Frame Relay Setup
Menu 3 Ethernet Setup
Menu 3.1 General Setup (LAN Port Filter Setup)
Menu 3.2 TCP/IP Setup
Menu 4 Internet Access Setup
Menu 6 Port Setup
Menu 6 Slot Selection
Menu 11.1 Remote Node Profile
Menu 11.2 Remote Node PPP Options
Menu 11.3 Remote Node Network Layer Options
Menu 11.5 Remote Node Filter
Menu 12 IP Static Route Setup
Menu 12.1 Edit IP Static Route
Menu 15 NAT Setup
Menu 15.1 Address Mapping Sets
Menu 15.1.1 Address Mapping Rules
Menu 15.1.1.1 Address Mapping Rule
Menu 15.2 NAT Server Setup
Menu 15.2 NAT Server Sets
Menu 15.2.1 NAT Server Setup
Menu 21 Filter Set Configuration
Menu 21.x Filter Rules Summary
Menu 21.x.y TCP/IP Filter Rule
Menu 21.x.y Generic Filter Rule
Menu 22 SNMP Configuration
Menu 23 System Security
Menu 23.1 Change Password
Menu 23.2 External Server
SMT 25 IP Routing Policy Setup
SMT 25.1 IP Routing Policy Setup
Menu 24 System Maintenance
Menu 24.1 System Maintenance -- Status
Menu 24.2 System Information and Console Port Speed
Menu 24.2.1 System Maintenance -- Information
Menu 24.2.2 System Maintenance -- Change Console Port Speed
Menu 24.3 System Maintenance -- Log and Trace
Menu 24.3.1 System Maintenance -- View Error Log
Menu 24.3.2 System Maintenance -- Syslog and Accounting
Menu 24.4 System Maintenance -- Diagnostic
Menu 24.5 System Maintenance -- Backup Configuration
Menu 24.6 System Maintenance -- Restore Configuration
Menu 24.7 System Maintenance -- Upload Firmware
Menu 24.7.1 System Maintenance -- Upload ZyNOS Code
Menu 24.7.2 System Maintenance -- Upload Router Configuration File
SMT 24.8 Command Interpreter Mode

3.3.1 P1600 Main Menu - Primary

The SMT displays a general Main Menu first. Once you configure the system in **Menu 1 - General Setup** you can see the P1600 primary Main Menu, as shown next.



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

                       Prestige 1600 Main Menu (MyPrimary)

Getting Started                   Advanced Management
                                  21. Filter Set Configuration
1. General Setup                  22. SNMP Configuration
2. WAN Setup                      23. System Security
3. Ethernet Setup                 24. System Maintenance
4. Internet Access Setup          25. IP Routing Policy Setup
6. Port Setup


Advanced Applications
11. Remote Node Setup
12. Static Routing Setup          99. Exit
15. NAT Setup


Enter Menu Selection Number:
```

Figure 3-3 Primary Main Menu

The following table shows the Main Menu Summary,

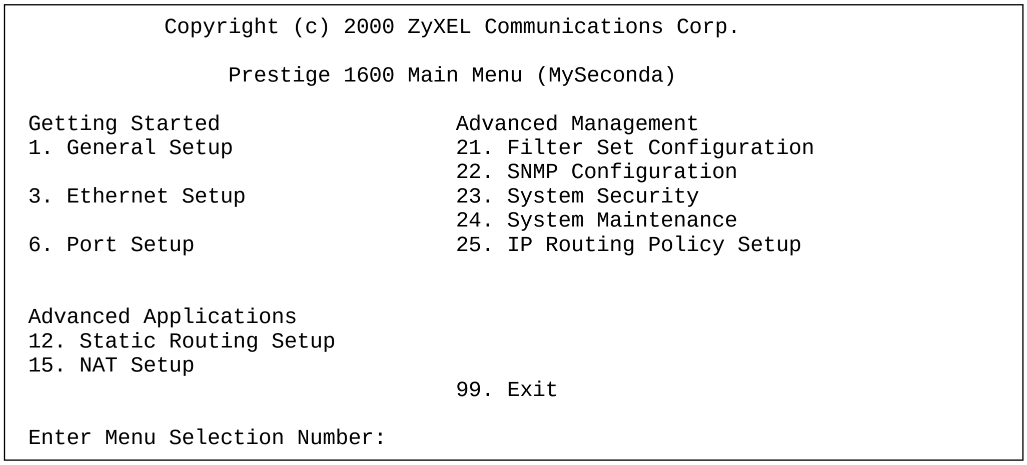
Table 3-2 Main Menu Summary

#	Menu Title	Description
1	General Setup	Use this menu to set up general information and enable routing or bridging of specific protocols. The name in brackets after Main Menu is the System Name you assign here.
2	WAN Setup	Use this menu to set up the WAN configuration.
3	Ethernet Setup	Use this menu to set up the Ethernet configuration.
4	Internet Access Setup	A quick and easy way to set up an Internet connection for the primary 1600.
6	Port Setup	Use this menu to configure DSL port parameters and to choose authentication options.
11	Remote Node Setup	Use this menu to set up the remote node for LAN-to-LAN connections, including an Internet connection for the primary and standalone models.
12	Static Routing Setup	Use this menu to set up static routes for different protocols. There are eight static routes for each protocol.
15	NAT Setup	Use this menu to configure NAT.
21	Filter Set Configuration	Set up filters to be applied in Menu 3 and Menu 11 to provide security, call control, etc.
22	SNMP Configuration	Use this menu to set up SNMP related parameters
23	System Security	Use this menu to set up security related parameters.
24	System Maintenance	Provides system status, diagnostics, firmware upload, etc.
25	IP Routing Policy Setup	Configure your routing policies here.

99	Exit	To exit the SMT and return to a blank screen.

3.3.2 Secondary and Standalone Main Menu

The SMT Main Menu for the secondary and standalone Prestige models is as shown next.



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

                 Prestige 1600 Main Menu (MySeconda)

Getting Started                  Advanced Management
1. General Setup                 21. Filter Set Configuration
                                 22. SNMP Configuration
3. Ethernet Setup                23. System Security
                                 24. System Maintenance
6. Port Setup                    25. IP Routing Policy Setup


Advanced Applications
12. Static Routing Setup
15. NAT Setup
                                 99. Exit

Enter Menu Selection Number:
```

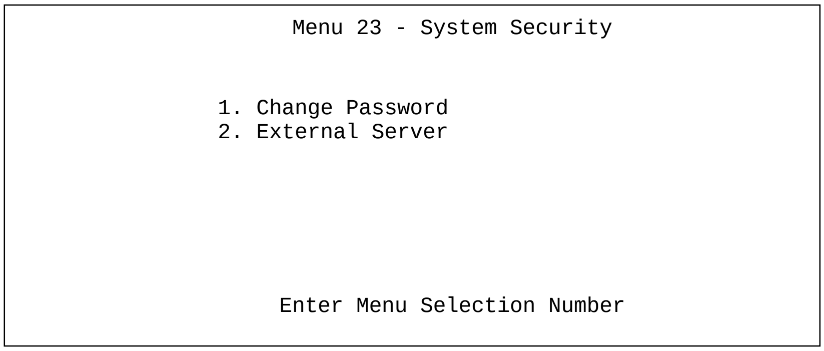
Figure 3-4 Secondary and Standalone Main Menu

Note: You will see the above screen when you set Configuration Type **in** Menu 1- General Setup **as** secondary **or** standalone**.**

3.4 Changing the System Password

The first thing you should do before anything else is to change the default system password by doing the following:

Step 1. Select option 23 from the Main Menu. This will open **Menu 23 - System Security** as shown:

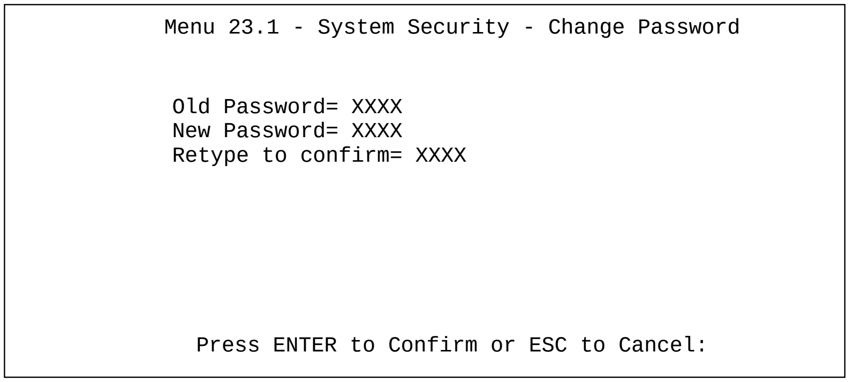


```
                      Menu 23 - System Security


                1. Change Password
                2. External Server







                     Enter Menu Selection Number
```

Figure 3-5 Menu 23 - System Security

Step 2. From the System Security Menu, select **Change Password** to bring up **Menu 23.1 - System Security - Change Password**.

Step 3. When submenu 23.1- System Security-Change Password appears, as shown below, enter the existing system password, i.e., `1234`, then press [ENTER].



```
                    Menu 23.1 - System Security - Change Password


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







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

Figure 3-6 Menu 23.1 - System Security - Change Password

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

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

3.5 Resetting the Prestige

If you forget your password or for some reason cannot access the SMT menu, you will need to reload the configuration file. Uploading the configuration file replace the current configuration file with the new configuration file. This means that you will lose all configurations that you had before and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control none. The password will be reset to 1234, also.

To obtain the default configuration file, download it from the FTP site, unzip it and save it in a folder. Turn off and then on the Prestige and begin a session. When you turn on the Prestige again you will see the initial screen. When you see the message “Press any key to enter Debug Mode within 3 seconds” press any key to enter debug mode.

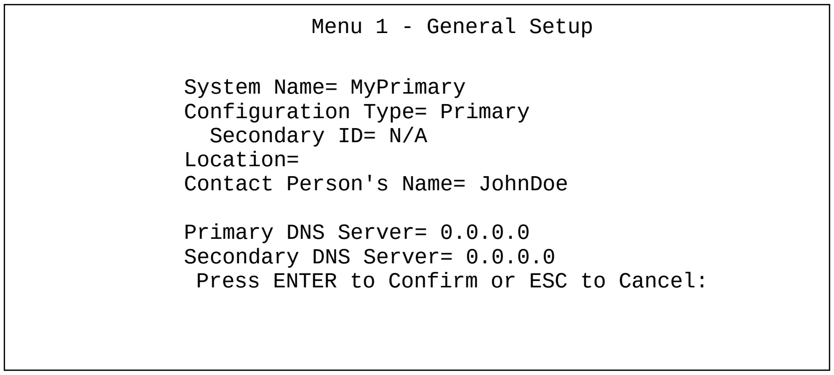
3.6 General Setup

Menu 1 - General Setup contains administrative and system-related information as well as DNS server information.

3.6.1 DNS Server Address

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

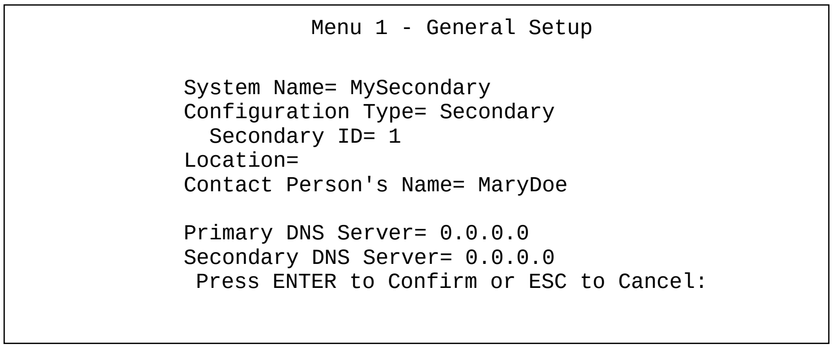
Select option 1 from the Main Menu by typing 1 at the menu selection number prompt. If your P1600 is configured as a primary you will see the following screen. Once you enter the system name it will be displayed in the Main Menu in brackets.



```
                    Menu 1 - General Setup

          System Name= MyPrimary
          Configuration Type= Primary
            Secondary ID= N/A
          Location=
          Contact Person's Name= JohnDoe

          Primary DNS Server= 0.0.0.0
          Secondary DNS Server= 0.0.0.0
           Press ENTER to Confirm or ESC to Cancel:
```

Figure 3-7 Menu 1 - General Setup (Primary)

When you configure the Prestige as a secondary or standalone model (**Configuration Type** field), you will see the following screen.



```
                    Menu 1 - General Setup

          System Name= MySecondary
          Configuration Type= Secondary
            Secondary ID= 1
          Location=
          Contact Person's Name= MaryDoe

          Primary DNS Server= 0.0.0.0
          Secondary DNS Server= 0.0.0.0
           Press ENTER to Confirm or ESC to Cancel:
```

Figure 3-8 Menu 1 - General Setup (Secondary/Standalone)

The **Menu 1 - General Setup** fields are explained in the next table.

Table 3-3 General Setup Fields

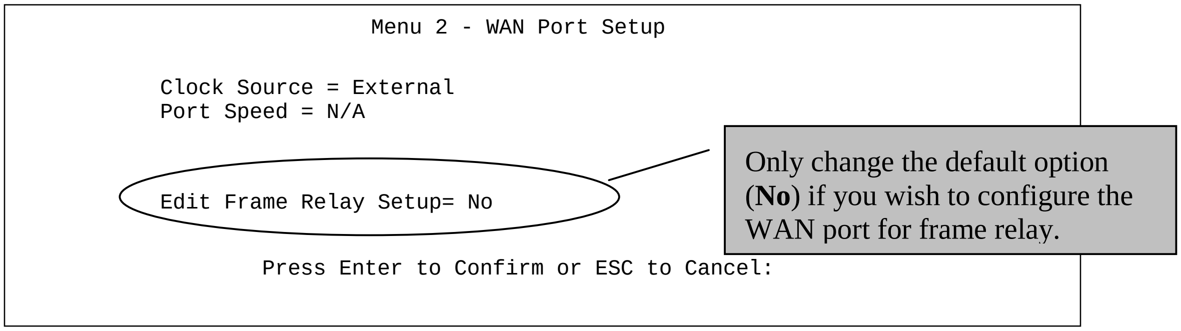
Field	Description	Example
System Name	Choose a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted. This name can be retrieved remotely via SNMP and will be displayed up to the first 9 characters at the prompt in the Command Mode.	MyPrimary
Note: Once you have configured the **System Name,** you can see it displayed (up to the first 9 characters) in the Main Menu within brackets next to "Prestige 1600 Main Menu".		
Configuration Type Secondary ID	You can configure the P1600 primary as only **Primary**. For P1600 Secondary choose **Secondary** or **Standalone**. State the ID of the P1600 secondary. You may have up to four secondaries with one primary.	**Primary** 1, 2, 3 or 4
Location (optional)	Enter the geographic location (up to 31 characters) of your Prestige 1600.	Hsinchu
Contact Person's Name (optional)	Enter the name (up to 30 characters) of the person in charge of this Prestige 1600.	JohnDoe
Primary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	

Field	Description	Example
Secondary DNS Server	Leave these entries at 0.0.0.0 if a WAN DHCP server provides them.	

Chapter 4
WAN Port Setup

This section describes setting up your WAN port including Frame Relay.

Select option 2 from the Main Menu by typing 2 at the menu selection number prompt. You will see a screen as shown next.



```
                            Menu 2 - WAN Port Setup

            Clock Source = External
            Port Speed = N/A


            Edit Frame Relay Setup= No


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

Only change the default option (**No**) if you wish to configure the WAN port for frame relay.

Figure 4-1 Menu 2 - WAN Port Setup

Table 4-1 WAN Setup Menu Fields

Field	Description	Example
Clock Source	The device connected to the WAN port controls timing. The P1600 currently *only* supports an external clock source.	**External**
Port Speed	Set by External Device	**N/A**
Edit Frame Relay Setup	To configure the WAN port for frame relay move the cursor to the **Edit Frame Relay Setup=** field, press the [SPACEBAR] once to display **Yes** and then press [ENTER]. This takes you to **Menu 2.1.2 - Frame Relay Setup** shown ahead.	

4.1 Configuring The WAN Port For PPP over HDLC

The following diagram depicts the configuration scenario for running PPP over HDLC (High-level Data Link Control).

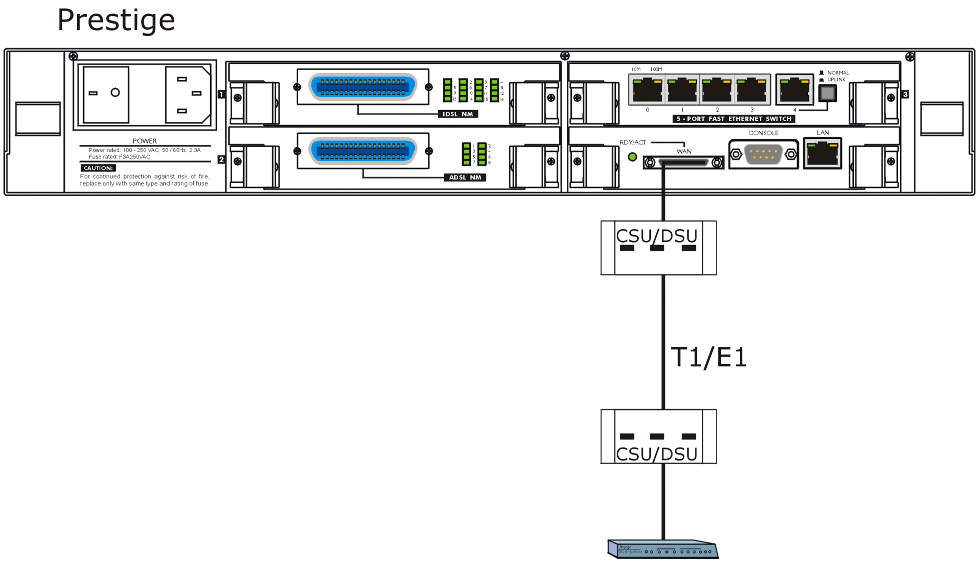


Figure 4-2 Configuring The WAN Port for PPP over HDLC

To run PPP over HDLC directly without frame relay, the **Line Type** field in **Menu 2.1.2 - Frame Relay Setup** must be set to **None**. To make sure frame relay is disabled, go to menu 2 and then to **Menu 2.1.2 – Frame Relay Setup**. If the **Line Type** field is not **None**, press [SPACE BAR] to change it before saving the configuration.

4.2 Configuring The WAN Port For Frame Relay

To configure the WAN port for frame relay go to **Menu 2 - WAN Port Setup** and change the default option (**No**) in the **Edit Frame Relay Setup** field to **Yes**. Frame relay is a form of packet-switching technology that routes frames of information from source to destination over a switched network owned by a carrier. Frames are “relayed” through switches in the network.

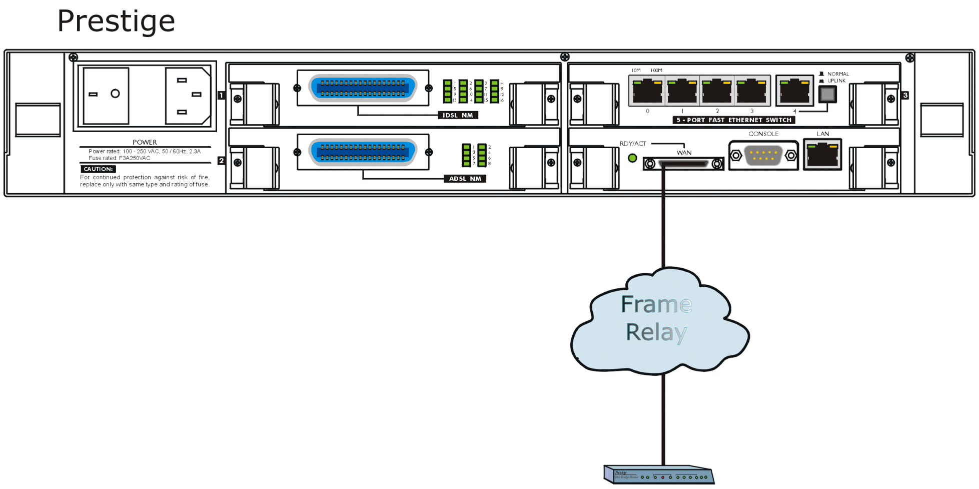


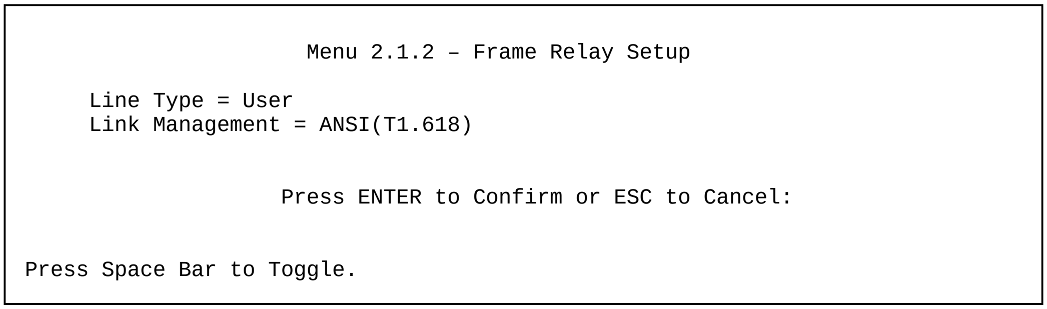
Figure 4-3 Configuring The WAN Port For Frame Relay

4.2.1 Standards

The two main groups that create recommendations and standards in the telecommunications field are ITU - T (International Telecommunication Union - Telecommunications Standardization Sector) and ANSI (American National Standards Institute). Standards vary slightly for both organizations, so please select the correct standard in the **Link Management** field. Your Network Service Provider (NSP) should provide you with this information.

4.2.2 How To Configure The WAN Port For Frame Relay

Go to menu 2, then move the cursor to the **Edit Frame Relay Setup=** field, press the [SPACEBAR] once to display **Yes** and then press [ENTER]. This takes you to **Menu 2.1.2 - Frame Relay Setup** shown next.



```
                         Menu 2.1.2 – Frame Relay Setup

     Line Type = User
     Link Management = ANSI(T1.618)


                       Press ENTER to Confirm or ESC to Cancel:


Press Space Bar to Toggle.
```

Figure 4-4 Menu 2.1.2 - Frame Relay Setup

Table 4-2 Menu 2.1.2 - Frame Relay Setup

Field	Description	Options
Link Type	Choose **User** if the Prestige is on the user side of the UNI (User Network Interface: defines the connection between user equipment and the Frame Relay network), i.e. if your Prestige is connected to a service provider. Choose **None** to disable Frame Relay.	**User (default)** **None**

Link Management	Press the [SPACEBAR] and then [ENTER] to select which standard is compatible with your Prestige. Both the Prestige and the peer must use the same standard. The standard defines functions that are responsible for monitoring the up/down status and error performance of an individual link. If failure occurs, recovery actions are initiated for the restoration of the failed link.	**ITU-T(Q.933)**
		ANSI(T1.618)

4.3 How To Configure Frame Relay for Internet Access

4.3.1 Encapsulation

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

RFC 1973 (PPP in Frame Relay)

RFC 1973 describes the use of Frame Relay for transporting PPP encapsulated packets. Please refer to RFC 1973 for more information.

RFC 1490

RFC 1490 describes Multiprotocol Interconnect over Frame Relay encapsulation which is an encapsulation method for carrying network interconnect traffic (both bridging and routing) over a frame relay network. It also describes a simple fragmentation procedure for carrying large frames over a frame relay network with a smaller MTU (Maximum Transmission Unit).

4.3.2 DLCI

The carrier gives you a DLCI (Data Link Connection Identifier) for each frame relay connection to a destination. Identifiers can range from 1 to 991 with restrictions as shown in the following table. The default DLCI for the first connection is 16.

Table 4-3 Data Link Connection Identifiers

DLCI	Usage
0	Channel Signaling
1-15	Reserved
16 - 991	Frame Relay

4.3.3 CIR (Committed Information Rate)

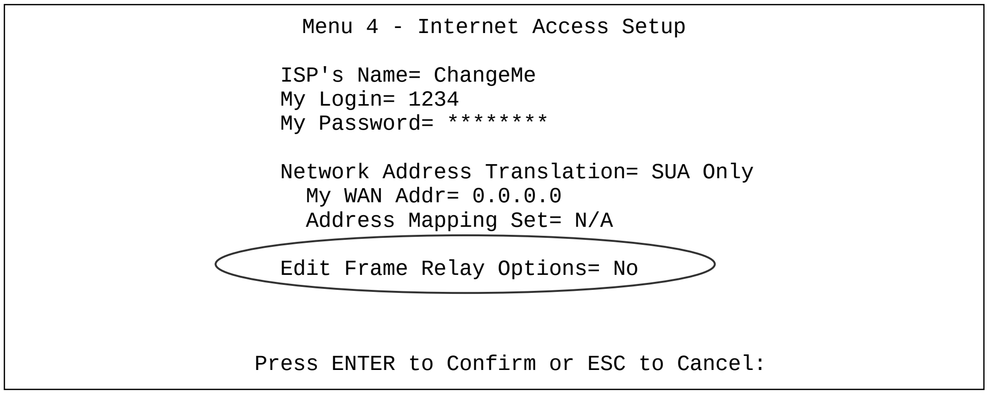
The carrier programs virtual circuits into the network between your sites and charges you for a specific level of service called the committed information rate (CIR). The CIR is basically a guarantee that the carrier will always have that bandwidth available. The CIR limit for the Prestige is 8Mbps. The sum of CIRs from all channels in a line cannot exceed 8Mbps due to the processing limit of the P1600 CPU.

4.3.4 EIR (Excess Information Rate)

This is the burst capability of the connection, i.e., the maximum allowable data transfer rate. EIR must be greater than or equal to the CIR.

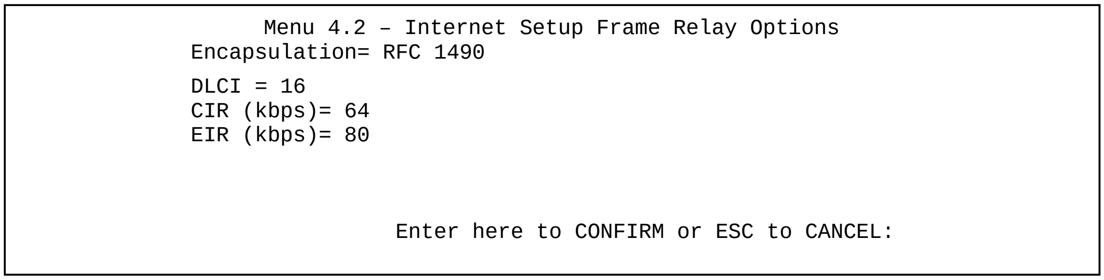
4.3.5 How To Configure Frame Relay for Internet Access

Go to **Menu 4 - Internet Access Setup**, move the cursor to the **Edit Frame Relay Options=** field, press the [SPACEBAR] once to display **Yes** and then press [ENTER]. This takes you to **Menu 4.2 - Internet Setup Frame Relay Options** shown next.



```
                     Menu 4 - Internet Access Setup

                   ISP's Name= ChangeMe
                   My Login= 1234
                   My Password= ********

                   Network Address Translation= SUA Only
                     My WAN Addr= 0.0.0.0
                     Address Mapping Set= N/A

                   Edit Frame Relay Options= No



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

Figure 4-5 Menu 4 - Internet Access Setup



```
           Menu 4.2 – Internet Setup Frame Relay Options
      Encapsulation= RFC 1490

      DLCI = 16
      CIR (kbps)= 64
      EIR (kbps)= 80



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

Figure 4-6 Menu 4.2 - Internet Setup Frame Relay Options

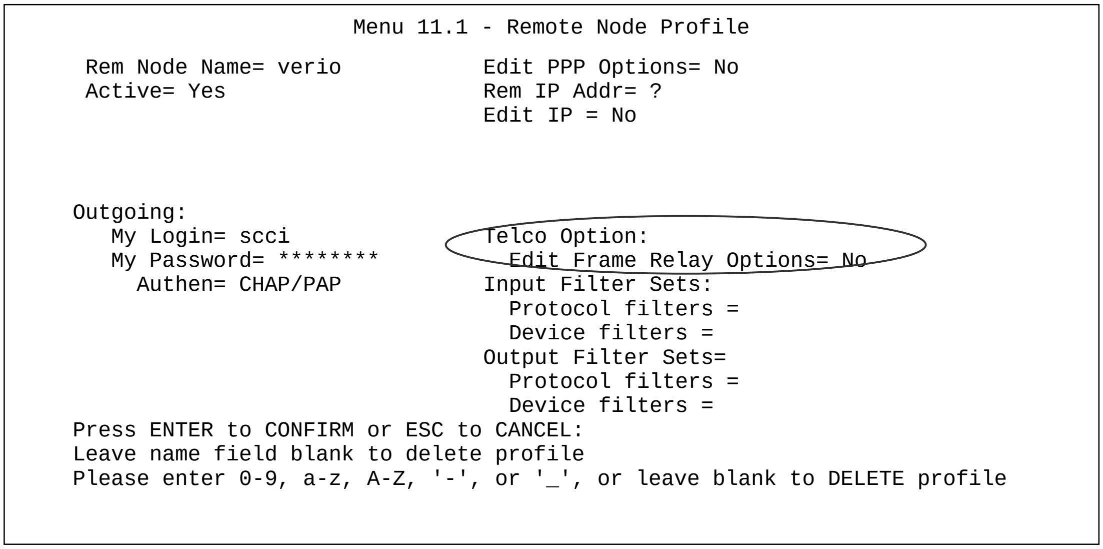
Table 4-4 Menu 4.2 - Internet Setup Frame Relay Options

Field	Description	Options/Examples
Encapsulation	Be sure to use the encapsulation method required by your ISP. The Prestige supports the following methods. See *section 4.3.1* for more information.	**RFC 1973 (PPP)** **RFC 1490**
DLCI	Enter the DLCI number required by your ISP. This is a path number of a portion of the PVC (the DLCI changes for each hop through the network), not the address of the destination. The default DLCI for the Prestige is 16 for the first PVC. See *section 4.3.2* for more information.	**16**
CIR (Kbps)	Enter the CIR as negotiated with your ISP. See *section 4.3.3* for more information.	**64**
EIR (Kbps)	Enter the EIR as negotiated with your ISP. See *section 4.3.4* for more information.	**80**

4.4 How To Configure Frame Relay For A Remote Node

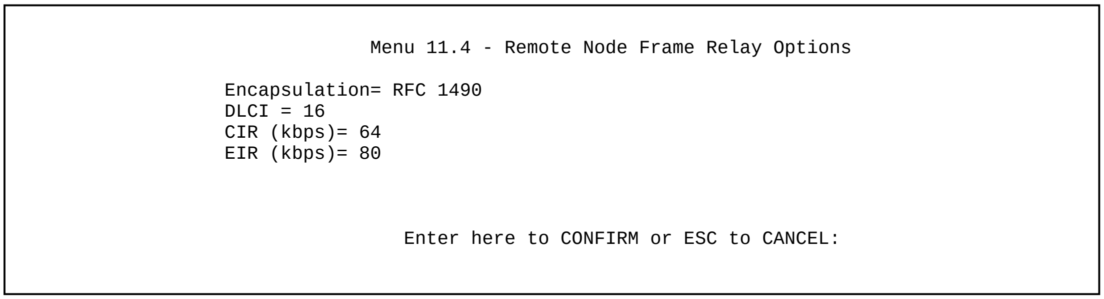
Configuring Frame Relay for a remote node is similar to configuring Frame Relay for Internet Access.

Go to **Menu 11.1 - Remote Node Profile**, move the cursor to the move the cursor to the **Edit Frame Relay Options=** field, press the [SPACEBAR] once to display **Yes** and then press [ENTER]. This takes you to **Menu 11.5 - Remote Node Frame Relay Options** shown next.



```
                      Menu 11.1 - Remote Node Profile

 Rem Node Name= verio           Edit PPP Options= No
 Active= Yes                    Rem IP Addr= ?
                                Edit IP = No



Outgoing:
   My Login= scci               Telco Option:
   My Password= ********          Edit Frame Relay Options= No
     Authen= CHAP/PAP           Input Filter Sets:
                                  Protocol filters =
                                  Device filters =
                                Output Filter Sets=
                                  Protocol filters =
                                  Device filters =
Press ENTER to CONFIRM or ESC to CANCEL:
Leave name field blank to delete profile
Please enter 0-9, a-z, A-Z, '-', or '_', or leave blank to DELETE profile
```

Figure 4-7 Menu 11.1 - Remote Node Profile



```
             Menu 11.4 - Remote Node Frame Relay Options

Encapsulation= RFC 1490
DLCI = 16
CIR (kbps)= 64
EIR (kbps)= 80



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

Figure 4-8 Menu 11.4 - Remote Node Frame Relay Options

The fields in this table are the same as described in *Table 4-4 above*.

Chapter 5
Internet Access

This chapter shows you how to configure the Prestige 1600 primary and Prestige 1600 standalone for Internet access.

5.1 Introduction

Menu 4 - Internet Access Setup of the SMT allows you to configure the Internet access parameters in a single screen. For Internet access using the Prestige 1600 standalone you need to only set up a default route using **Menu 12 - Static Default Route**. While configuring your Prestige for Internet access you have to be careful when setting the IP addresses to avoid IP conflict. The following section shows the various IP networks in the P1600.

5.1.1 IP Address assignment

Table 5-1 Default DSL IP Address Assignment

Configuration Type (Menu 1)	P1600 IP address	Port numbers		IP address range assigned to DSL Clients (Menu 6.1)
Primary	192.168.1.1	Slot 1	IDSL:16 ports	192.168.255.1 ~ 192.168.255.16
			ADSL/SDSL: 8 ports	192.268.255.1 ~ 192.168.255.8
		Slot 2	IDSL:16 ports	192.168.255.17 ~ 192.168.255.32
			ADSL/SDSL: 8 ports	192.168.255.17 ~ 192.168.255.24
		Slot 3	IDSL	Not Available
			ADSL/SDSL: 8 ports	192.168.255.33 ~ 192.168.255.40
Secondary 1	192.168.1.2	Slot 1	IDSL:16 ports	192.168.254.1 ~ 192.168.254.16
			ADSL/SDSL: 8 ports	192.268.254.1 ~ 192.168.254.8
		Slot 2	IDSL:16 ports	192.168.254.17 ~ 192.168.254.32
			ADSL/SDSL: 8 ports	192.168.254.17 ~ 192.168.254.24
		Slot 3	IDSL	Not Available
			ADSL/SDSL: 8 ports	192.168.254.33 ~ 192.168.254.40
Secondary 2	192.168.1.3	Slot 1	IDSL:16 ports	192.168.253.1 ~ 192.168.253.16
			ADSL/SDSL: 8 ports	192.268.253.1 ~ 192.168.253.8

Configuration Type (Menu 1)	P1600 IP address	Port numbers		IP address range assigned to DSL Clients (Menu 6.1)
		Slot 2	IDSL:16 ports	192.168.253.17 ~ 192.168.253.32
			ADSL/SDSL: 8 ports	192.168.253.17 ~ 192.168.253.24
		Slot 3	IDSL	Not Available
			ADSL/SDSL: 8 ports	192.168.253.33 ~ 192.168.253.40
Secondary 3	192.168.1.4	Slot 1	IDSL:16 ports	192.168.252.1 ~ 192.168.252.16
			ADSL/SDSL: 8 ports	192.268.252.1 ~ 192.168.252.8
		Slot 2	IDSL:16 ports	192.168.252.17 ~ 192.168.252.32
			ADSL/SDSL: 8 ports	192.168.252.17 ~ 192.168.252.24
		Slot 3	IDSL	Not Available
			ADSL/SDSL: 8 ports	192.168.252.33 ~ 192.168.252.40
Secondary 4	192.168.1.5	Slot 1	IDSL:16 ports	192.168.251.1 ~ 192.168.251.16
			ADSL/SDSL: 8 ports	192.268.251.1 ~ 192.168.251.8
		Slot 2	IDSL:16 ports	192.168.251.17 ~ 192.168.251.32
			ADSL/SDSL: 8 ports	192.168.251.17 ~ 192.168.251.24
		Slot 3	IDSL	Not Available
			ADSL/SDSL: 8 ports	192.168.251.33 ~ 192.168.251.40
Standalone	192.168.1.1	Slot 1	IDSL:16 ports	192.168.255.1 ~ 192.168.255.16
			ADSL/SDSL: 8 ports	192.268.255.1 ~ 192.168.255.8
		Slot 2	IDSL:16 ports	192.168.255.17 ~ 192.168.255.32
			ADSL/SDSL: 8 ports	192.168.255.17 ~ 192.168.255.24
		Slot 3	IDSL	Not Available
			ADSL/SDSL: 8 ports	192.168.255.33 ~ 192.168.255.40

All DSL users who do not have public IP address can get one private IP address from the Prestige IP address pool according to the configuration type setup in Menu 1. The default IP addresses for the DSL clients are arranged sequentially as shown in the table above. A port is identified as e.g., "Primary, Slot 3, port 6" or "Secondary 1, Slot 2, port 4", etc.

5.1.2 Standalone IP Pool

When the Prestige **Configuration Type** (Menu 1) is set up as **Standalone** and Internet access is configured through the Ethernet port, you have to manually enter Ethernet TCP/IP information using **Menu 3.** There are no dynamic default IP address assignments in this scenario. The default route has to be configured in Menu 12.

5.2 TCP/IP Parameters

If you wish to know more about TCP/IP, please read on. Or you can skip to *4.3 TCP/IP Ethernet Setup* for the actual configuration.

5.2.1 IP Address and Subnet Mask

Machines on a LAN share one common network number; once you have decided on the network number, pick an IP address that is easy to remember, e.g., 192.168.1.1, for your Prestige 1600.

The subnet mask specifies the network number portion of an IP address. Your Prestige 1600 will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Prestige 1600 unless you are instructed to do otherwise.

5.2.2 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to:

1. **Both -** the Prestige 1600 will broadcast its routing table periodically and incorporate the RIP information that it receives.
2. **In Only -** the Prestige will not send any RIP packets but will accept all RIP packets received.
3. **Out Only -** the Prestige will send out RIP packets but will not accept any RIP packets received.
4. **None -** the Prestige will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the Prestige 1600 sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have a unusual network topology.

Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting.

5.2.3 IP Multicast

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

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

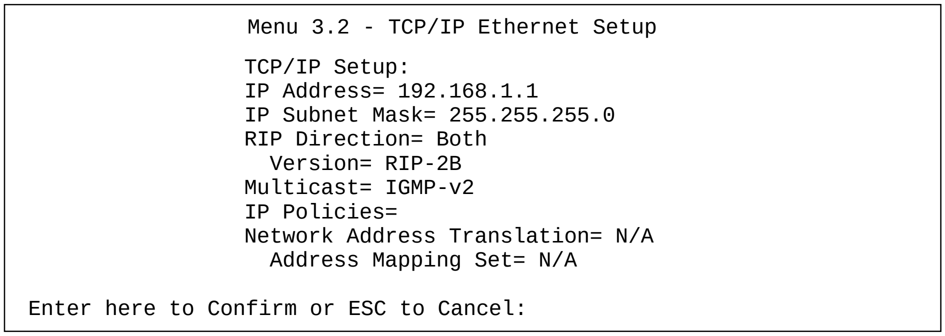
The Prestige supports both IGMP version 1 (**IGMP-v1**) and **IGMP-v2**. At start up, the Prestige queries all directly connected networks to gather group membership. After that, the Prestige periodically updates this information by sending a membership query to 224.0.0.1. IP Multicasting can be enabled/disabled on the Prestige LAN and/or WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN). Select **None** to disable IP Multicasting on these interfaces.

5.3 IP Policies

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

5.4 TCP/IP Ethernet Setup

To edit **Menu 3.2**, select **Menu 3 Ethernet Setup** in the Main Menu and then the appropriate LAN. Then select the submenu option 2, and press [ENTER]. The screen now displays **Menu 3.2 - TCP/IP Ethernet Setup** as shown next.



```
                  Menu 3.2 - TCP/IP Ethernet Setup

                  TCP/IP Setup:
                  IP Address= 192.168.1.1
                  IP Subnet Mask= 255.255.255.0
                  RIP Direction= Both
                    Version= RIP-2B
                  Multicast= IGMP-v2
                  IP Policies=
                  Network Address Translation= N/A
                    Address Mapping Set= N/A

 Enter here to Confirm or ESC to Cancel:
```

Figure 5-1 Menu 3.2 - TCP/IP Ethernet Setup

Follow *Table 5-2* to configure TCP/IP parameters for the Ethernet port.

Table 5-2 TCP/IP Ethernet Setup Menu Fields

Field	Description	Example
IP Address	Enter the IP address of your Prestige 1600 in dotted decimal notation.	192.168.1.1
IP Subnet Mask	Your Prestige 1600 automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the value computed by the Prestige 1600.	255.255.255.0
RIP Direction	Press [SPACE BAR] to select the RIP direction among **Both/In Only/Out Only/None**	**Both** (default)
Version	Press [SPACE BAR] to select the RIP version among **RIP-1/RIP-2B/RIP-2M.**	**RIP-1** (default)
Multicast	Turn on/off IGMP support and select the version from **IGMP-v2/IGMP-v1/None.**	**IGMP-v2**

Field	Description	Example
IP Policies	You can apply up to four IP Policy sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11.	
Network Address Translation Address Mapping Set=	Please see the NAT chapter for a more detailed discussion on the Network Address Translation feature. The choices are **Full Feature, None** and **SUA Only.**	**Full Feature**
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. **Note:** When NAT is enabled you can connect the LAN port to any broadband device such as a cable modem or DSL device. You can also use the LAN port to connect to the ISP's internal LAN and access the Internet using the ISP's router.		

5.5 Collecting Internet Account Information

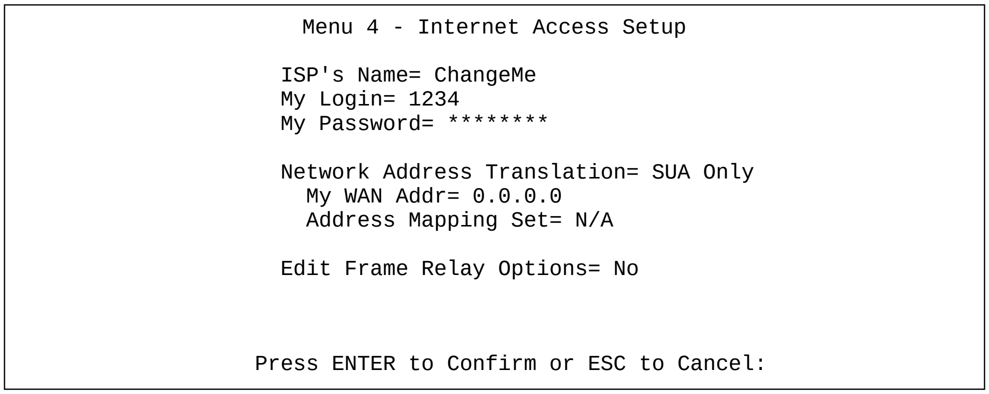
Before you configure your Prestige 1600 for Internet access, you need to collect your Internet account information from your ISP. Use *Table 5-3* to record your Internet Account Information.

Table 5-3 Internet Account Information

Internet Account Information	Write your account information here
IP Address of the ISP's Gateway	—
Login Name	—
Password	—

5.6 Internet Access using the Prestige 1600 Primary

Menu 4 allows you to enter the Internet access parameters in one screen. Menu 4 is actually a simplified setup for one of the remote nodes that you can access through menu 11. From the Main Menu, enter option **4** to go to **Menu 4 - Internet Access Setup**, as displayed in the next figure.



```
                       Menu 4 - Internet Access Setup

                     ISP's Name= ChangeMe
                     My Login= 1234
                     My Password= ********

                     Network Address Translation= SUA Only
                       My WAN Addr= 0.0.0.0
                       Address Mapping Set= N/A

                     Edit Frame Relay Options= No



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

Figure 5-2 Menu 4 - Internet Access Setup

Table 5-4 contains instructions on how to configure your Prestige 1600 for Internet access.

Table 5-4 Internet Access Setup Menu Fields

Field	**Description**	**Observation**
ISP's Name	Enter the name of your Internet Service Provider. (This information is for identification purposes only.)	myISP
My Login Name	Enter the login name assigned to you by your ISP.	(required)
My Password	Enter the password associated with the login name above. Note that this login name/password pair is only for your Prestige 1600 to connect to the ISP's gateway. For TCP/IP applications, e.g., FTP, you will need a separate login name and password for each server.	(required)
Network Address Translation	See the *NAT Chapter* for more details on this field and **Address Mapping Set** below.	
My WAN Addr	Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your Prestige 1600. Note that this is the address assigned to your local Prestige 1600, not the remote router.	
Address Mapping Set	See the *NAT Chapter*	
Edit Frame Relay Options	Please see the WAN Port Setup chapter for a full discussion of this feature.	
Press [ENTER] at the message “Press ENTER to Confirm...” to confirm your configuration, or press [ESC] at any time to cancel.		

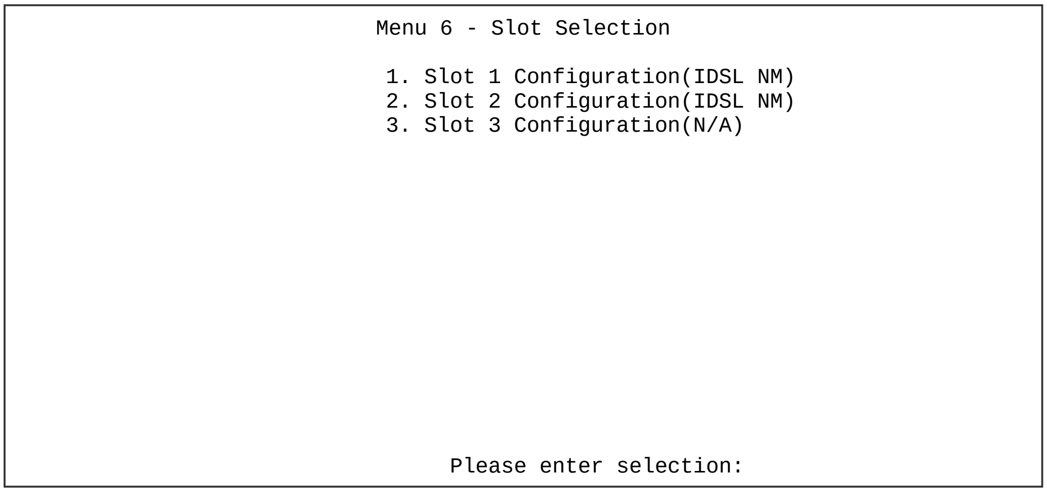
Chapter 6
DSL Port Setup

This chapter explains how to edit DSL Port information.

Use **Menu 6** to configure the DSL ports. Select 6 from the Main Menu to enter **Menu 6 - Slot Selection**.

The Prestige automatically detects which network module is inserted in each slot. The following menu appears when you have 2 ISDL network modules inserted in slots 1 and 2.

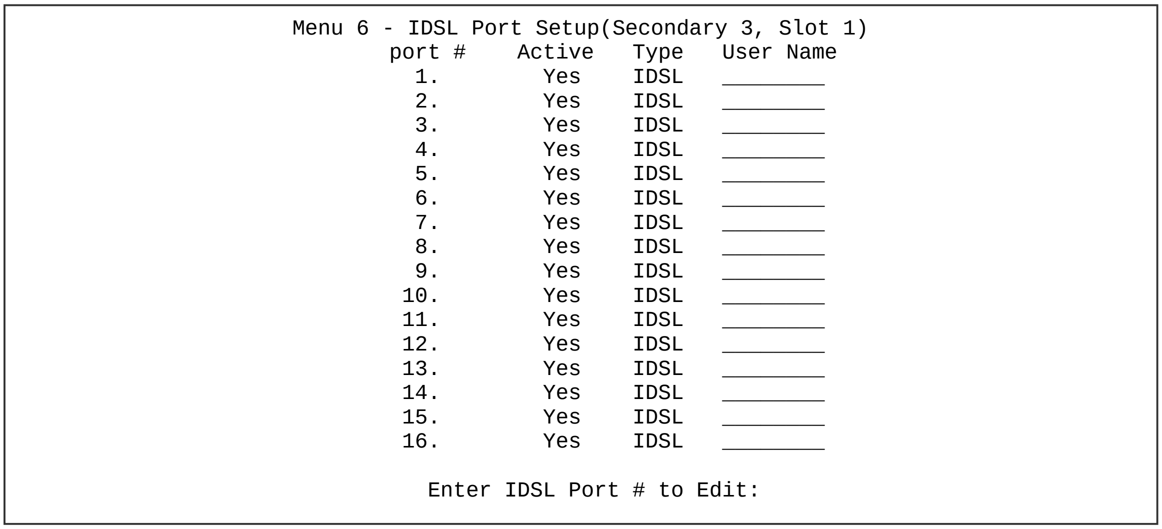
Note that ISDL network modules (32 ports per module) may only be inserted in slots 1 and 2 but not slot 3. ADSL or SDSL network modules (24 ports per module) may be inserted in either slots 1, 2 or 3. Combinations of network modules are also allowed.



```
                              Menu 6 - Slot Selection

                               1. Slot 1 Configuration(IDSL NM)
                               2. Slot 2 Configuration(IDSL NM)
                               3. Slot 3 Configuration(N/A)









                                    Please enter selection:
```

Figure 6-1 Menu 14 - IDSL Port setup

Choose a slot to configure by entering its index number. The following screen displays an IDSL module in slot 1 of a Secondary 3 device.



```
                    Menu 6 - IDSL Port Setup(Secondary 3, Slot 1)
                           port #    Active   Type   User Name
                             1.        Yes    IDSL   ________
                             2.        Yes    IDSL   ________
                             3.        Yes    IDSL   ________
                             4.        Yes    IDSL   ________
                             5.        Yes    IDSL   ________
                             6.        Yes    IDSL   ________
                             7.        Yes    IDSL   ________
                             8.        Yes    IDSL   ________
                             9.        Yes    IDSL   ________
                            10.        Yes    IDSL   ________
                            11.        Yes    IDSL   ________
                            12.        Yes    IDSL   ________
                            13.        Yes    IDSL   ________
                            14.        Yes    IDSL   ________
                            15.        Yes    IDSL   ________
                            16.        Yes    IDSL   ________

                              Enter IDSL Port # to Edit:
```

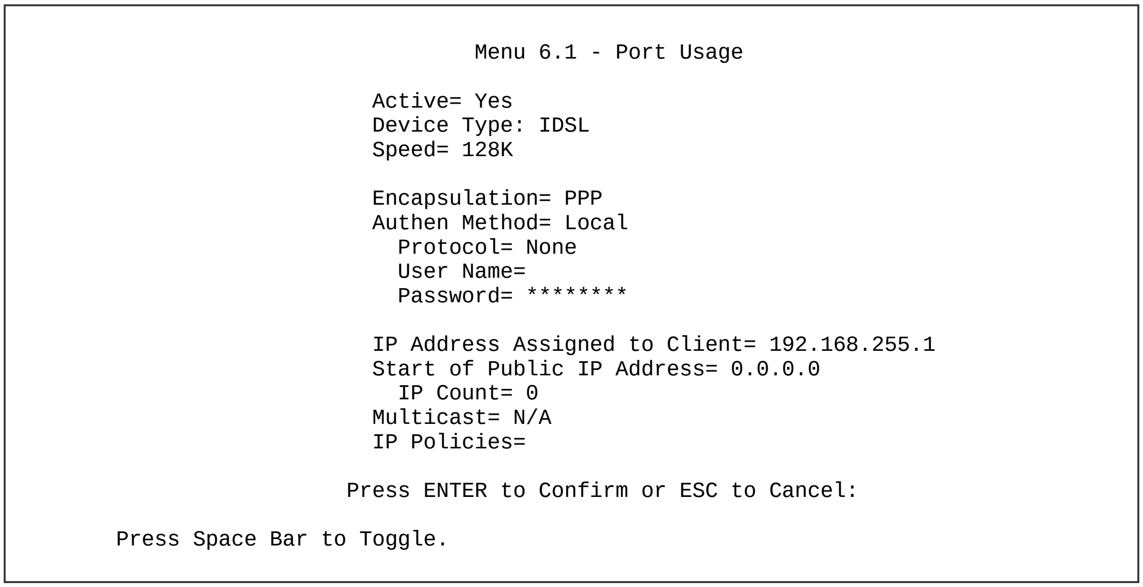
Figure 6-2 DSL Port Setup

Table 6-1 DSL Port Setup Fields

Field	Description	Option
port #	Refers to the DSL port number. The port number range changes according to the configuration type and network module type.	
Active	Indicates whether the DSL port is active or not. You can configure this in Menu 6.1 Port Usage.	**Yes/No**
Type	Displays the network module type in this slot.	**IDSL** **ADSL** **SDSL**
User Name	Refers to the name of the user. You can configure this in Menu 6.1 Port Usage. Your Prestige displays up to 8 characters in this field and if you have entered a user name with more than 8 characters a '+' is appended to the eighth character.	

6.1 Port Usage

Enter a port number to bring up the following menu (for an IDSL module installed).



```
                                Menu 6.1 - Port Usage

                        Active= Yes
                        Device Type: IDSL
                        Speed= 128K

                        Encapsulation= PPP
                        Authen Method= Local
                          Protocol= None
                          User Name=
                          Password= ********

                        IP Address Assigned to Client= 192.168.255.1
                        Start of Public IP Address= 0.0.0.0
                          IP Count= 0
                        Multicast= N/A
                        IP Policies=

                      Press ENTER to Confirm or ESC to Cancel:

    Press Space Bar to Toggle.
```

Figure 6-3 Menu 6.1 - Port Usage

The following table describes fields in this menu.

Table 6-2 Port Usage Menu Fields

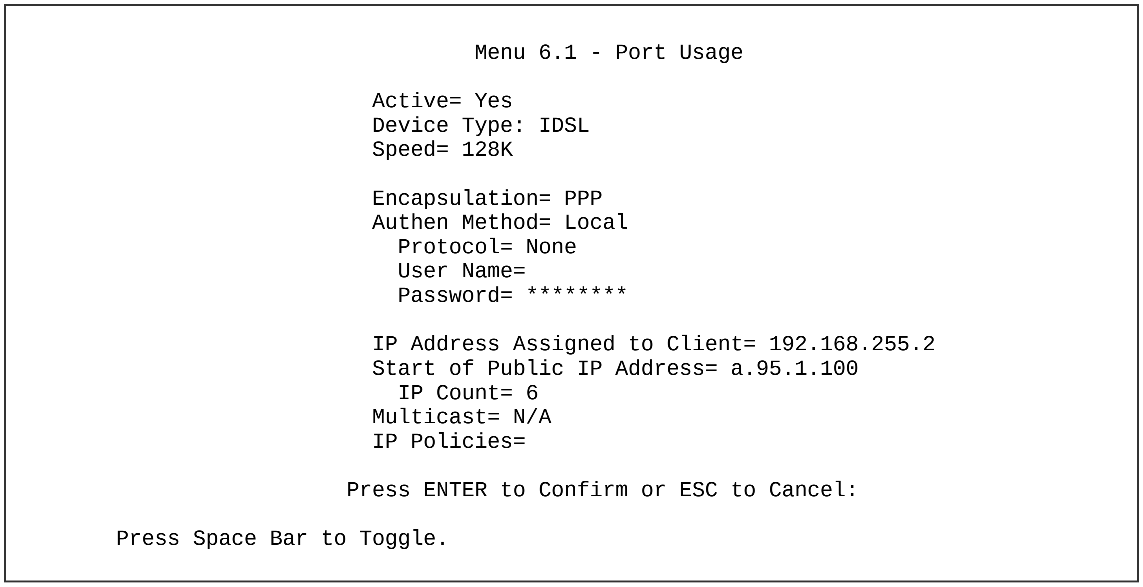
Field	Description	Option			
Active	You can disable this port by setting the field to **No**. Press [SPACE BAR] to toggle between **Yes** and **No**. This field will be <N/A> if no network module is installed.	**Yes/No**			
Device Type	The Prestige automatically detects the types of network module installed in the slot.				
Speed	Press [SPACE BAR] to toggle between speeds. Step-through SDSL speeds are in 64Kbps increments. This field will be <N/A> if no network module is installed.	**IDSL**	**ADSL**		**SDSL**
		64K **128K**	**Up Stream** **64K** **128K** **256K** **512K**	**Down Stream** **256K** **512K** **1M** **1.5M**	**144K** **272K** **400K** **528K** **784K** **1168K** **1552K** **2320K**
Encapsulation	The Prestige supports PPP encapsulation.[1]	**PPP**			

[1] RFC 1483 is not supported at the time of writing this manual.

Field	Description	Option
Authen(tication) Method	This field sets the authentication method for incoming calls. You can choose Local or RADIUS. The default for this field is Local. Please see the next section on User Authentication for more details.	**Local, RADIUS**
Protocol	Press the [SPACE BAR], then [ENTER] to choose from **None**, **CHAP/PAP**, **CHAP** or **PAP**. The default is **None**.	**None, CHAP, PAP, CHAP/PAP**
User Name	This will be used as the login name for local authentication. You can enter a name with up to 31 characters. This will be N/A when you choose RADIUS as your authentication method.	
Password	Enter the password for the remote user. This will be N/A when you choose RADIUS as your authentication method.	
IP Address Assigned to Client	Refers to the IP address assigned to the CPE (Customer Premises Equipment), i.e., the client device connected to the Prestige.	
Start of Public IP Address	Refers to the public IP address assigned to the hosts behind the CPE. The IP range contains contiguous IP addresses and this field specifies the first one in the range.	
IP Count	In this field enter the number of addresses in the public IP range. For example, if the starting address is 202.x.x.1 and the IP count is 6, then the pool will be from 202.x.x.1 to 202.x.x.6.	
Multicast	Turn on/off IGMP support IGMP-v2/IGMP-v1/None. Please refer to the Multicast section earlier in this manual for more details about this feature.	**IGMP-v1** **IGMP-v2** **None**
IP Policies	You can apply up to four IP policy sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, and 11.	

6.1.1 Example IDSL Port Setup

In **Menu 6.1,** the **Start of Public IP Address** and **IP Count** fields are for public IP addresses only. If NAT is not enabled, and the hosts behind the CPE have been assigned public IPs, then you must enter that information here to enable proper routing.



```
                          Menu 6.1 - Port Usage

                  Active= Yes
                  Device Type: IDSL
                  Speed= 128K

                  Encapsulation= PPP
                  Authen Method= Local
                    Protocol= None
                    User Name=
                    Password= ********

                  IP Address Assigned to Client= 192.168.255.2
                  Start of Public IP Address= a.95.1.100
                    IP Count= 6
                  Multicast= N/A
                  IP Policies=

                Press ENTER to Confirm or ESC to Cancel:

        Press Space Bar to Toggle.
```

Figure 6-4 Example IDSL Port Setup Configuration

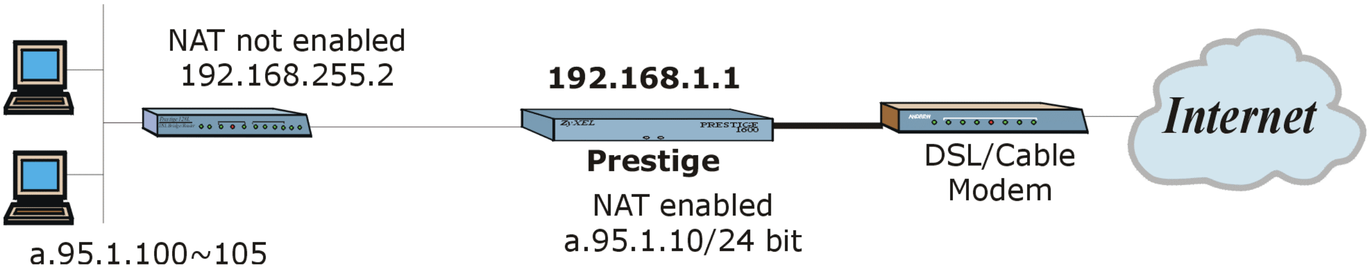


Figure 6-5 Example IDSL Port Setup Scenario

In this example, “a” is a number between 0 and 255 and is not acceptable entry for an IP address.

6.1.2 User Authentication

DSL users are authenticated against the DSL user profile in **Menu 6** or user information located at the external RADIUS server. Two options are available: **Local** and **RADIUS**.

Table 6-3 DSL User Authentication

Option	Action
Local	Use the user name and password entered in this menu for authentication.
RADIUS	Use the external RADIUS server to authenticate the user.

6.1.3 PAP/CHAP

Your Prestige supports both Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). CHAP is more secure than PAP because the password is not sent in clear text.

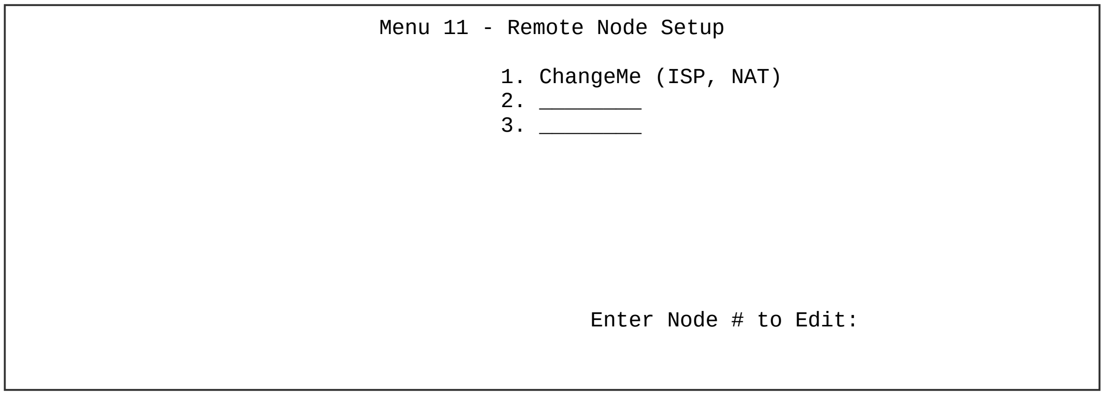
Chapter 7 Remote Node Configuration

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

A remote node is required for placing calls to a remote gateway. A remote node represents both the 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 a remote node.

7.1 Remote Node Setup

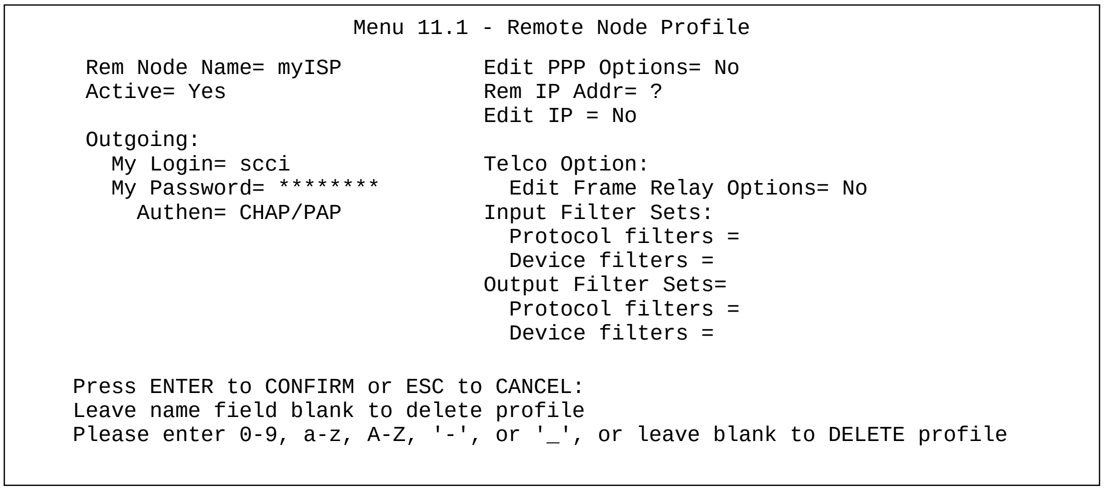
Select menu option 11 from the Main Menu to enter **Menu11.1 Remote Node Profile** as shown next.



```
                         Menu 11 - Remote Node Setup

                                  1. ChangeMe (ISP, NAT)
                                  2. ________
                                  3. ________







                                         Enter Node # to Edit:
```

Figure 7-1 Menu 11 – Remote Node Setup

Enter a remote node index number to bring up the following screen.



```
                        Menu 11.1 - Remote Node Profile

      Rem Node Name= myISP           Edit PPP Options= No
      Active= Yes                    Rem IP Addr= ?
                                     Edit IP = No
      Outgoing:
        My Login= scci               Telco Option:
        My Password= ********          Edit Frame Relay Options= No
          Authen= CHAP/PAP           Input Filter Sets:
                                       Protocol filters =
                                       Device filters =
                                     Output Filter Sets=
                                       Protocol filters =
                                       Device filters =

     Press ENTER to CONFIRM or ESC to CANCEL:
     Leave name field blank to delete profile
     Please enter 0-9, a-z, A-Z, '-', or '_', or leave blank to DELETE profile
```

Figure 7-2 Menu 11.1 - Remote Node Profile

The following table contains the instructions on how to configure the Remote Node Profile Menu for leased lines.

Table 7-1 Remote Node Profile Menu Fields for Leased Lines

Field	Description	Options
Rem Node Name	This is a required field. Enter a descriptive name for the remote node, e.g., myISP. This field can be up to eight characters.	
Active	Press [SPACE BAR] to toggle between **Yes** and **No**.	**Yes/No**
Outgoing: My Login Name	Enter the login name for your Prestige 1600 when it calls this remote node.	
Outgoing: My Password	Enter the password for your Prestige 1600 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 1600 will accept either CHAP or PAP when requested by this remote node. **CHAP** - accept CHAP only. **PAP** - accept PAP only.	**CHAP/PAP** **(default)** **CHAP** **PAP**
Edit PPP Options	To edit the PPP options for this remote node, move the cursor to this field, press the [SPACE BAR] to select **Yes** and press [ENTER]. This will bring you to **Menu 11.2 - Remote Node PPP Options**. For more information on configuring PPP options, see the section *Editing PPP Options*.	**Yes**
Rem IP Addr	This is a required field. Enter the IP address of the remote gateway.	
Edit IP	To edit the IP parameters, select **Yes** and press [ENTER]. This will bring you to Menu 11.3 - Remote Node Network Layer Options. For more information on this screen, refer to the section *Remote Node TCP/IP Configuration.*	**Yes**
Telco Option: Edit Frame Relay Options	Please see the WAN Port Setup chapter for a full discussion of this feature.	
Session Options: Input Filter Sets, Output Filter Sets	In these fields, enter the filter set(s) you wish to apply to the incoming and outgoing traffic between this remote node and your Prestige 1600. You can choose from 12 different filter sets. In addition, you can link up to 4 filter sets together for further customization, e.g., 1, 5, 9, 12. Note that spaces are accepted in this field. For more information on customizing your filter sets, *see Chapter 8*. The default is blank, i.e., no filters	**Default = Blank**

Field	Description	Options
	defined.	
Once you have completed filling in Menu 11.1.1 - Remote Node Profile, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

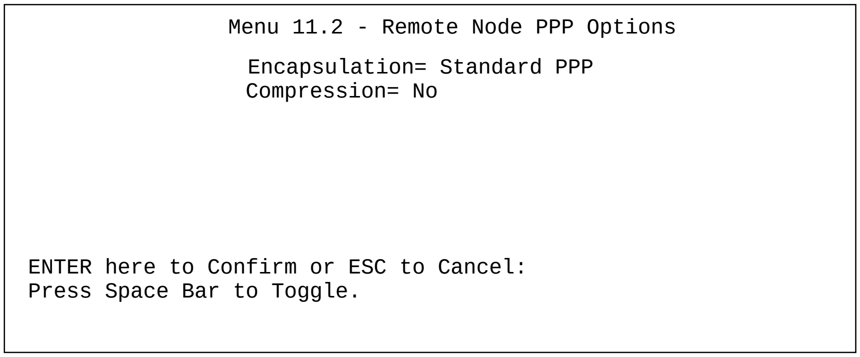
7.2 Outgoing Authentication Protocol

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

Note: Generally, the authentication option is decided by the server hence, for outgoing calls it is not necessary for you to configure this field except in cases where you are told by the remote server’s operator.

7.3 Editing PPP Options

To edit the PPP options of a remote node, move the cursor to the **Edit PPP Options** field in **Menu 11.1 - Remote Node Profile**, and press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.2**, as shown.



```
                 Menu 11.2 - Remote Node PPP Options

                  Encapsulation= Standard PPP
                  Compression= No







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

Figure 7-3 Menu 11.2 - Remote Node PPP Options

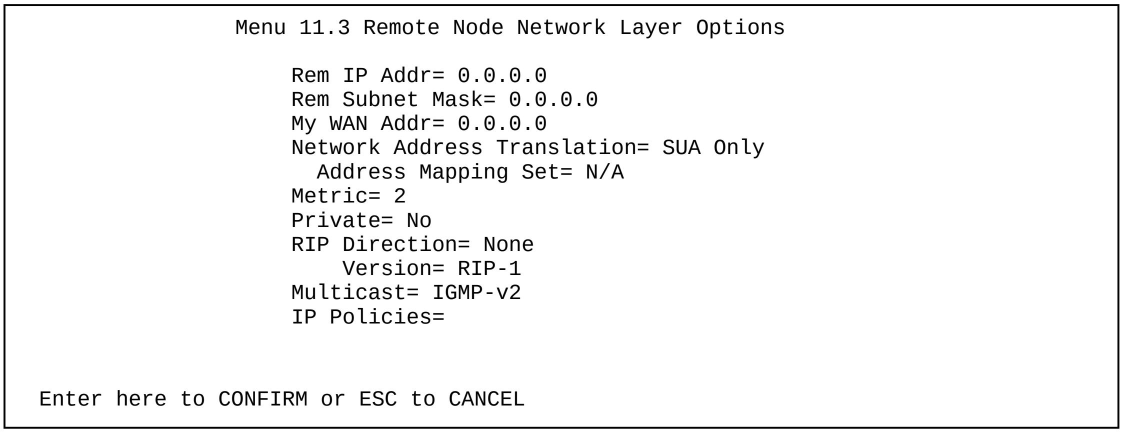
Table 7-2 Remote Node PPP Options Menu Fields describes the Remote Node PPP Options Menu, and contains instructions on how to configure the PPP options fields.

Table 7-2 Remote Node PPP Options Menu Fields

Field	Description	Option
Encapsulation	Select the vendor-specific encapsulation for the link. The default is Standard PPP. Select Cisco PPP only when the remote gateway is a Cisco machine. **Standard PPP** - Standard PPP encapsulation will be used. **CISCO PPP** - Cisco PPP encapsulation will be used.	 **Standard PPP** **CISCO PPP**
Compression	Turn on/off Stac data compression. The default for this field is **Off**.	**On/Off** (Default = Off)
Once you have completed filling in **Menu 11.2 - Remote Node PPP Options**, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.		

7.4 Edit IP Parameters

Move the cursor to the **Edit IP** field in **Menu 11.1 - Remote Node Profile**, then press [SPACE BAR] to toggle the value to **Yes**, and press [ENTER] to edit **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
                      Network Address Translation= SUA Only
                        Address Mapping Set= N/A
                      Metric= 2
                      Private= No
                      RIP Direction= None
                          Version= RIP-1
                      Multicast= IGMP-v2
                      IP Policies=


  Enter here to CONFIRM or ESC to CANCEL
```

Figure 7-4 Menu 11.3- Remote Node TCP/IP Options

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

Table 7-3 TCP/IP related fields in Menu 11.1 - Remote Node Profile

Field	Description	Option
Rem IP Address	Enter the IP address of the remote gateway in Menu 11.1 Remote Node Profile.	
Edit IP	Press [SPACE BAR] to select **Yes** and press [ENTER] to go to Menu 11.3 - Remote Node Network Layer Options.	**Yes/No**

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

Table 7-4 Remote Node TCP/IP Configuration

Field	Description	Option
Rem IP Address	This shows the IP address you entered for this remote node in the previous menu, Remote Node Profile.	
Rem IP Subnet Mask	Enter the subnet mask for the remote network.	
My WAN Addr	Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your Prestige 1600. Note that this is the address assigned to your local Prestige 1600, not the remote router.	
Network Address Translation	Please see the NAT chapter for a more detailed discussion on the Network Address Translation feature. The choices are **Full Feature, None** and **SUA Only.**	**Full Feature None** and **SUA Only**
Address Mapping Set= N/A	Enter the address mapping set you are applying to this remote node. **255** is the default (read-only) **SUA Only** set.	**1** to **4, 255**
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	**1 to 15**
Private	This parameter determines if the Prestige 1600 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 the RIP direction from **Both/In Only/Out Only/None**.	**Both/In Only/Out Only/None**
Version=	Press [SPACE BAR] to select the RIP version from **RIP-1/RIP-2B/RIP-2M**.	**RIP-1/ RIP-2B/ RIP-2M**

Field	Description	Option
Multicast	Turn on/off IGMP support and select the version from IGMP-v2/IGMP-v1/None.	**IGMP-v2** **IGMP-v2** **None**
IP Policies	You can apply up to four IP Policy sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11.	
Once you have completed filling in the Network Layer Options Menu, press [ENTER] to return to Menu 11. Press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.		

Chapter 8
Static Route

This chapter tells you how to configure static routes for the Prestige.

8.1.1 Basics

If you wish to know more about static route basics , please read on. Skip to the *Static Route Setup* section for the actual configuration.

Static routes tell a router 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 a router has no knowledge of the networks beyond. For instance, the Prestige knows about network N2 in the following diagram through remote node Router 1. However, the Prestige is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the Prestige about the networks beyond the remote nodes.

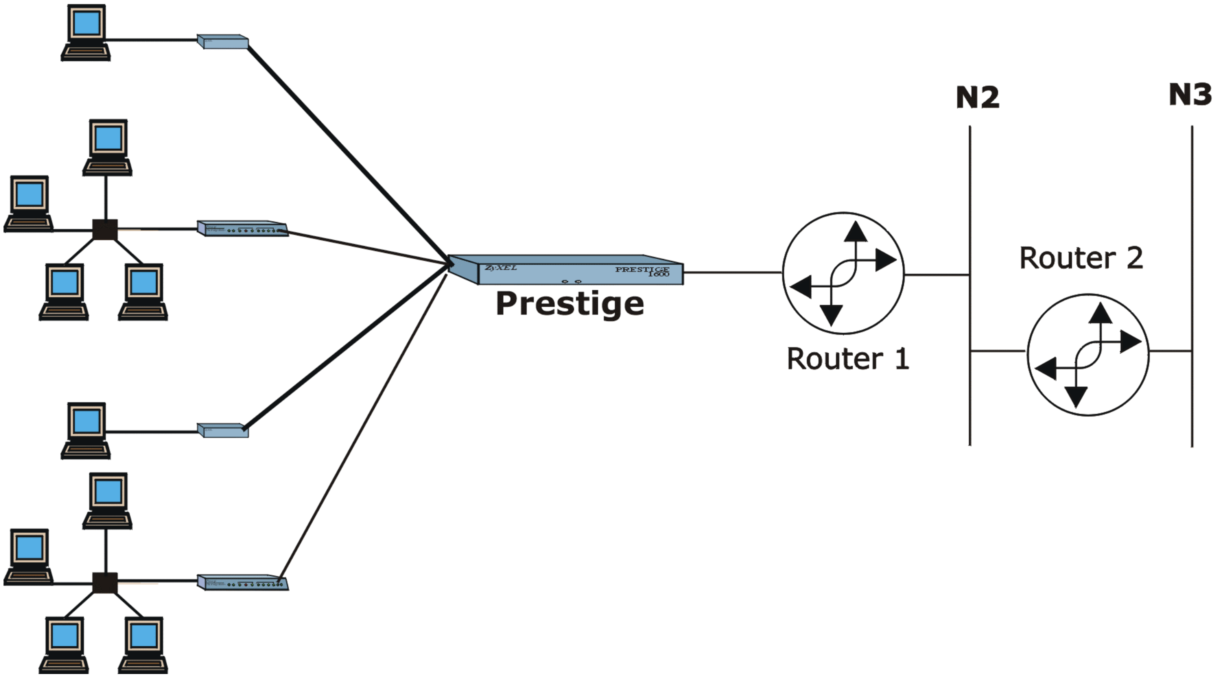
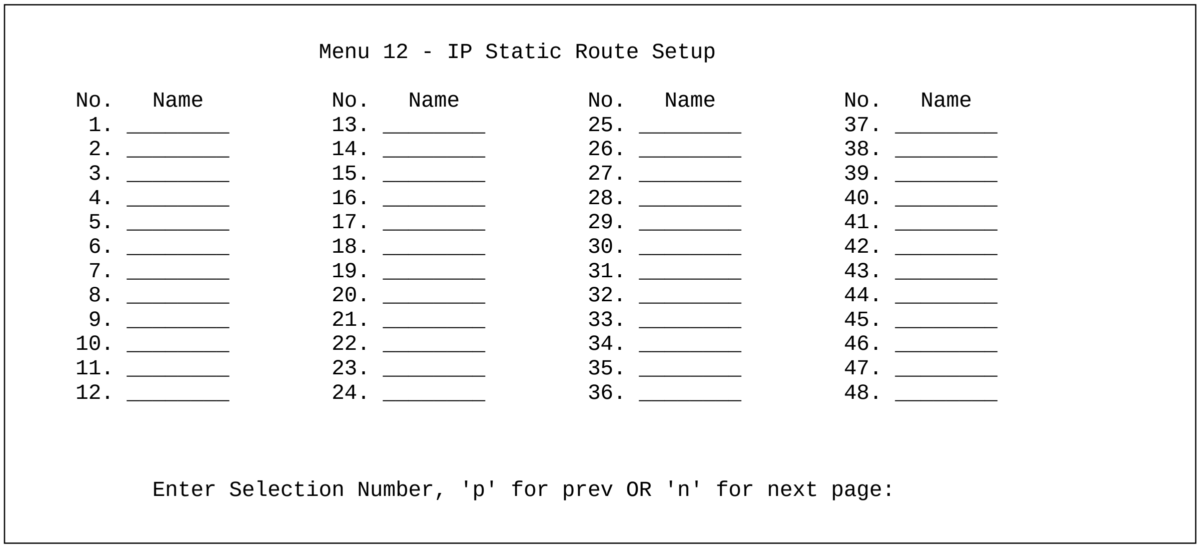


Figure 8-1 An Example of Static Routing Topology

8.1.2 Static Route Setup

Static routes are required if the DSL client has more than one public IP address. The routing information (static route) entered in the secondary machine will be passed to the primary machine through RIP. By adding static routes, the Prestige knows how to route packets belonging to the public IP addresses back to the DSL client's local network. The Prestige supports up to 240 static routes. Enter "p" to view a precious page of static routes and "n" to view the next page.

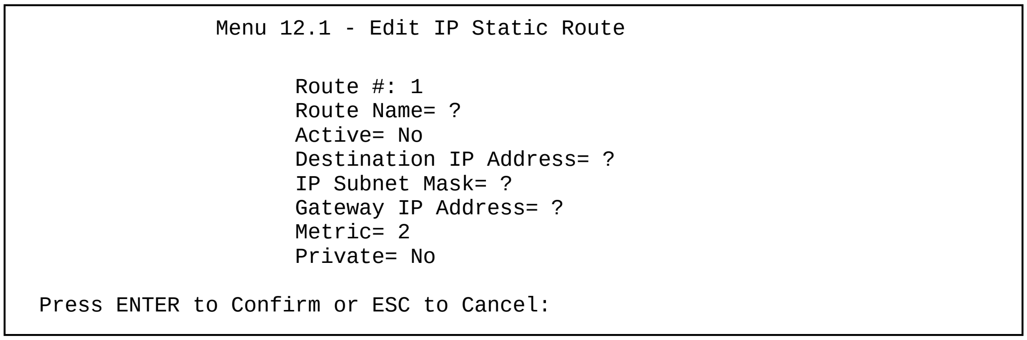
To configure an IP static route, use **Menu 12 - IP Static Route Setup**, as displayed next.



```
                   Menu 12 - IP Static Route Setup

No.   Name           No.   Name           No.   Name           No.   Name
 1. ________         13. ________         25. ________         37. ________
 2. ________         14. ________         26. ________         38. ________
 3. ________         15. ________         27. ________         39. ________
 4. ________         16. ________         28. ________         40. ________
 5. ________         17. ________         29. ________         41. ________
 6. ________         18. ________         30. ________         42. ________
 7. ________         19. ________         31. ________         43. ________
 8. ________         20. ________         32. ________         44. ________
 9. ________         21. ________         33. ________         45. ________
10. ________         22. ________         34. ________         46. ________
11. ________         23. ________         35. ________         47. ________
12. ________         24. ________         36. ________         48. ________



      Enter Selection Number, 'p' for prev OR 'n' for next page:
```

Figure 8-2 Menu 12 - IP Static Route Setup

Choosing a static route to edit produces the following screen.



```
                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 8-3 Menu 12.1 - Edit IP Static Route

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

Table 8-1 Edit IP Static Route Menu Fields

Field	Description	Options
Route #	This is the index number of the route as listed in **Menu 12 - IP Static Route Setup**.	
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.	**Yes/No**
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.	
IP Subnet Mask	Enter the subnet mask for this destination. Follow the discussion on IP subnet mask in this chapter.	
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Prestige that will forward the packet to the destination. On the LAN the gateway must be a router on the same segment as your Prestige; over WAN, the gateway must be the IP address of one of the remote nodes.	
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	**1 to 15**
Private	This parameter determines if the Prestige 1600 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**

Chapter 9
Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

9.1 Introduction

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, e.g., the source address of an outgoing packet, used within one network to a different IP address known within another network.

9.1.1 NAT Definitions

Inside/*outside* denotes where a host is located relative to the Prestige, e.g., the workstations of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts. *Global*/*local* denotes the IP address of a host in a packet as the packet traverses across a router, e.g., the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is travelling in the WAN side. Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Term	Definition
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

Please note that the IP address (either local or global) of an outside host is never changed.

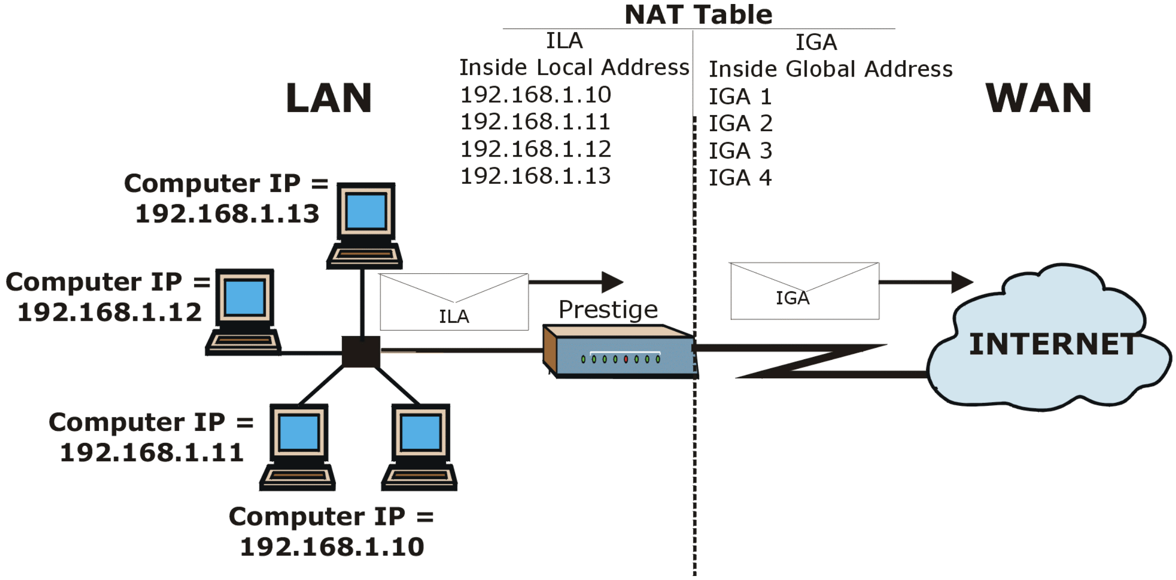
9.1.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, e.g., a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping - see below), NAT offers the additional benefit of firewall protection. If no server is defined in these cases, all incoming inquiries will be filtered out by your Prestige, thus preventing intruders from probing your network. For more information on IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT).*

9.1.3 How NAT works

Each packet has two addresses - a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) 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. NAT maps 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) in each packet and then forwards it to the Internet. 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

ILA Inside Local Address	IGA Inside Global 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
ILA
Prestige
IGA
INTERNET

Figure 9-1 How NAT Works

9.1.4 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.
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. One-to-One (range): In One-to-One (range) mode, the Prestige maps each local IP address to a unique global IP address.
5. Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
6. No-Change: This NAT mapping type allows you to assign global IPs to machines behind NAT.

Port numbers do *not* change for One-to-One, One-to-One (range) and No-Change NAT mapping types.

The following table summarizes these types.

Table 9-1 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

One-to-One (range):	ILA1←→ IGA1
	ILA2←→ IGA2
	ILA3←→ IGA3
	…
		1-1 Ra

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

No Change	IGA1←→ IGA1
	IGA2←→ IGA2
	IGA3←→ IGA3
	…
		No-Ch

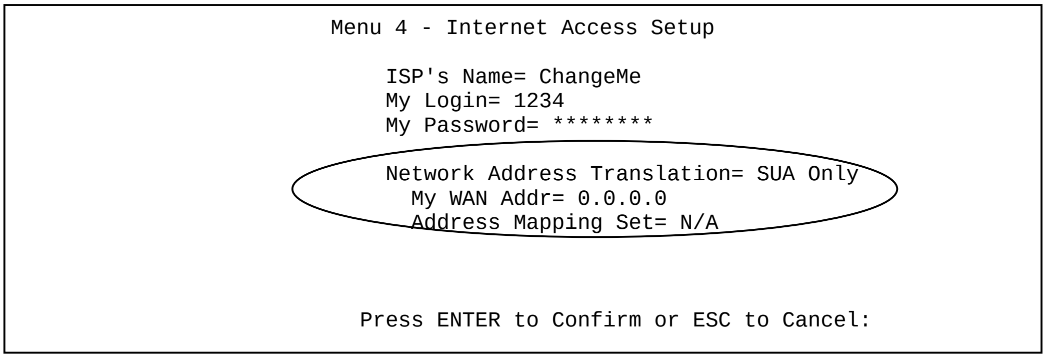
9.1.5 SUA (Single User Account) Versus NAT

SUA (Single User Account) in previous ZyNOS versions is a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See *section 9.2.3* for a detailed description of the NAT set for SUA. The Prestige has **Full Feature** NAT support to map local IP addresses to global IP addresses of clients or servers using all mapping types as outlined in *Table 9-1*. The Prestige supports NAT sets on a remote node basis. The mapping sets are reusable, but only one set is allowed for each remote node. Set 255 is for **SUA Only** which is a convenient, pre-configured, read only Many-to-1 port mapping set, sufficient for users with just one public IP.

9.2 SMT Menus

9.2.1 Applying NAT in the SMT Menus

You apply NAT via menus 4 or 11.3. 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**.



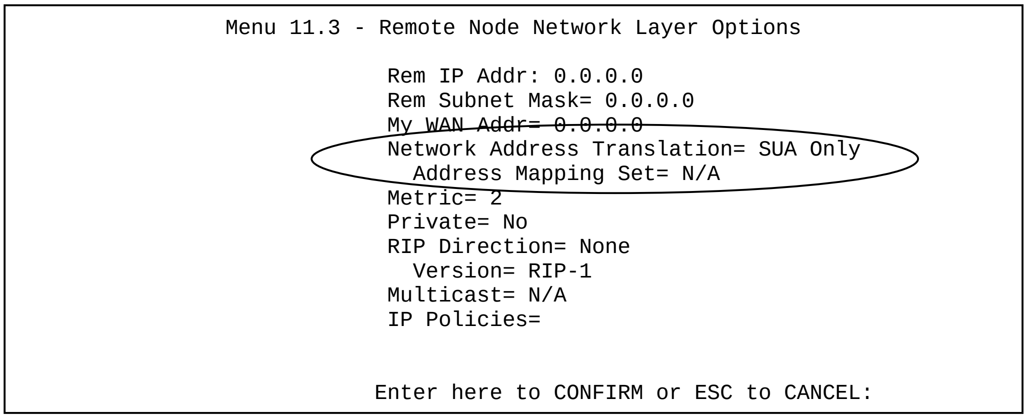
```
                    Menu 4 - Internet Access Setup

                        ISP's Name= ChangeMe
                        My Login= 1234
                        My Password= ********

                        Network Address Translation= SUA Only
                          My WAN Addr= 0.0.0.0
                          Address Mapping Set= N/A



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

Figure 9-2 Applying NAT for Internet Access

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

Step 1. Enter 11 from the Main Menu.

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



```
                Menu 11.3 - Remote Node Network Layer Options

                             Rem IP Addr: 0.0.0.0
                             Rem Subnet Mask= 0.0.0.0
                             My WAN Addr= 0.0.0.0
                             Network Address Translation= SUA Only
                               Address Mapping Set= N/A
                             Metric= 2
                             Private= No
                             RIP Direction= None
                               Version= RIP-1
                             Multicast= N/A
                             IP Policies=


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

Figure 9-3 Applying NAT to the Remote Node

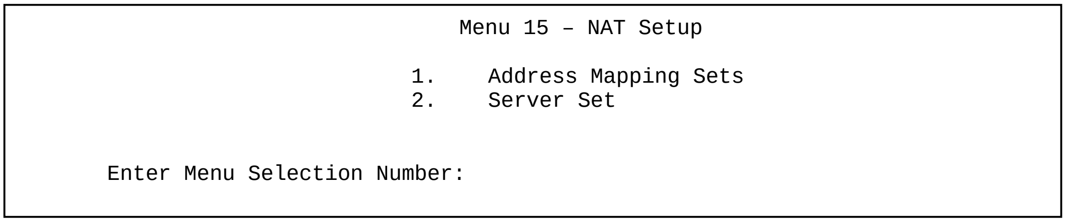
The following table describes the options for Network Address Translation.

Table 9-2 Applying NAT in Menus 4 & 11.3

Field	Description
Network Address Translation	**Full Feature:** You can configure any of the 6 mapping types described in *Table 9-1*.
	SUA Only: When you select this option the SMT will use Address Mapping Set 255 (Menu 15.1 - *see section 9.2.3*). It is a convenient, pre-configured, read only Many-to-1 port mapping set, sufficient for most purposes (especially for users with just one public IP) and helpful to people already familiar with SUA in previous ZyNOS versions. Note that there is also a **Server** type whose IGA is 0.0.0.0 in this set.
	None: NAT is disabled when you select this option.
Address Mapping Set	This is the Address Mapping Set that you wish to apply to this node. Set 255 is reserved for SUA.

9.2.2 Configuring NAT

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



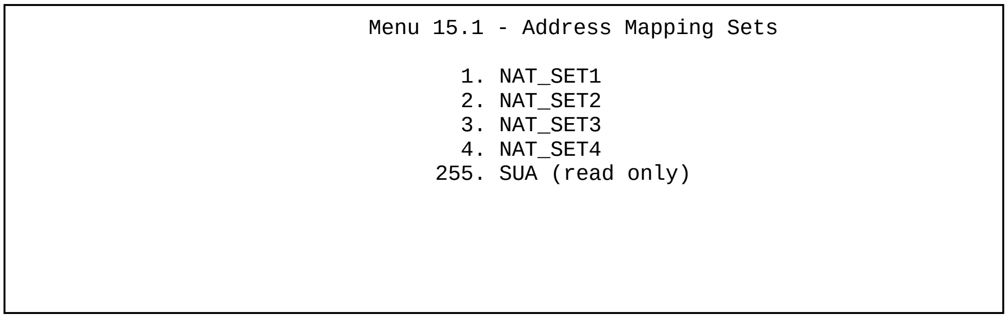
```
                              Menu 15 – NAT Setup

                          1.    Address Mapping Sets
                          2.    Server Set


        Enter Menu Selection Number:
```

Figure 9-4 Menu 15 NAT Setup

9.2.3 Address Mapping Sets and NAT Server Sets:

Use the Address Mapping Sets menus and submenus to create the mapping table for translation. Each remote node must specify which NAT Address Mapping Set to use. You can only configure set 1 to 4, which supports all mapping types as outlined in *Table 9-1*. Set 255 is used for SUA. When you select **SUA Only**, the SMT will use the pre-configured Set 255 (read only) **-** *see section 9.1.5*.

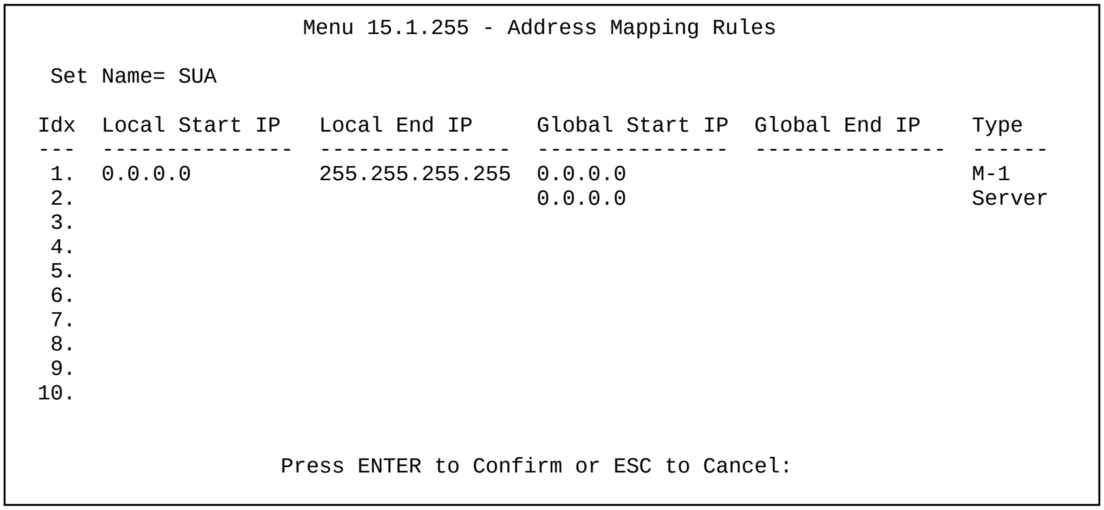
Enter 1 to bring up **Menu 15.1 - Address Mapping Sets**.



```
                    Menu 15.1 - Address Mapping Sets

                          1. NAT_SET1
                          2. NAT_SET2
                          3. NAT_SET3
                          4. NAT_SET4
                        255. SUA (read only)
```

Figure 9-5 Menu 15.1 Address Mapping Sets

Let's look first at Option 255 (*see section 9.1.5)*. The fields in this menu cannot be changed. Entering 255 brings up the following screen.



```
                       Menu 15.1.255 - Address Mapping Rules

   Set Name= SUA

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


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

Figure 9-6 SUA Address Mapping Rules

The following table explains the fields in this screen.

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

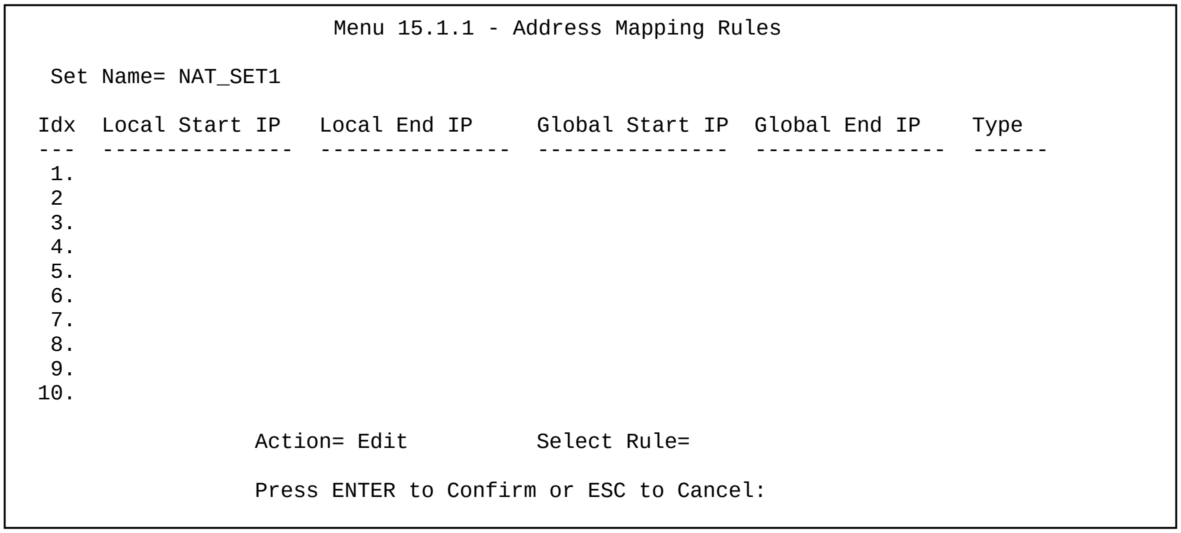
Table 9-3 SUA Address Mapping Rules

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 Local End IP	Local Start IP is the starting local IP address (ILA) (*see Figure 9-1)*. Local End IP 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.	**0.0.0.0** **255.255.255.255**
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the Global Start IP.	**0.0.0.0**
Global End IP	This is the ending global IP address (IGA).	**N/A**
Type	These are the mapping types discussed above (*see Table 9-1*). Type **Server** allows you to specify a server of a given service behind NAT. *See section 9.4.3 below* for some examples.	**Server**

Note: For all Local and Global IPs, the End IP address must be numerically greater than the IP Start address.

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

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



```
                       Menu 15.1.1 - Address Mapping Rules

  Set Name= NAT_SET1

 Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
 ---  ---------------  ---------------  ---------------  ---------------  ------
  1.
  2
  3.
  4.
  5.
  6.
  7.
  8.
  9.
 10.

                 Action= Edit          Select Rule=

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

Figure 9-7 First Set in Menu 15.1.1

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

9.2.4 Ordering Your Rules

Ordering your rules is important because the Prestige applies the rules in the order that you specify. When a rule matches the current packet, the Prestige takes the corresponding action and the remaining rules are ignored. 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 rules 5, 6 and 7 become new rules 4, 5 and 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.

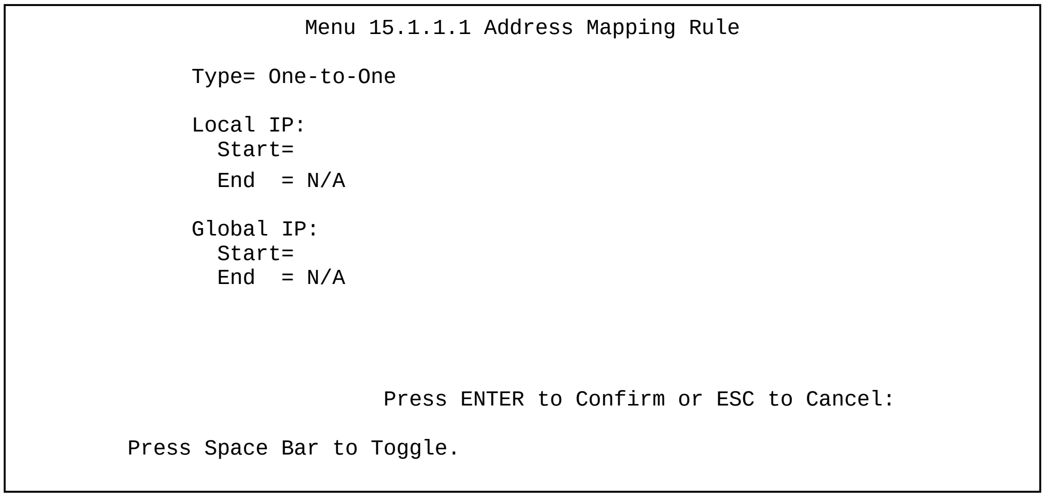
Table 9-4 Menu 15.1.1

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.	
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 indices of the rules after the selected one will be decremented by 1. **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.	

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

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

Selecting **Edit** in the **Action** field and then entering a rule number 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 Address Mapping Rule

              Type= One-to-One

              Local IP:
                Start=
                End  = N/A

              Global IP:
                Start=
                End  = N/A




                             Press ENTER to Confirm or ESC to Cancel:

         Press Space Bar to Toggle.
```

Figure 9-8 Editing an Individual Rule in a Set

The following table describes the fields in this screen.

Table 9-5 Menu 15.1.1.1 - configuring an individual rule

Field	Description	Option/Example
Type	Press the [SPACEBAR] to toggle through a total of 6 types. These are the mapping types discussed above (*see Table 9-1*). Type Server allows you to specify multiple servers of different types behind NAT to this machine. *See section 9.4.3 below* for some examples.	**One-to-One** **Many-to-One** **Many-to-Many Overload** **One-to-One (range)** **Server** **No Change**
Local IP	Only local IP fields are N/A for server; Global IP fields MUST be set for Server.	
Start	This is the starting local IP address (ILA).	**0.0.0.0**
End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is N/A for One-to-One and Server types.	**255.255.255.255**
Global IP		
Start	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the Global IP Start. Note that Global IP Start can be set to 0.0.0.0 only if the types are Many-to-One or Server.	**0.0.0.0**
End	This is the ending global IP address (IGA). This field is N/A for One-to-One, Many-to-One and Server types.	**172.16.23.55**

Note: For all Local and Global IPs, the End IP address must be numerically greater than the Start IP address.

9.3 NAT Server Sets

A NAT server set is a list of inside servers (behind NAT on the LAN) that you can make visible to the outside world. **Menu 15.2 - NAT Server Sets** is used to configure these servers.

9.3.1 Multiple Servers behind NAT

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

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

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

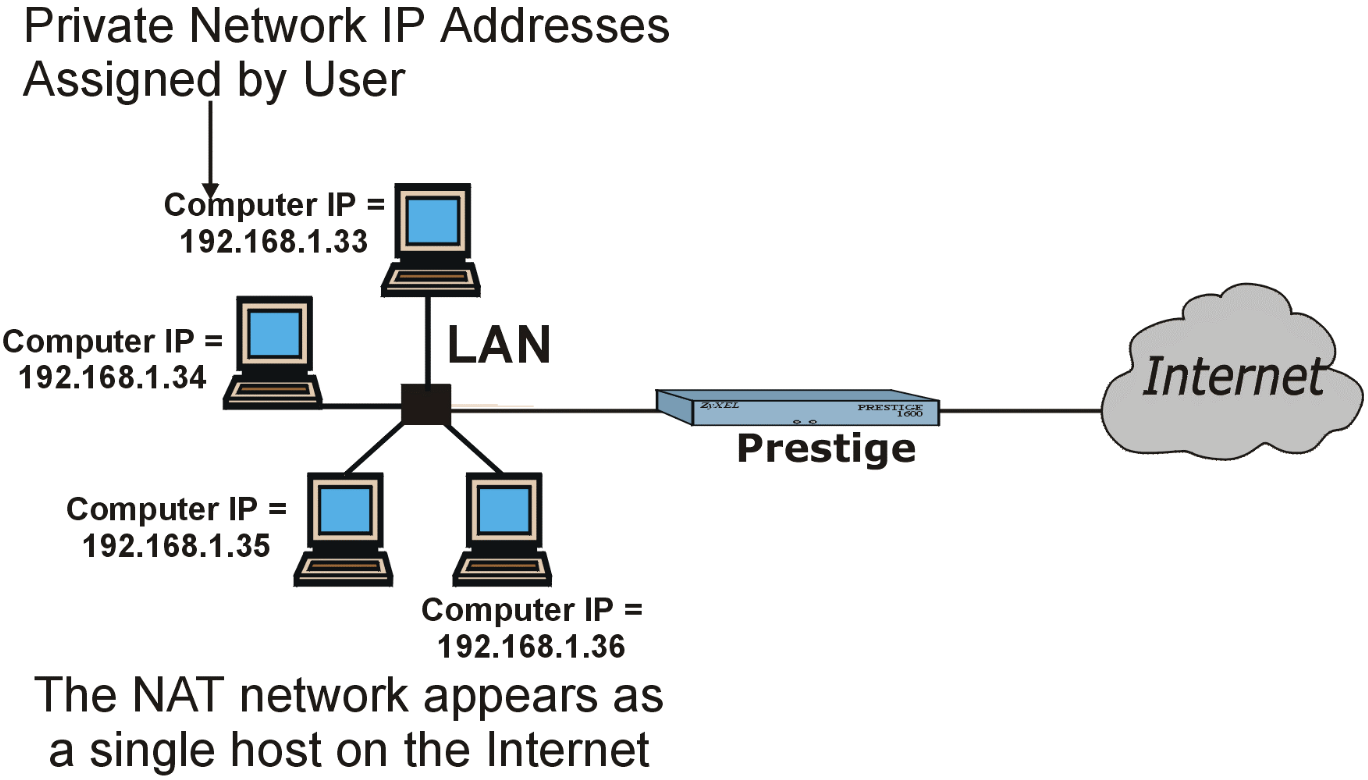

Private Network IP Addresses Assigned by User
Computer IP = 192.168.1.33
Computer IP = 192.168.1.34
LAN
Computer IP = 192.168.1.35
Computer IP = 192.168.1.36
ZyXEL
PRESTIGE 1600
Prestige
Internet
The NAT network appears as a single host on the Internet

Figure 9-9 Multiple Servers Behind NAT

9.3.2 Configuring Inside Servers

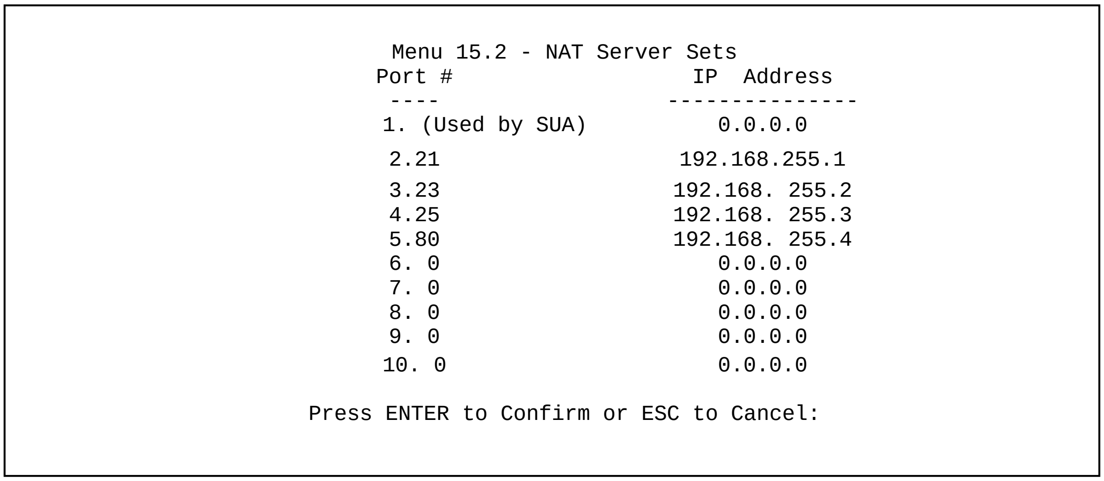
Follow the steps below to configure a server behind NAT:

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

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

Step 3. Enter the service port number in the **Port #** field and the inside IP address of the server in the IP Address field.

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 the included disk for more examples and details on NAT.



```
                          Menu 15.2 - NAT Server Sets
                         Port #                  IP  Address
                          ----                 ---------------
                          1. (Used by SUA)          0.0.0.0
                          2.21                  192.168.255.1
                          3.23                 192.168. 255.2
                          4.25                 192.168. 255.3
                          5.80                 192.168. 255.4
                          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

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

Figure 9-10 Menu 15.2 - NAT Server Setup

Table 9-6 Common Services & Port numbers

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

9.4 Examples

9.4.1 Internet Access Only

In this Internet access example, you only need one rule where all the ILAs (Inside Local Addresses) map to one dynamic IGA (Inside Global Address) assigned by your ISP.

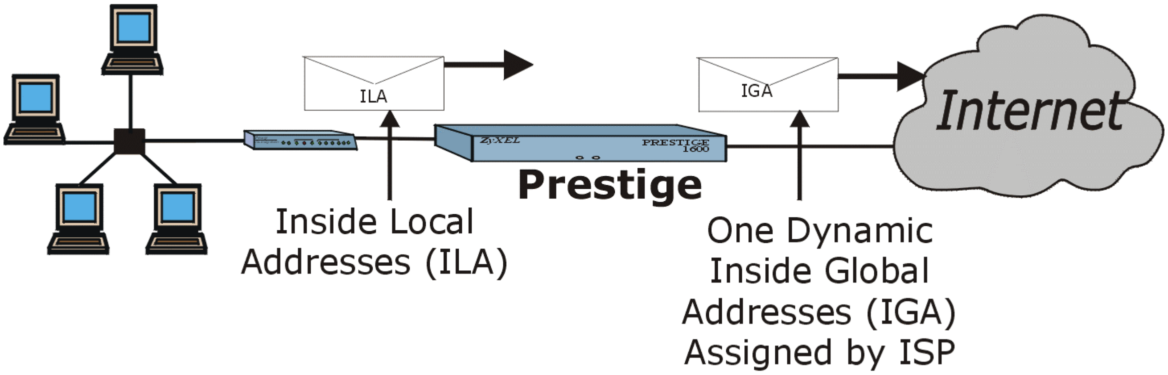
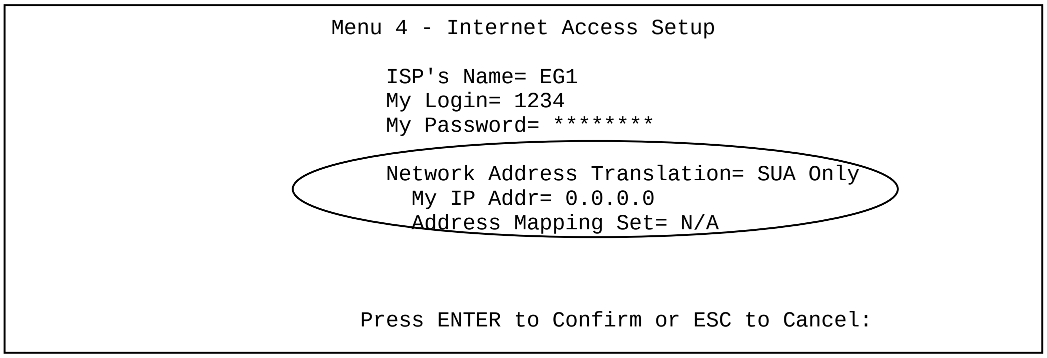


Figure 9-11 NAT Example 1



```
                          Menu 4 - Internet Access Setup

                              ISP's Name= EG1
                              My Login= 1234
                              My Password= ********

                              Network Address Translation= SUA Only
                                My IP Addr= 0.0.0.0
                                Address Mapping Set= N/A



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

Figure 9-12 NAT Example for Internet Access

In Menu 4 choose the **SUA Only** option for the **Network Address Translation** field. This is a pre-configured Many-to-One mapping discussed in *section 9.1.4.*

9.4.2 Example 2 - Internet Access with a Default Inside Server

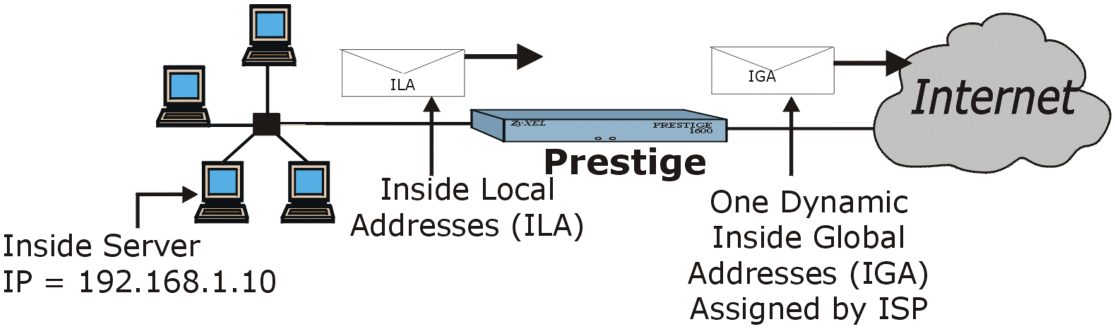
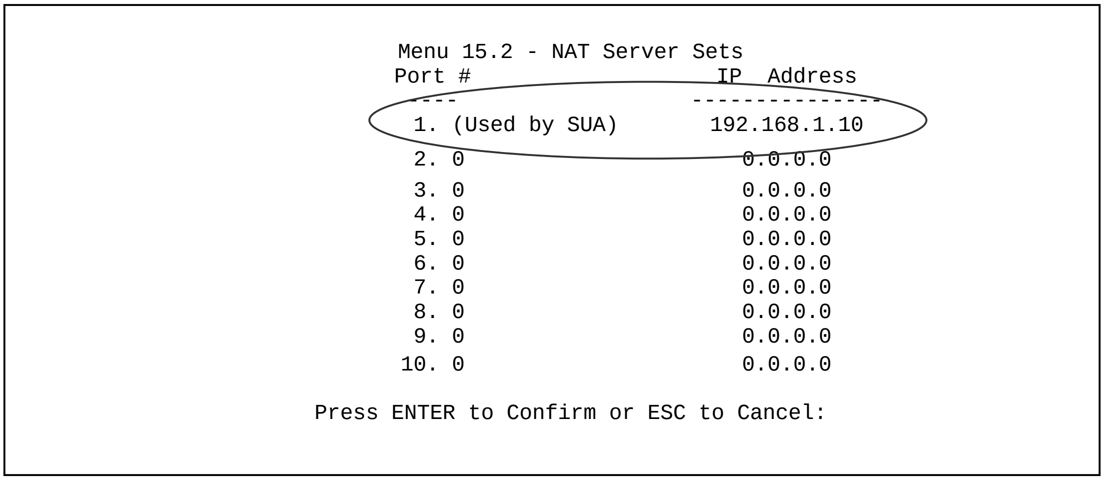


Figure 9-13 NAT Example 2

In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to Menu 15.2 to specify the inside server behind the NAT as shown in the next figure. All incoming connections are forwarded to the default inside server at the IP address specified.



```
                    Menu 15.2 - NAT Server Sets
                    Port #                   IP  Address
                     ----                  ---------------
                     1. (Used by SUA)       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

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

Figure 9-14 Specifying an Inside Sever

9.4.3 Example 3 - General Case

In this example, there are 3 IGAs from your ISP. There are many departments but two have their own FTP server. All departments share the same router. You want to reserve 1 IGA for each department with an FTP server and the other IGA is used by all. You want to map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. You also want to map the third IGA to an inside web server and mail server. You need to configure 4 rules as follows.

Rule 1. You map the first IGA to the first inside FTP server (**1: 1** mapping, giving both local and global IP addresses).

Rule 2. You map the second IGA to the second inside FTP server (**1: 1** mapping, giving both local and global IP addresses).

Rule 3. You map all other addresses to IGA3 (**Many : 1** mapping).

Rule 4. You also use the third IGA to open the web server and mail server on the LAN. Type **Server** allows us to specify a server, of a given service behind NAT.

The situation looks somewhat like this:

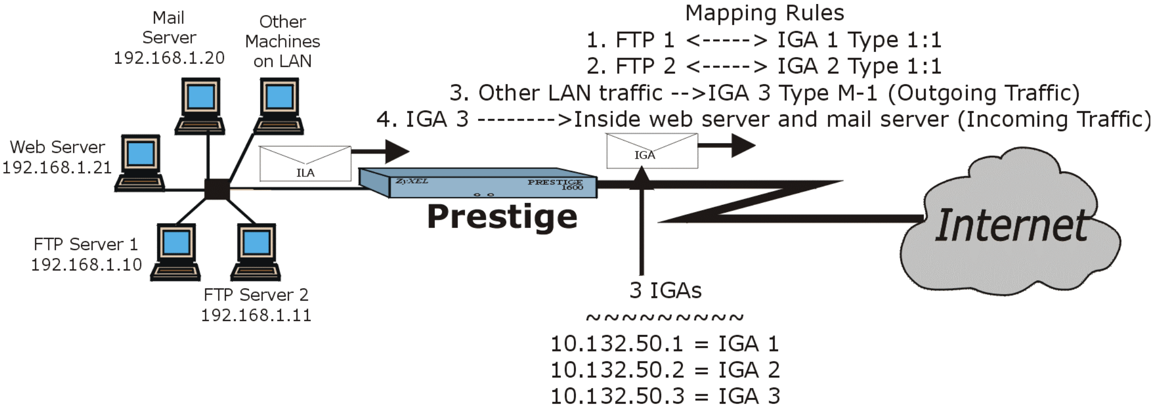

Mail Server 192.168.1.20
Other Machines on LAN
Web Server 192.168.1.21
FTP Server 1 192.168.1.10
FTP Server 2 192.168.1.11
ILA
ZyXEL
PRESTIGE 1600
Prestige
IGA
Internet
Mapping Rules
1. FTP 1 <-----> IGA 1 Type 1:1
2. FTP 2 <-----> IGA 2 Type 1:1
3. Other LAN traffic -->IGA 3 Type M-1 (Outgoing Traffic)
4. IGA 3 -------->Inside web server and mail server (Incoming Traffic)
3 IGAs
~~~~~~~~~~
10.132.50.1 = IGA 1
10.132.50.2 = IGA 2
10.132.50.3 = IGA 3

Figure 9-15 NAT - Example 3
~~~~~~~~~~

Step 1. You need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets.** Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in Menu 4 or Menu 11.3).

Step 2. Enter 15 from the Main Menu.

Step 3. Enter 1 to configure the Address Mapping Sets.

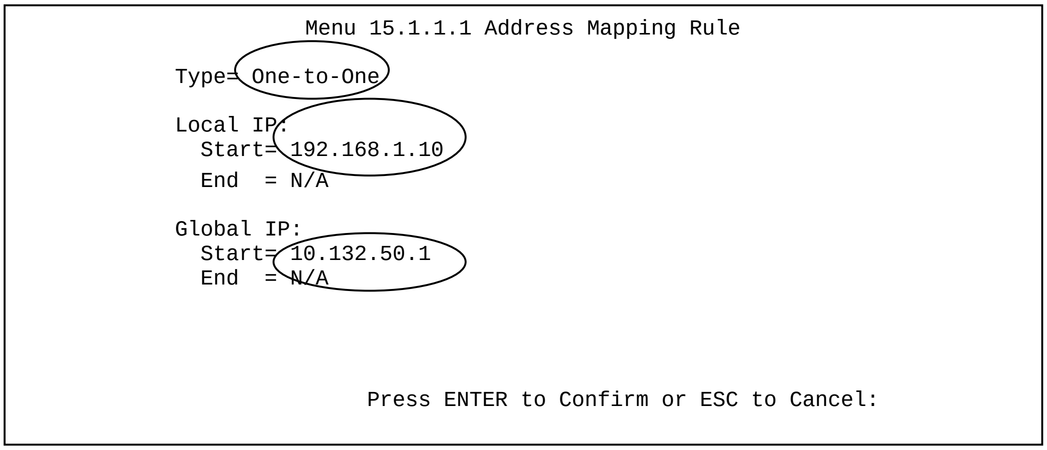
Step 4. Choose 1 to begin configuring this new set. Enter a **Set Name**, choose the **Edit Action** and then select **1** from **Select Rule** field. Press [ENTER] to confirm.

Step 5. Select **Type=** as **One-to-One** 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 (the first IGA). (*See Figure 9-16)*

Step 6. Repeat the previous step for rules 2 to 4 as outlined above.

Step 7. When finished, Menu 15.1.1 should look like as shown in *Figure 9-17*.

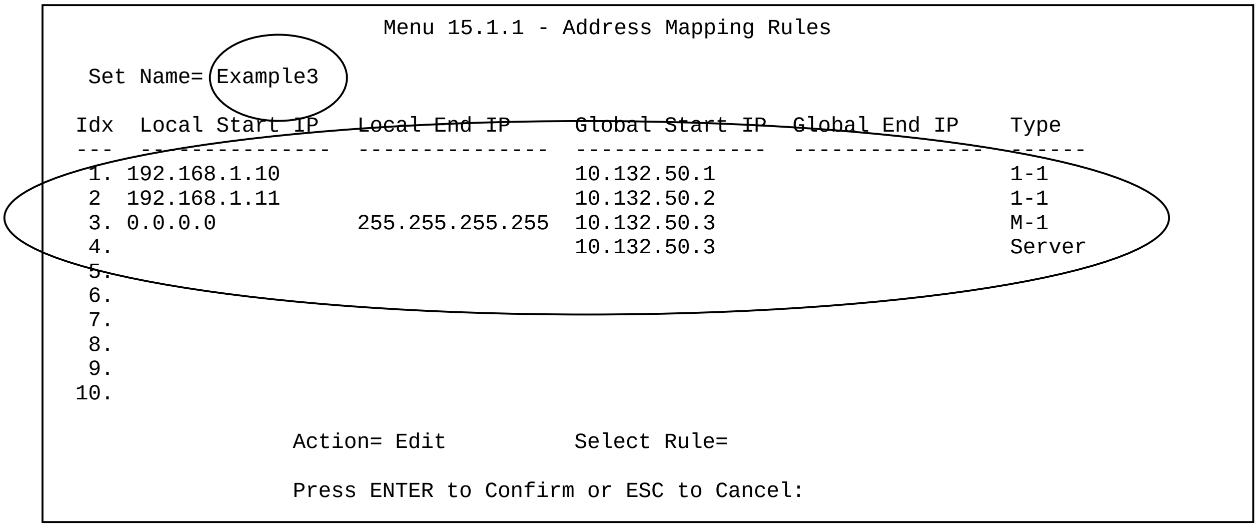
The following figure shows how to configure the first rule.



```
                       Menu 15.1.1.1 Address Mapping Rule

             Type= One-to-One

             Local IP:
               Start= 192.168.1.10
               End  = N/A

             Global IP:
               Start= 10.132.50.1
               End  = N/A




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

Figure 9-16 Example 3 - Menu 15.1.1.1

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



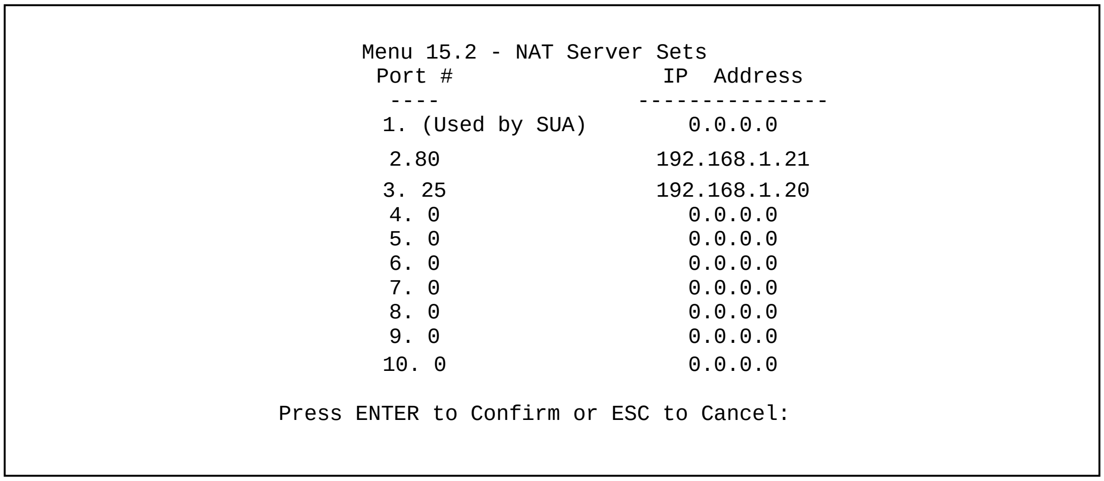
```
                         Menu 15.1.1 - Address Mapping Rules

   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.                                    10.132.50.3                       Server
   5.
   6.
   7.
   8.
   9.
  10.

                  Action= Edit          Select Rule=

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

Figure 9-17 Example 3 Final Menu 15.1.1

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

Step 8. Enter 15 from the Main Menu.

Step 9. Enter 2 from this menu and configure it as shown in *Figure 9-18*.



```
                     Menu 15.2 - NAT Server Sets
                      Port #                IP  Address
                       ----               ---------------
                      1. (Used by SUA)        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

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

Figure 9-18 Example 3 - Menu 15.2

9.4.4 NAT Unfriendly Application Programs

Many applications, e.g., gaming programs are NAT unfriendly because they embed addressing information in the data stream. In this case it is better to use the **No Change** NAT mapping type for computers running such applications behind NAT.

9.4.5 Example 4 - Remote Management

You can remotely manage a secondary P1600 behind NAT on the primary. Please see the *Remote Management* chapter.

9.4.6 Applying NAT to the Ethernet Port

You can also apply NAT to the Ethernet port if the **Configuration Type in** Menu 1 is **Standalone**. This feature is useful when you connect a broadband device such as a DSL modem or cable modem via the Ethernet port. NAT in **Menu 3.2** applies solely to the Ethernet port.

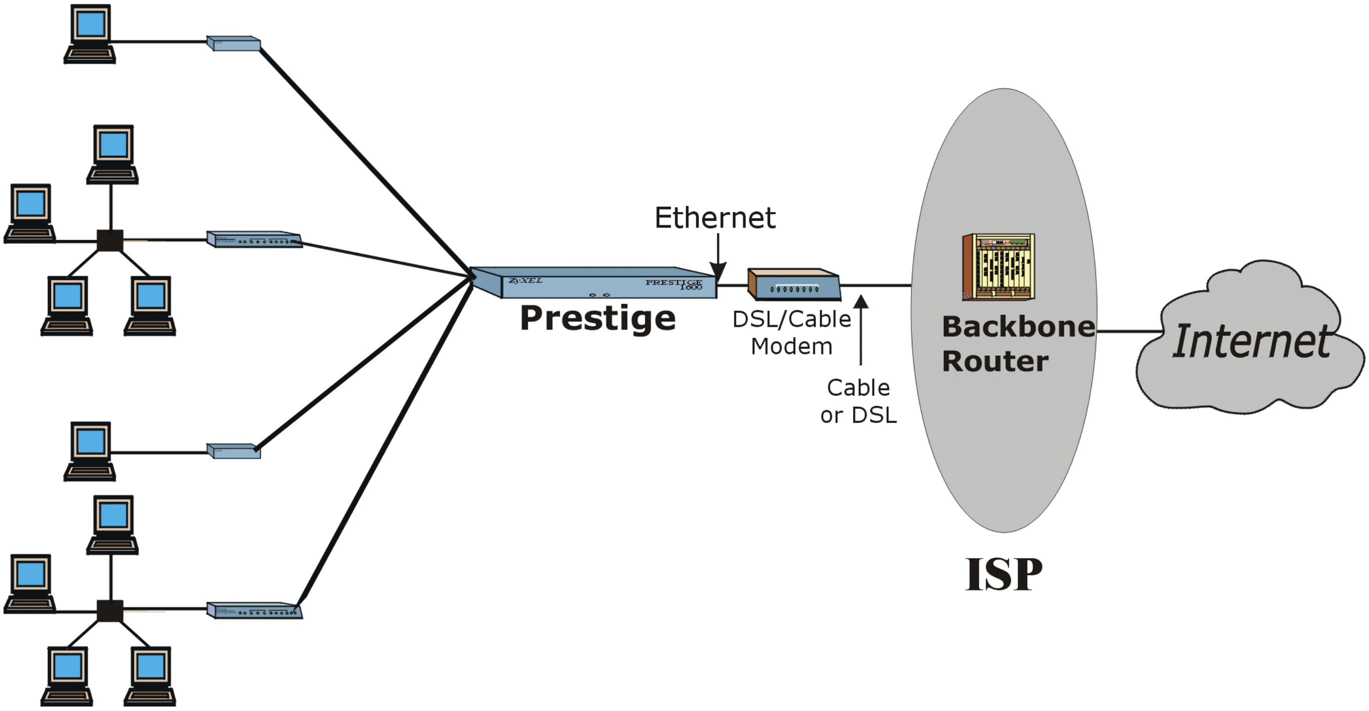
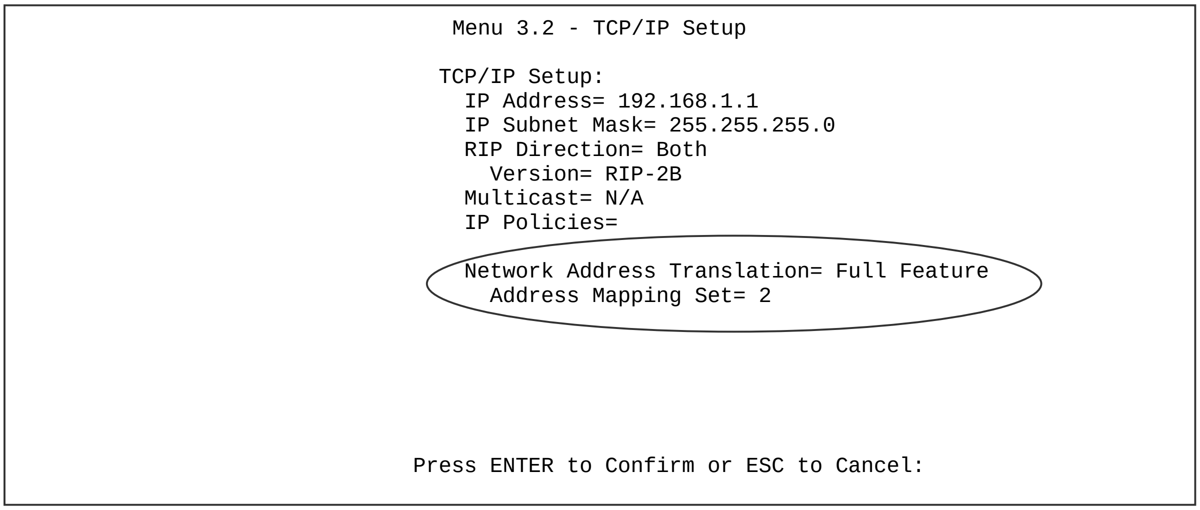


Figure 9-19 Ethernet SUA



```
   Menu 3.2 - TCP/IP Setup

  TCP/IP Setup:
    IP Address= 192.168.1.1
    IP Subnet Mask= 255.255.255.0
    RIP Direction= Both
      Version= RIP-2B
    Multicast= N/A
    IP Policies=

    Network Address Translation= Full Feature
      Address Mapping Set= 2




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

Figure 9-20 Applying NAT on the LAN Port

To use the Ethernet port for Internet Access, go to **Menu 12 - IP Static Route Setup** to set up the static default route using a P1600 standalone. Please refer to the chapter on *Remote Node Configuration* for more details.

Chapter 10
Filter Configuration

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

10.1 About Filtering

Your Prestige uses filters to decide whether to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens the data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the LAN 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 as shown in the following figure.

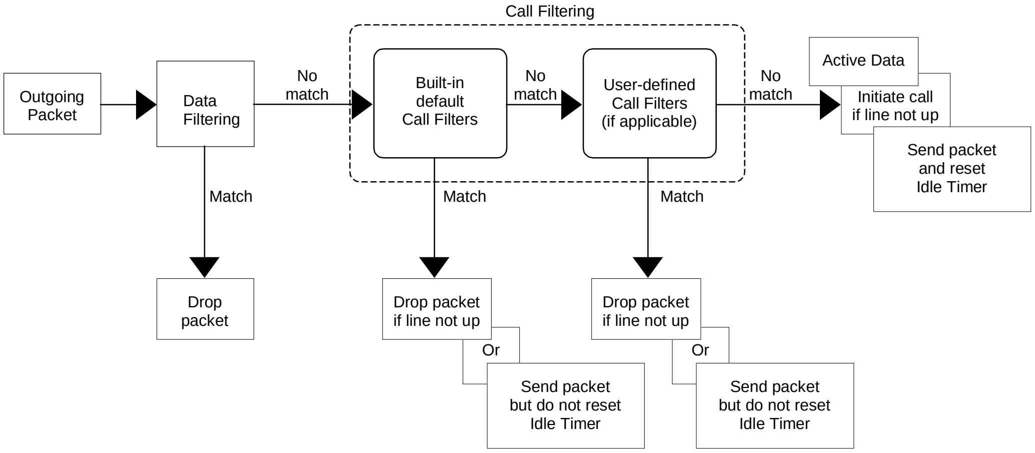

Call Filtering
Outgoing Packet
Data Filtering
No match
Built-in default Call Filters
No match
User-defined Call Filters (if applicable)
No match
Active Data
Initiate call if line not up
Send packet and reset Idle Timer
Match
Match
Match
Drop packet
Drop packet if line not up
Or
Send packet but do not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

Figure 10-1 Outgoing Packet Filtering Process

The following sections describe how to configure filter sets. Please see the application notes for more information and examples on creating and configuring filters.

10.2 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.

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

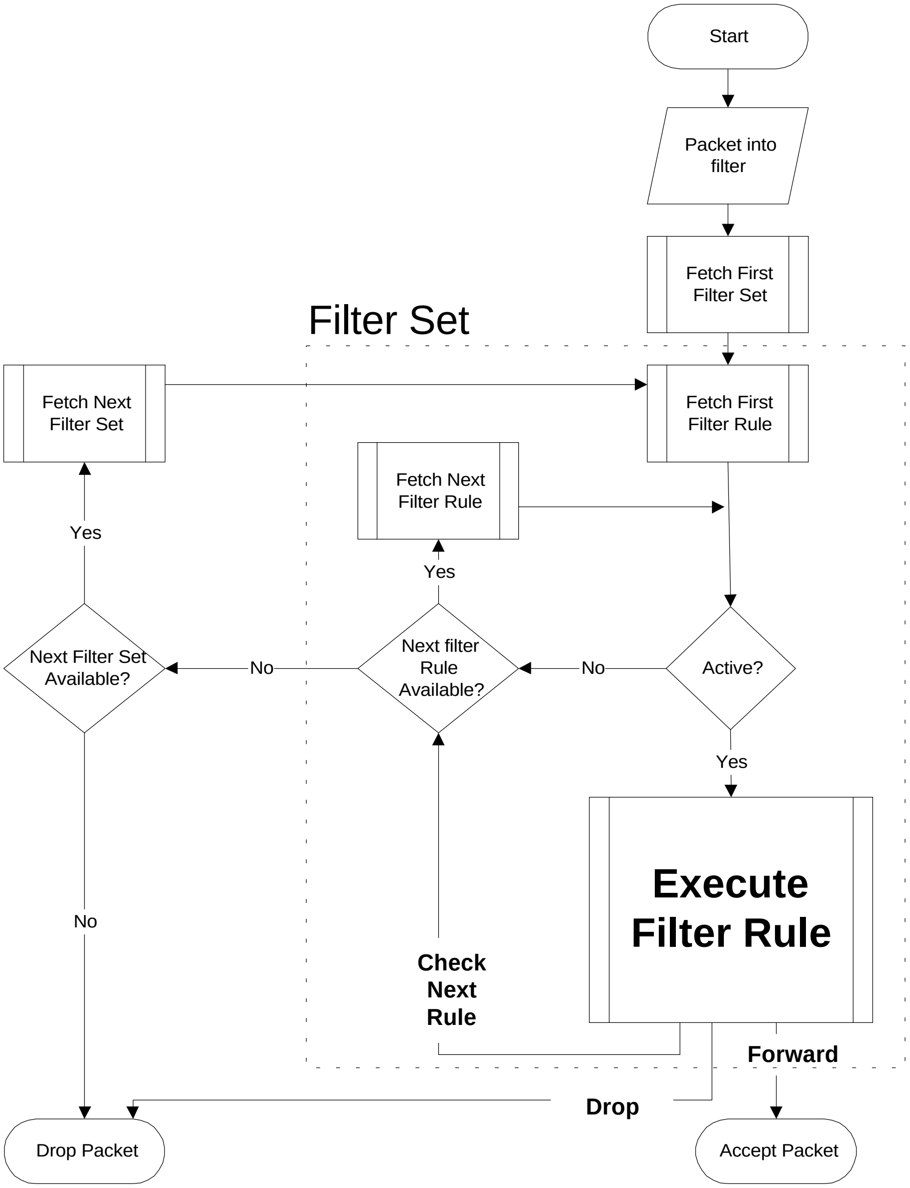
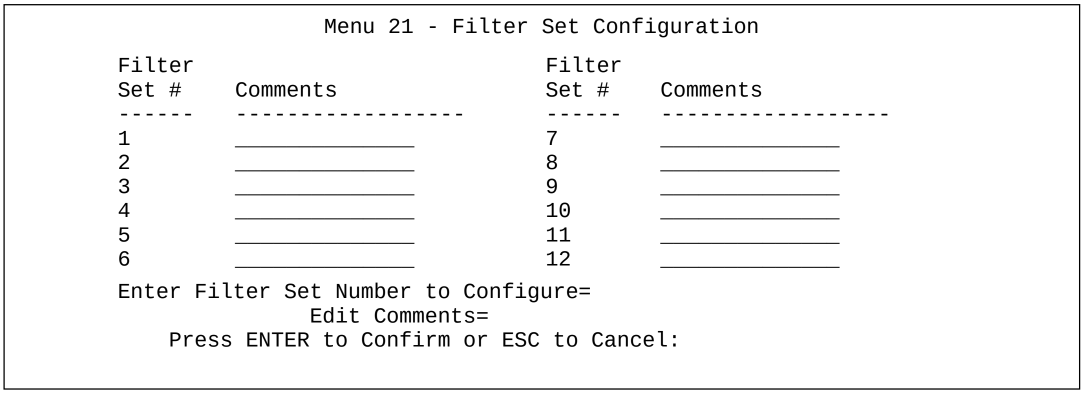


Figure 10-2 Filter Rule Process

10.3 Configuring a Filter Set

To configure a filter sets, follow the procedure below:

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



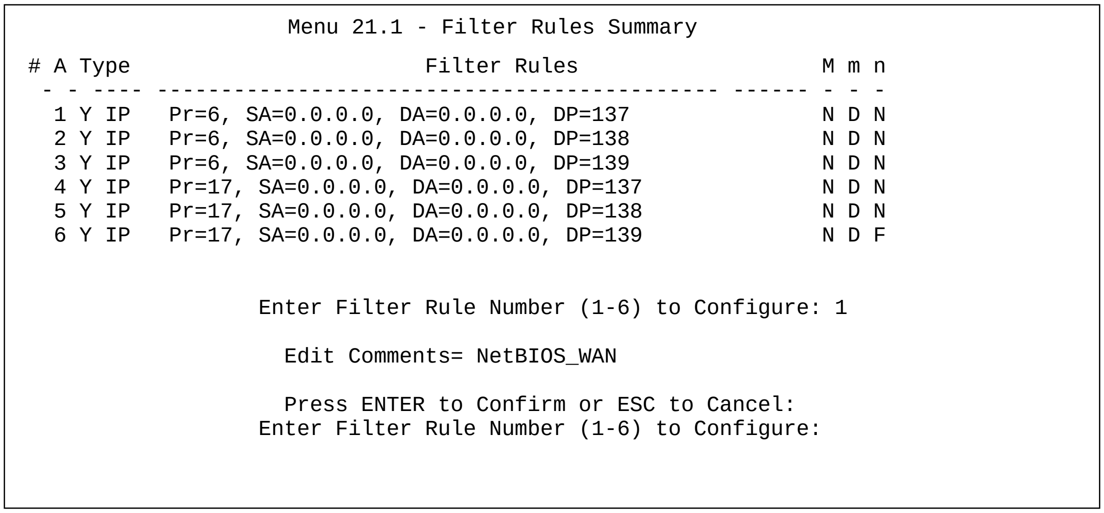
```
                Menu 21 - Filter Set Configuration

Filter                           Filter
Set #    Comments                Set #    Comments
------   ------------------      ------   ------------------
1        ______________          7        ______________
2        ______________          8        ______________
3        ______________          9        ______________
4        ______________          10       ______________
5        ______________          11       ______________
6        ______________          12       ______________
Enter Filter Set Number to Configure=
               Edit Comments=
    Press ENTER to Confirm or ESC to Cancel:
```

Figure 10-3 Menu 21 - Filter Set Configuration

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

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

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



```
                    Menu 21.1 - Filter Rules Summary

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


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

                    Edit Comments= NetBIOS_WAN

                    Press ENTER to Confirm or ESC to Cancel:
                  Enter Filter Rule Number (1-6) to Configure:
```

Figure 10-4 Menu 21.1 - Filter Rules Summary

10.3.1 Filter Rules Summary Menu

These screens show a summary of the existing rules in an example filter set. The following tables contain a brief description of the abbreviations used in **Menu 21.1** and **Menu 21.2**.

Table 10-1 Abbreviations Used in the Filter Rules Summary Menu

Abbreviations	Description	Display
#	Refers to the filter rule number (1-6).	
A	Refers to Active.	[Y] means the filter rule is active. [N] means the filter rule is inactive.
Type	Refers to the type of filter rule. This shows IP for TCP/IP, and Device	[IP] for TCP/IP [Dev] for Device
Filter Rules	The filter rule parameters are displayed here (see below).	
M	Refers to More. [Y] means an action can not yet be taken as there are more rules to check, which are concatenated with the present rule to form a rule chain. When the rule chain is complete an action can be taken. [N] means you can now specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked. If More is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**.	[Y] means there are more rules to check. [N] means there are no more rules to check.
m	Refers to Action Matched.	[F] means to forward the

Abbreviations	Description	Display
	[F] means to forward the packet immediately and skip checking the remaining rules if any.	packet. [D] means to drop the packet. [N] means check the next rule.
n	Refers to Action Not Matched [F] means to forward the packet immediately and skip checking the remaining rules if any.	[F] means to forward the packet. [D] means to drop the packet. [N] means check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

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

Table 10-2 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 Dev (device), the following abbreviations listed in the following table will be used.

Table 10-3 Abbreviations Used If Filter Type Is Dev

Abbreviation	Description
Off	Offset
Len	Length

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

10.4 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.

10.5 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** (Device) rules and Protocol Filter (**TCP/IP**) rules. Generic Filter rules act on the raw data from/to LAN and WAN. Protocol Filter rules act on the IP packets. Generic and TCP/IP filter rules are discussed in more detail in the next section. 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.

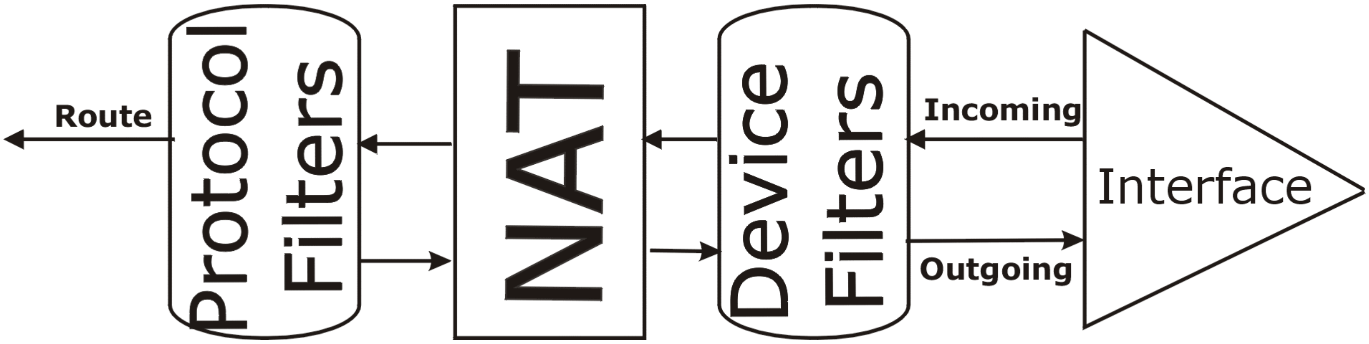


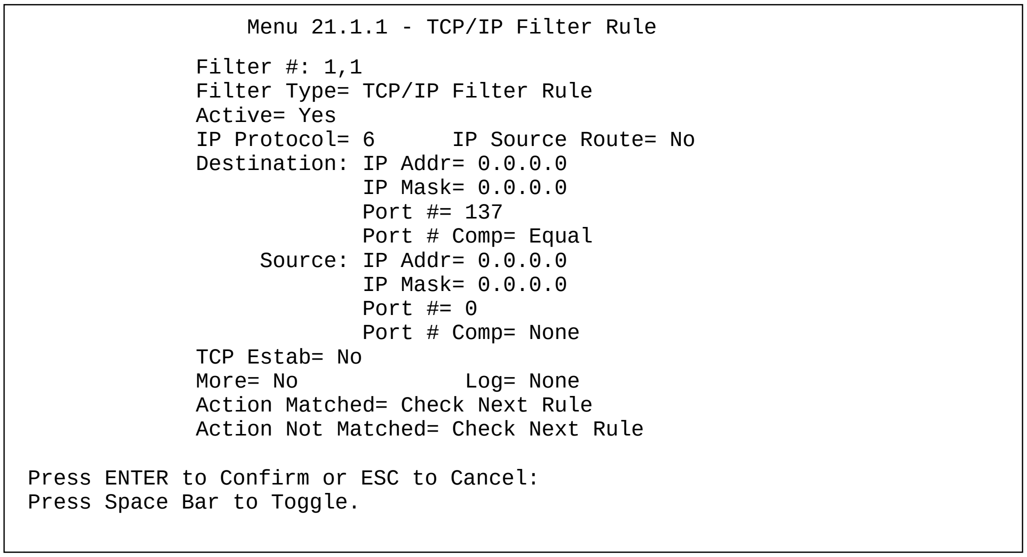
Figure 10-5 Protocol and Device Filter Sets

To speed up filtering, all rules in a filter set must be of the same type, i.e., Protocol filters or Device 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.

10.5.1 TCP/IP Filter Rule

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

To configure a TCP/IP rules, select TCP/IP Filter Rule from the Filter Type field and press Enter to open **Menu 21.1.1 - TCP/IP Filter Rule**, as shown 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= Check Next Rule
                Action Not Matched= Check Next Rule

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

Figure 10-6 Menu 21.1.1 - TCP/IP Filter Rule

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

Table 10-4 TCP/IP Filter Rule Menu Fields

Field	Description	Option
Filter #	This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third filter rule of that set.	
Filter Type	Press [SPACE BAR] to toggle between types of rules. Parameters displayed below each type will be different.	**Device Filter Rule / TCP/IP 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 and 255. Enter 0 if IP protocol is don't care.	**0-255**
IP Source Route	If **Yes**, the rule applies to packet with IP source route option; else the packet must not have source route option. The majority of IP packets do not have source route.	**Yes/No**
Destination: IP Addr	Enter the destination IP Address of the packet you wish to filter. This field is a ignored if it is 0.0.0.0.	
Destination: IP Mask	Enter the IP subnet mask to apply to the Destination: IP Addr. To filter a single host, enter 255.255.255.255 as the 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.	**0-65535**
Destination: Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in	**None/Less/Greater/Equal/Not**

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

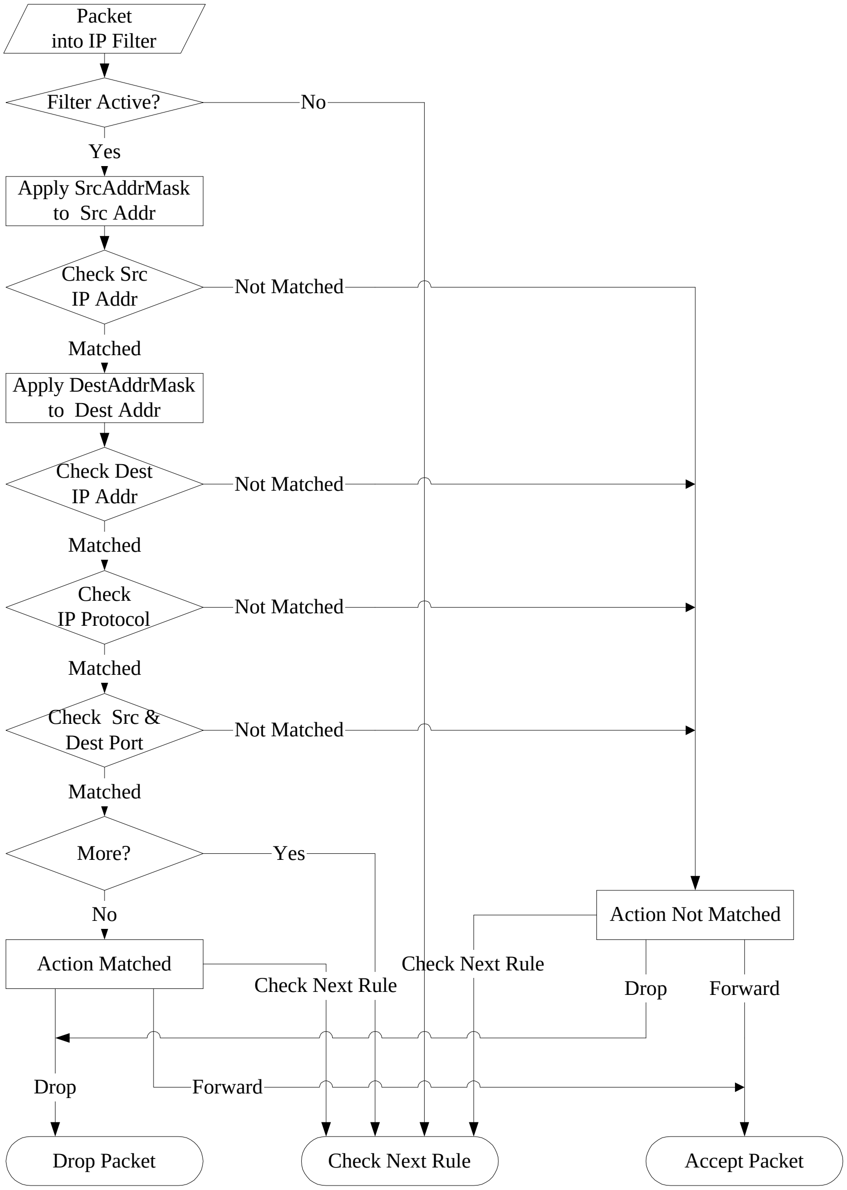


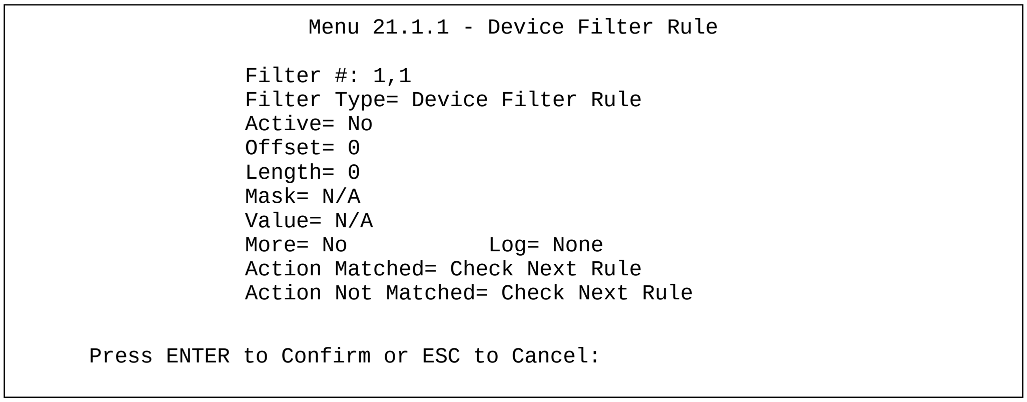
Figure 10-7 Executing an IP Filter

10.5.2 Device Filter Rule

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

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

To configure a device rule, select Device Filter Rule in the Filter Type field and press [ENTER] to open **Menu 21.1.1 - Device Filter Rule**, as shown below.



```
                        Menu 21.1.1 - Device Filter Rule

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


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

Figure 10-8 Menu 21.1.2 - Device Filter Rule

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

Table 10-5 Device Filter Rule Menu Fields

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

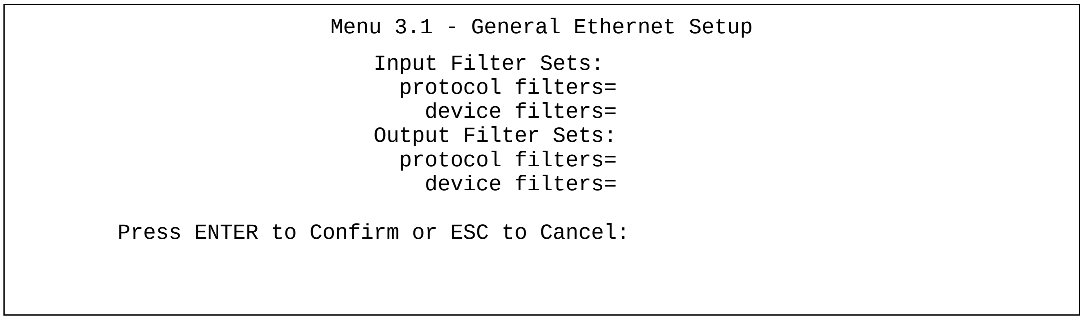
Field	Description	Option
	Both - All packets will be logged.	**Both**
Action Matched	Select the action for a matching packet.	**Check Next Rule** **Forward** **Drop**
Action Not Matched	Select the action for a packet not matching the rule.	**Check Next Rule** **Forward** **Drop**
Once you have completed filling in **Menu 21.1.1 - Device 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**.		

10.6 Applying a Filter

This section shows you where to apply the filter(s) after you design it (them).

10.6.1 Ethernet traffic

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

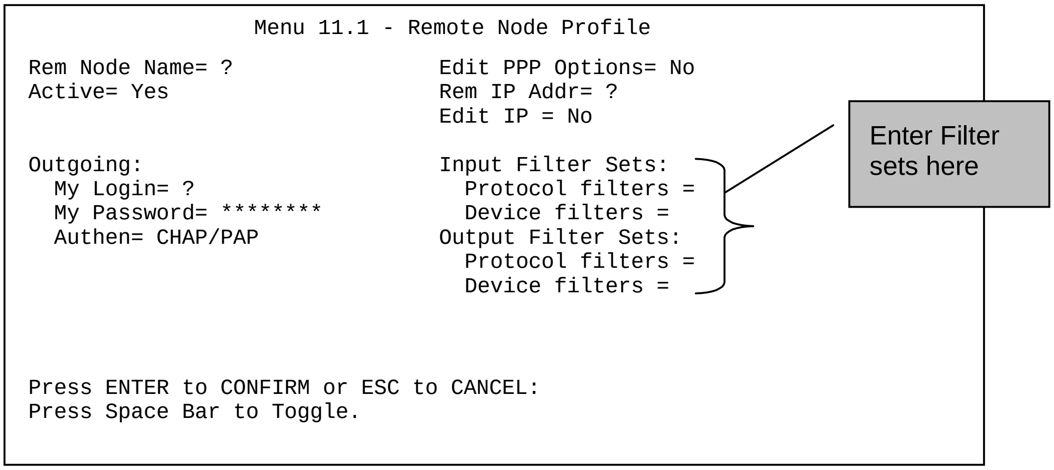


```
                         Menu 3.1 - General Ethernet Setup

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

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

Figure 10-9 Filtering Ethernet Traffic

10.6.2 Remote Node Filters

Go to **Menu 11.1** (shown next) and enter the number(s) of the filter set(s) as appropriate. You can specify up to four filter sets by entering their numbers separated by commas.



```
                  Menu 11.1 - Remote Node Profile

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

Outgoing:                       Input Filter Sets:
  My Login= ?                     Protocol filters =
  My Password= ********           Device filters =
  Authen= CHAP/PAP              Output Filter Sets:
                                  Protocol filters =
                                  Device filters =



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

Enter Filter sets here

Figure 10-10 Filtering Remote Node traffic

10.7 Filter Example

The Prestige 1600 supports the firmware and configuration files upload using FTP connections via LAN and WANs. So, it is possible that anyone can make an FTP connection over the Internet to your Prestige. To prevent outside users from connecting to your Prestige via FTP, you can configure a filter to block FTP connections from the WAN.

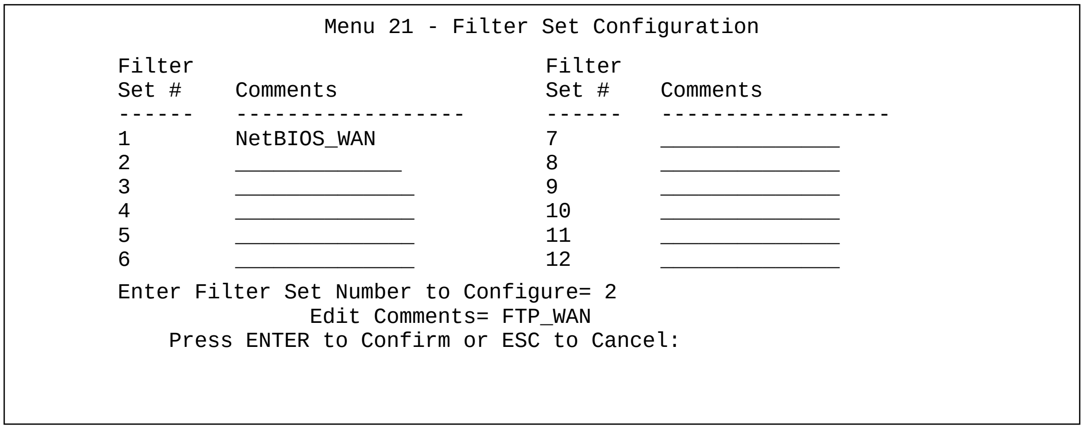
Before configuring a filter, you need to know the following information:

1. The inbound packet type (protocol & port number) - in this case, it is **TCP** (06) protocol with port **20 or 21**.
2. The source IP address - in this case, to block all connections from the outside, the source IP is **0.0.0.0**.

The destination IP address is the Prestige's IP address, but it is unknown when SUA is enabled since most WAN IP addresses are dynamically assigned by the ISP. Therefore, enter **0.0.0.0** as the destination IP in the filter rule. Once **0.0.0.0** is set as the destination IP, no FTP connections can reach 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 in the filter rule. After you apply the FTP filter to the remote node, it only blocks the FTP connection to the Prestige but still permits the FTP connection to the local FTP server.

10.7.1 Configuring a FTP_WAN Filter Rule

Create a filter set in **Menu 21**, e.g., set 2.

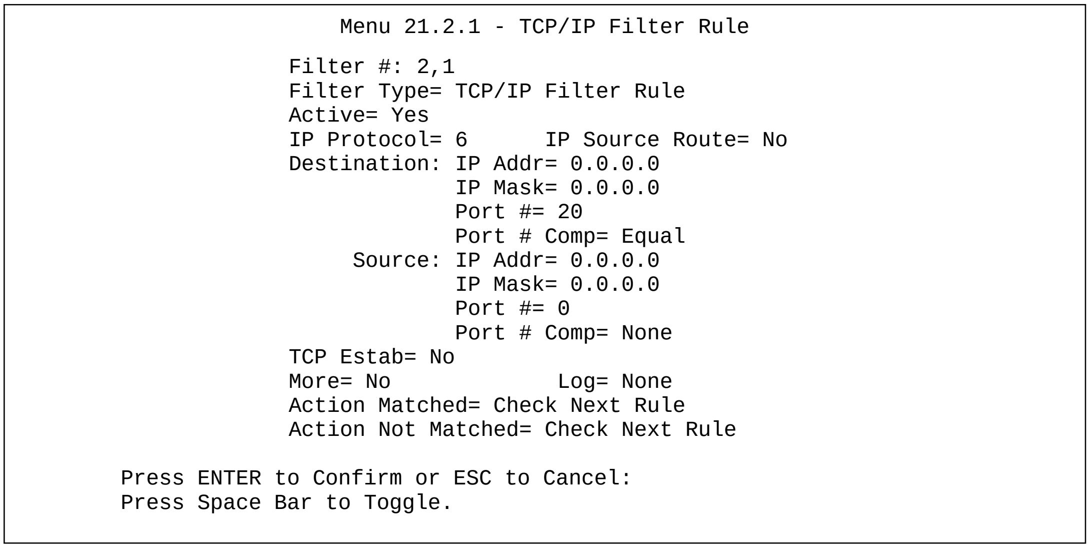


```
                    Menu 21 - Filter Set Configuration

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

         Enter Filter Set Number to Configure= 2
                        Edit Comments= FTP_WAN
             Press ENTER to Confirm or ESC to Cancel:
```

Figure 10-11 FTP_WAN Filter Configuration

Create two filter rules in **Menu 21.2.1** and **Menu 21.2.2**

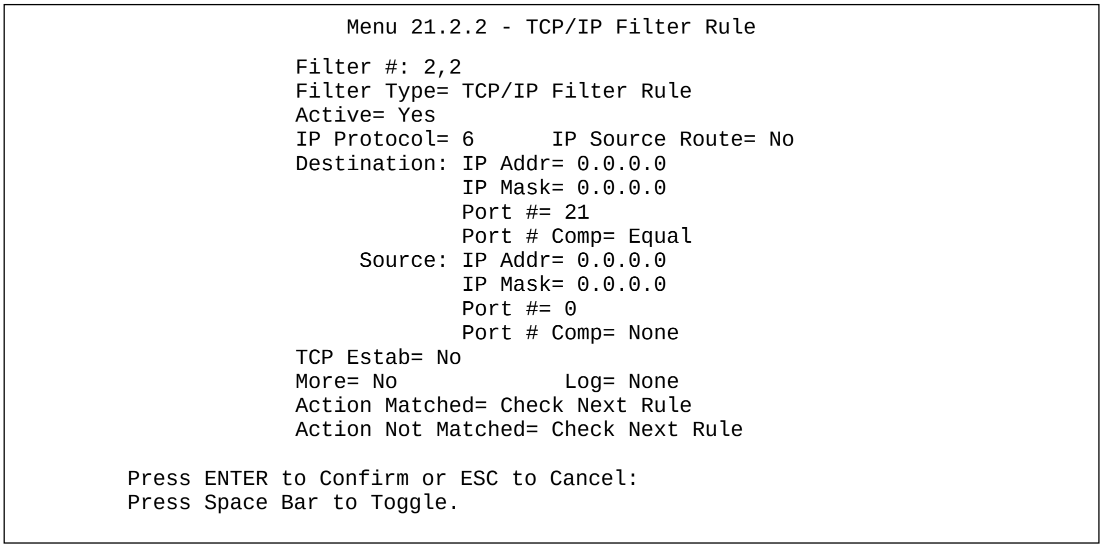
Rule 1**-** block the inbound FTP packet, TCP (06) protocol with port number 20



```
                         Menu 21.2.1 - TCP/IP Filter Rule

                      Filter #: 2,1
                      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 #= 0
                                   Port # Comp= None
                      TCP Estab= No
                      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 10-12 Filter Rule Configuration

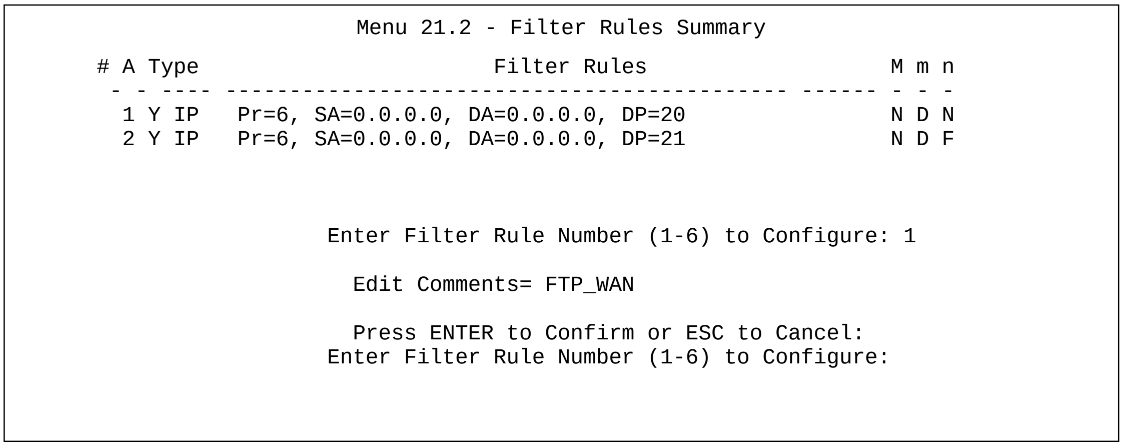
Rule 2- block the inbound FTP packet, TCP (06) protocol with port number 21



```
                 Menu 21.2.2 - TCP/IP Filter Rule

             Filter #: 2,2
             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 #= 0
                          Port # Comp= None
             TCP Estab= No
             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 10-13 Filter Rule Configuration

Check if the filter rules have been correctly configured using the Menu 21.2

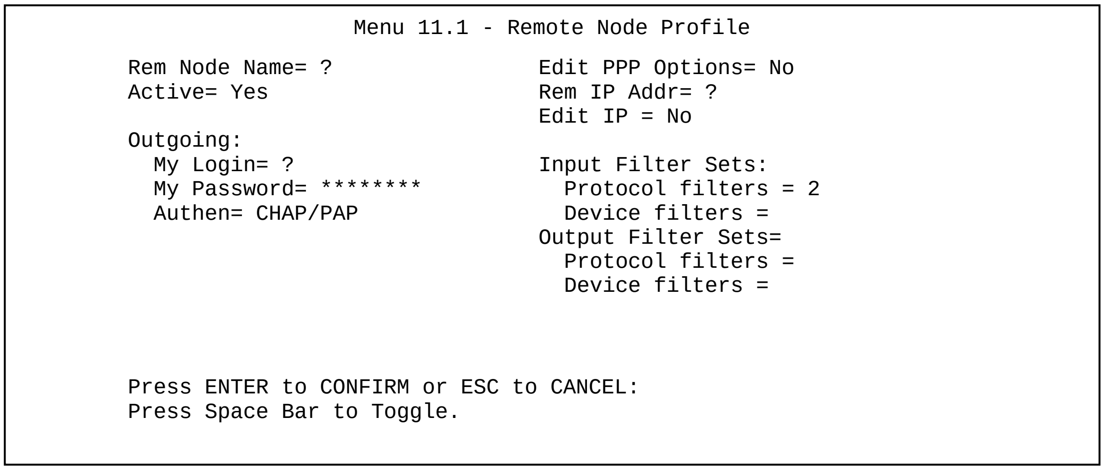


```
                    Menu 21.2 - Filter Rules Summary

# 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



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

                    Edit Comments= FTP_WAN

                    Press ENTER to Confirm or ESC to Cancel:
                  Enter Filter Rule Number (1-6) to Configure:
```

Figure 10-14 FTP_WAN Filter Rules Summary

Note: Please refer to the *Support Notes* for more examples.

Apply the filter set in **Menu 11. 1 - Remote Node Profile.** Put the filter set number **2** to the **Input Protocol Filter Set** for activating the FTP_WAN filter.



```
                          Menu 11.1 - Remote Node Profile

         Rem Node Name= ?                Edit PPP Options= No
         Active= Yes                     Rem IP Addr= ?
                                         Edit IP = No
         Outgoing:
           My Login= ?                   Input Filter Sets:
           My Password= ********           Protocol filters = 2
           Authen= CHAP/PAP                Device filters =
                                         Output Filter Sets=
                                           Protocol filters =
                                           Device filters =




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

Figure 10-15 Remote Node Profile

Chapter 11
SNMP Configuration

This chapter explains how to configure SNMP.

11.1 About SNMP

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of TCP/IP protocol suite. Your Prestige 1600 supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige 1600 through the network. The Prestige 1600 supports SNMP version one (SNMPv1).

Keep in mind that SNMP is only available if TCP/IP is configured on your Prestige 1600.

The next figure illustrates an SNMP management operation.

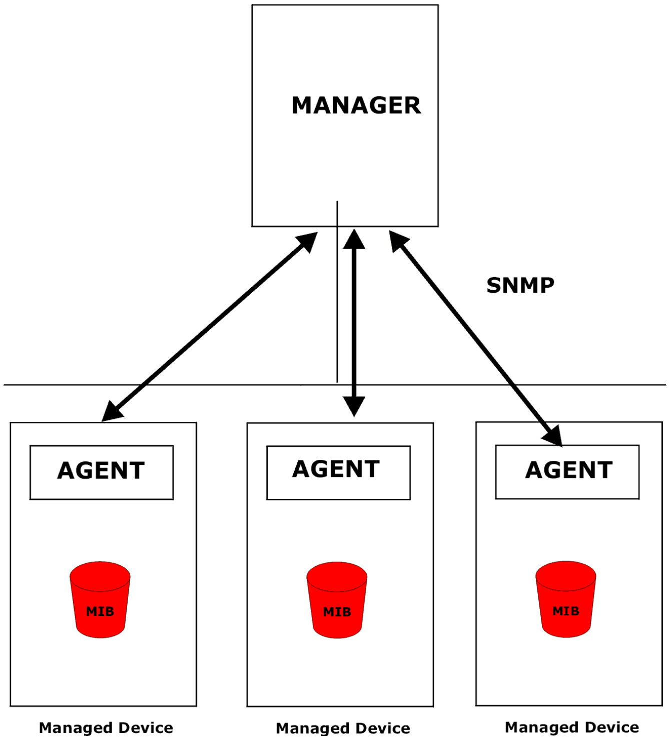


Figure 11-1 SNMP Management Model

An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed device (P1600). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A

Management Information Base (MIB) is a collection of managed objects. SNMP allows manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get

  Allows the manager to retrieve an object variable from the agent.

- GetNext

  Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.

- Set
  Allows the manager to set values for object variables within an agent.

- Trap
  Used by the agent to inform the manager of some events.

11.2 Supported MIBs

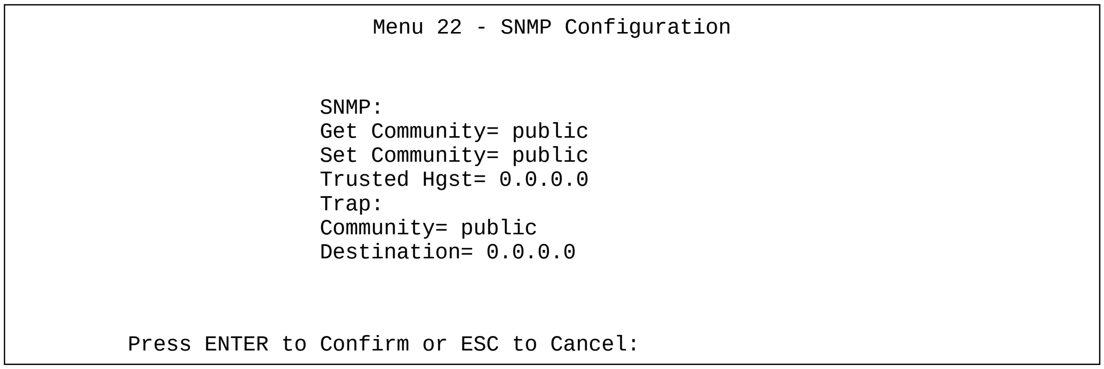
The P1600 supports MIB II that is defined in RFC-1213 and RFC-1215. The P1600 can also respond with specific data from the ZyXEL private MIB (ZYXEL-MIB). The focus of the MIBs is to let administrators collect statistic data and monitor status and performance.

The only implement MIBs in P1600 as a SNMP agent. Users must implement their own GUI on SNMP platform (SNMP manager).

When the user logs in using SMT, the set-request will be ignored for the protection of data.

11.3 SNMP Configuration

To configure SNMP, select option 22 from the Main Menu to open **Menu 22 - SNMP Configuration** as shown next. The “community” for Get, Set and Trap fields is SNMP’s terminology for password.



```
                             Menu 22 - SNMP Configuration



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



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

Figure 11-2 Menu 22 - SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 11-1 SNMP Configuration Menu Fields

Field	Description	Option
Get Community	Enter the Get Community, which is the password for the incoming Get- and GetNext- requests from the management station.	**Public**
Set Community	Enter the set community, which is the password for incoming Set requests from the management station.	**Public**
Trusted Host	If you enter a trusted host, your Prestige 1600 will only respond to SNMP messages from this address. If you leave the field blank (default), your Prestige 1600 will respond to all SNMP messages it receives, regardless of source.	**Blank**
Trap: Community	Enter the trap community, which is the password sent with each trap to the SNMP manager.	**Public**
Trap: Destination	Enter the IP address of the station to send your SNMP traps to.	**Blank**
Once you have completed filling in Menu 22 - SNMP Configuration, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] to cancel.		

11.4 SNMP Traps

P1600 will send traps to the SNMP manager when any one of the following events occurs:

1. coldStart (defined in RFC-1215) :

When the machine coldstarts, a trap will be sent after booting (power on).

2. warmStart (defined in RFC-1215) :

When the machine warmstarts, a trap will be sent after booting (software reboot).

3. linkDown (defined in RFC-1215) :

When any of the links is down, a trap will be sent with the port number. The port number is its interface index under the interface group.

Port 1 : Ethernet LAN

Port 2 : PVC 1

Port 3 : PVC 2

Port 4 : PVC 3

Port 5 : xDSL 1

Port 6 : xDSL 2

…

Port 36 : xDSL 32

Please note that xDSL refers to the type of network module installed, i.e., ADSL, IDSL, SDSL.

4. linkUp (defined in RFC-1215) :

When a link is up, the trap will be sent with the port number . The port number is its interface index under the interface group.

5. authenticationFailure (defined in RFC-1215) :

When receiving any SNMP get or set requirement with wrong community (password), this trap is sent to the manager.

6. whyReboot (defined in ZYXEL-MIB) :

When the system is going to restart (warmstart), a trap will be sent with the reason of restart before rebooting.

a. For intentional reboot :

In some cases (download new files, CI command "sys reboot", …), reboot is done intentionally. When this happens, traps with the message "System reboot by user !" will be sent.

b. For fatal error :

If the system reboots because of some fatal errors, traps with the message of the fatal code will be sent.

Chapter 12
System Security

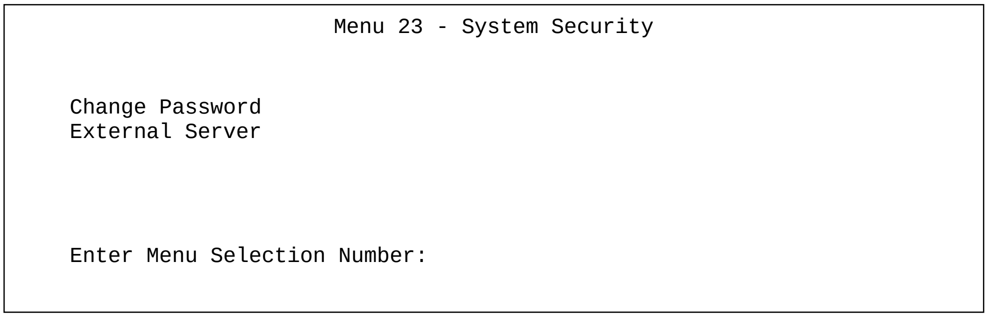
This chapter discusses the system password and RADIUS authentication.

The first step towards ensuring security is changing your system password from the default value to your personal password.

12.1 Changing the System Password

To change the system password, following steps below:

Step 1. Select option **23. System Security** in the Main Menu to open **Menu 23 - System Security** as shown in Figure 12-1.

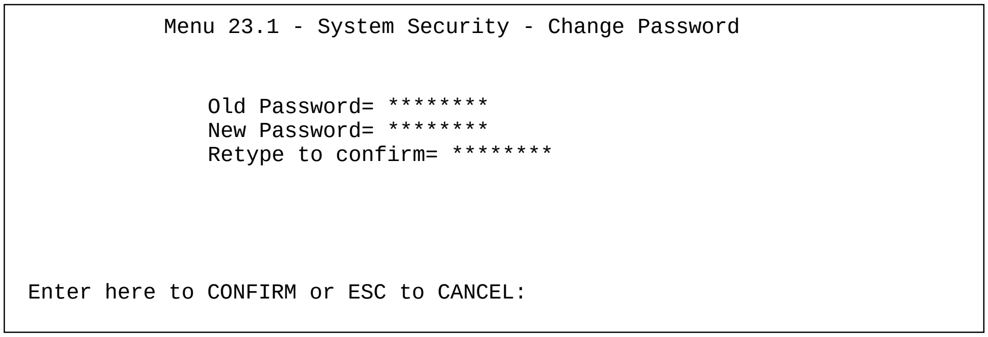


```
                          Menu 23 - System Security



     Change Password
     External Server





     Enter Menu Selection Number:
```

Figure 12-1 Menu 23 - System Security

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

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



```
            Menu 23.1 - System Security - Change Password



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






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

Figure 12-2 Menu 23.1 - System Security - Change Password

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

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

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

12.2 RADIUS Support

This section shows you to configure user authentication and accounting using an external RADIUS server.

12.2.1 About RADIUS

RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share.

12.2.2 Using RADIUS Authentication

12.3 RADIUS Authentication

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

12.3.1 Installing a RADIUS Server

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

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

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

`ftp://ftp.livingston.com/pub/le/radius`/

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

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

```
# Zyxel proprietary attributes
ATTRIBUTE  Zyxel-Callback-Option  192  int0eger
VALUE      Zyxel-Callback-Option  None       0
VALUE      Zyxel-Callback-Option  Optional   1
VALUE      Zyxel-Callback-Option  Mandatory  2

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

The message exchange of RADIUS authentication is shown next.

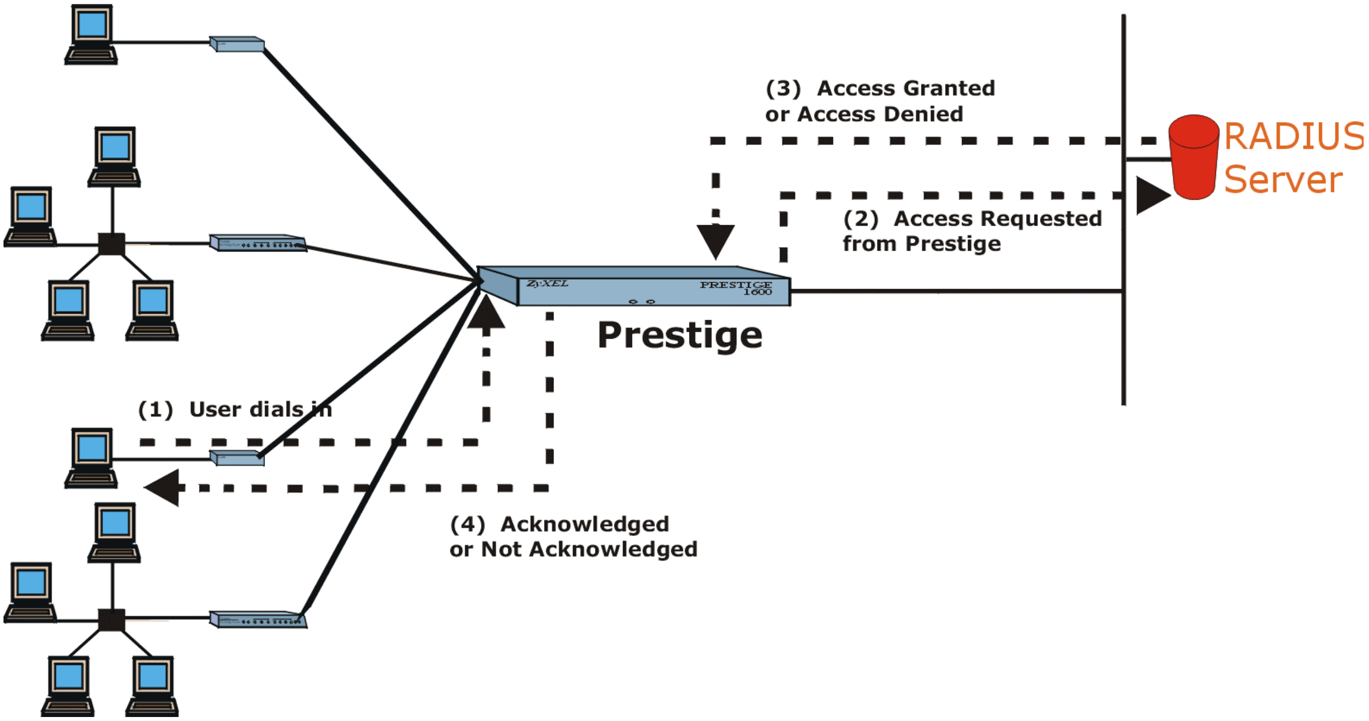


Figure 12-3 RADIUS Authentication Example

12.3.2 The Key Field

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

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

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

12.3.3 Adding Users to the RADIUS Database

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

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

The `users file` contains an entry for each user that RADIUS will authenticate. The user profile contains user name and password that the RADIUS server uses for authentication.

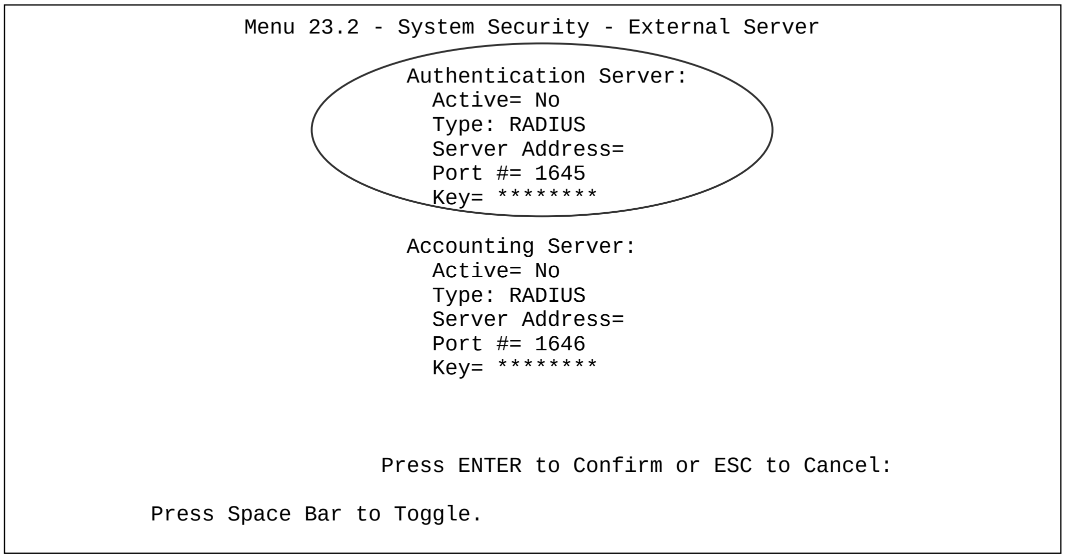
Check Menu 6 to make sure that you do not duplicate user names.

12.3.4 RADIUS Server Configuration

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

The early deployment of RADIUS was done using the chosen port number 1645. Currently, the officially assigned port number for RADIUS is 1812. So, check the port number used by your RADIUS server before configuring it in the Prestige.

You must reboot your Prestige after changing the RADIUS port number for the change to take effect.



```
                     Menu 23.2 - System Security - External Server

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

                                  Accounting Server:
                                    Active= No
                                    Type: RADIUS
                                    Server Address=
                                    Port #= 1646
                                    Key= ********



                                Press ENTER to Confirm or ESC to Cancel:

            Press Space Bar to Toggle.
```

Figure 12-4 Menu 23.2 - System Security - External Server

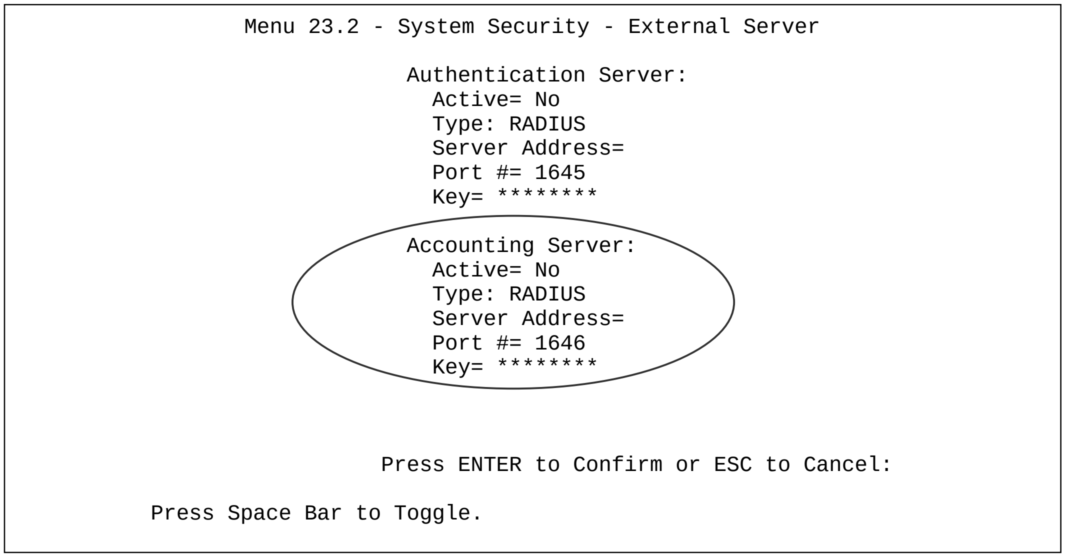
The fields in the System Security - External Server Menu are listed in the following table.

Table 12-1 System Security - Authentication Server Menu Fields

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

12.4 RADIUS Accounting

This facility logs information about dial-in connections. It can be used independently of RADIUS Authentication. It allows data to be sent at the start and the end of sessions, indicating the amount of resources (time, packets, bytes etc.) used during the session. An ISP could use this function for billing needs. The accounting port for RADIUS Accounting is 1646. The RADIUS accounting server may be located on the same host as the RADIUS authentication server, or on a separate host. RADIUS accounting can be configured in **Menu 24.3.2 - System Maintenance - External Server** as shown next.



```
                   Menu 23.2 - System Security - External Server

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

                                Accounting Server:
                                  Active= No
                                  Type: RADIUS
                                  Server Address=
                                  Port #= 1646
                                  Key= ********



                          Press ENTER to Confirm or ESC to Cancel:

           Press Space Bar to Toggle.
```

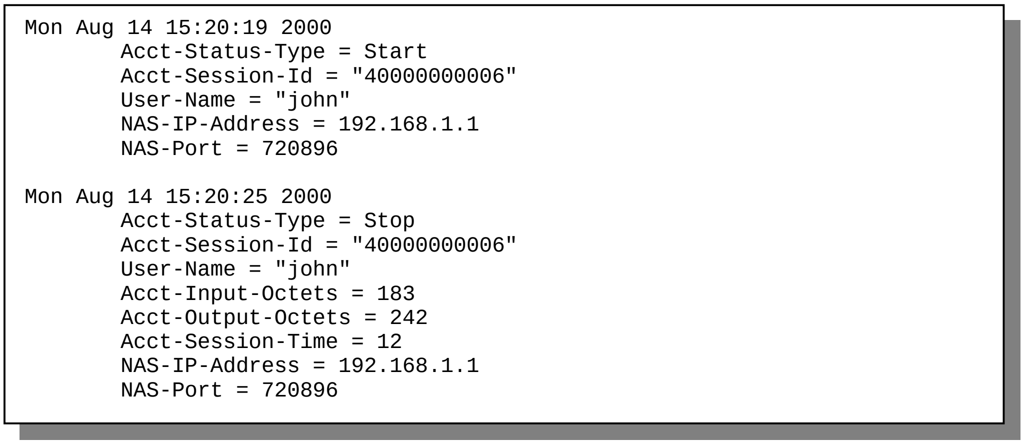
Figure 12-5 Menu 24.3.2 - System Maintenance - Accounting Server

These fields are explained in the following table.

Table 12-2 Menu 24.3.3 System Maintenance - Accounting Server Fields

Field	Description
Active	Determines whether the accounting facility is on or off.
Type	Determines the type of the accounting server. At present only RADIUS is supported.
Server Address	The IP address of the accounting server.
Port #	The port number used by the accounting server. The default is port 1646.
Key	The “password” used to authenticate your Prestige to the RADIUS server. Please note that this is between the Prestige and the server; it has nothing to do with the dial-in users.

Once the accounting server is enabled and a user is authenticated, the Prestige sends messages to the external server. Some examples are shown next.



```
Mon Aug 14 15:20:19 2000
        Acct-Status-Type = Start
        Acct-Session-Id = "40000000006"
        User-Name = "john"
        NAS-IP-Address = 192.168.1.1
        NAS-Port = 720896

Mon Aug 14 15:20:25 2000
        Acct-Status-Type = Stop
        Acct-Session-Id = "40000000006"
        User-Name = "john"
        Acct-Input-Octets = 183
        Acct-Output-Octets = 242
        Acct-Session-Time = 12
        NAS-IP-Address = 192.168.1.1
        NAS-Port = 720896
```

Figure 12-6 Examples of RADIUS Accounting Message

The following table describes the accounting attributes mentioned in the above example.

Accounting attributes may vary depending on the external server.

Table 12-3 Accounting Attributes

Field	Description
Acct-Status-Type	Account Status Type has four values: Accounting On, Accounting Off, Start and Stop. An Accounting On message is sent when the Prestige starts the RADIUS Accounting service. An Accounting Off message is sent when the Prestige ends the service. A Start message is sent when a user session begins. A Stop message is sent when the session ends.
Acct-Session-Id	Account Session Id is a unique number assigned to each session to make it easy to match the Start and Stop records in a detail file, and to eliminate duplicate records. Note that in the above example this value matches in the Start and Stop record, indicating that these records correspond to the same session.
User-Name	Specifies the user name.
NAS-Port	Refers to the Network Access Server (NAS), i.e., the Prestige, port used in the connection.
NAS-Port-DNIS	Refers to the called party’s directory number.
Caller Id	Refers to the dial-in user’s directory number.
Acct-Input-Octets	This is the number of inbound bytes.
Acct-Output-Octets	This is the number of outbound bytes.
Acct-Session-Time	This is the length of the session in seconds.

Chapter 13
Remote Management

This chapter discusses Telnet and remote management of the Prestige using NAT.

13.1 About Telnet

Before the Prestige 1600 is properly setup for TCP/IP, the only option for configuring it is through the console port. Once your Prestige 1600 is configured, you can use telnet to configure it remotely. You can also use a modem for remote configuration as shown in chapter One.

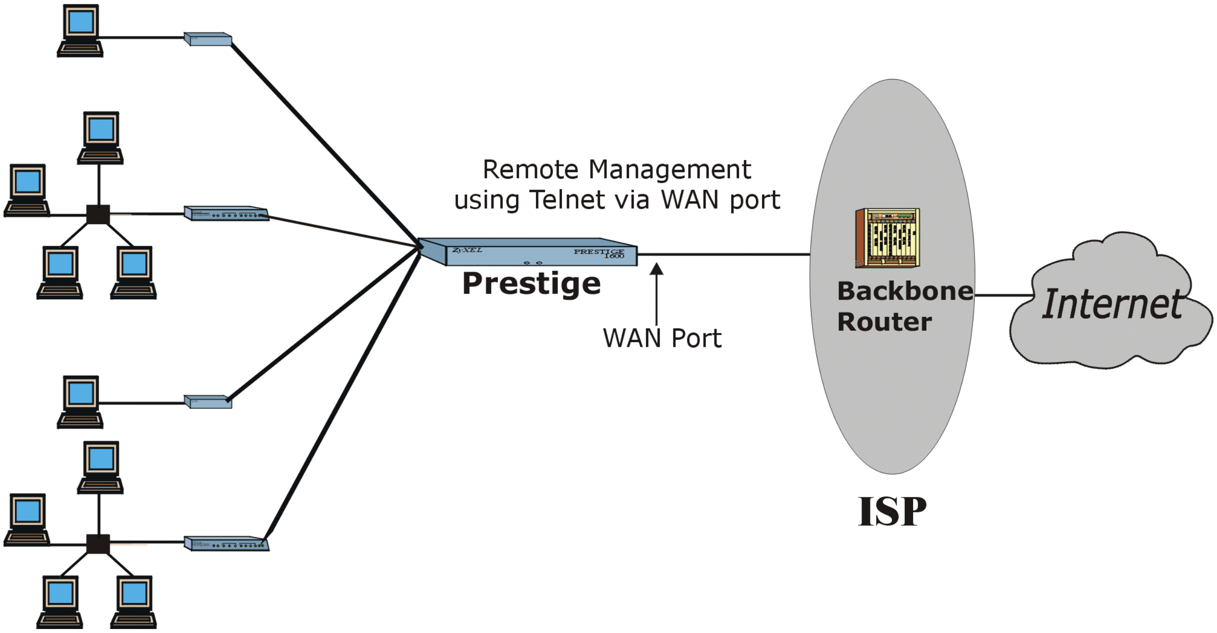


Figure 13-1 Remote Management Using Telnet

To manage the Prestige primary, telnet directly to the primary, using your computer's telnet client. For example on a PC, type:

telnet <primary machine WAN IP address> (where "primary machine WAN IP address" is a real IP address.)

13.2 Telnet Behind NAT

To manage Prestige secondaries, telnet to the Primary first and then use the embedded Prestige telnet client to telnet to the secondary. Go to SMT **Menu 24.8 Command Interpreter Mode** and type:

ip telnet <secondary machine IP address> (where "secondary machine IP address" may be a private IP address.)

A later section in this chapter shows you how to configure NAT on the Prestige for this scenario.

Note: Only one connection can be active at any given time. The console port connection has precedence. Remote users cannot telnet in when the local administration is logged in.

13.3 Telnet Capabilities

13.3.1 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.

13.3.2 System Timeout

There is a system timeout of 5 minutes (300 seconds) for either the console port or telnet. Your Prestige 1600 will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in Menu 24.1.1, 24.1.2 and 24.1.3.

13.4 Remote Management Through NAT

The powerful NAT features allow you to manage Prestige secondaries via Telnet even when using private IPs. Suppose the network is as shown in the following diagram.

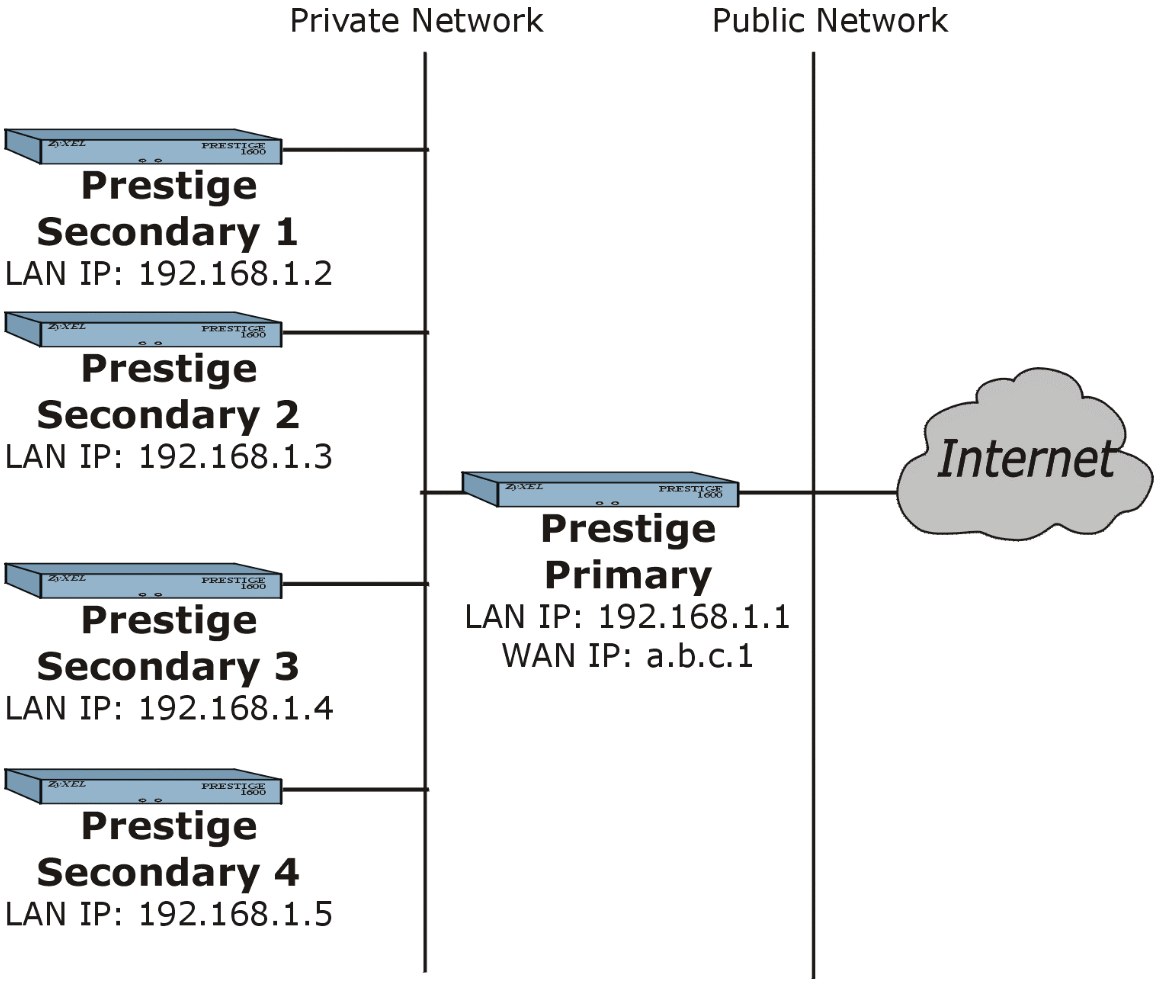


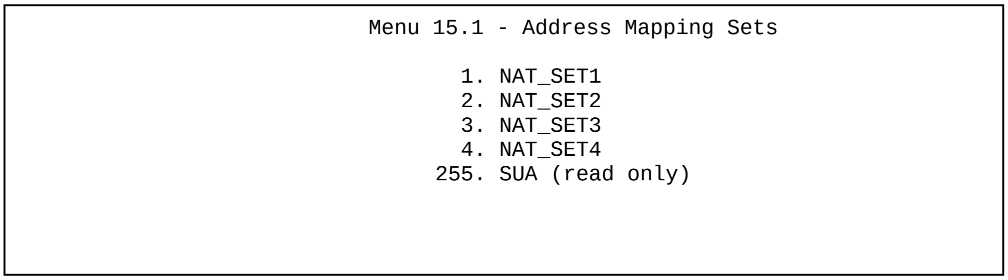
Figure 13-2 Remote Management Via NAT

The ISP assigns an IP address of a.b.c.1 to the Prestige primary and IP addresses of a.b.c.2 to a.b.c.5 to the Prestige secondary units. The private IP addresses for the primary and secondaries are 192.168.1.1 to 192.168.1.5 inclusive. We wish to map public IP addresses a.b.c.2 to a.b.c.5 to the secondary units.

Please note that "a.b.c.digit" represents a real, public IP address and that alphabetical characters cannot be accepted as parts of an IP address.

13.4.1 Procedure to Set Up NAT for Remote Management

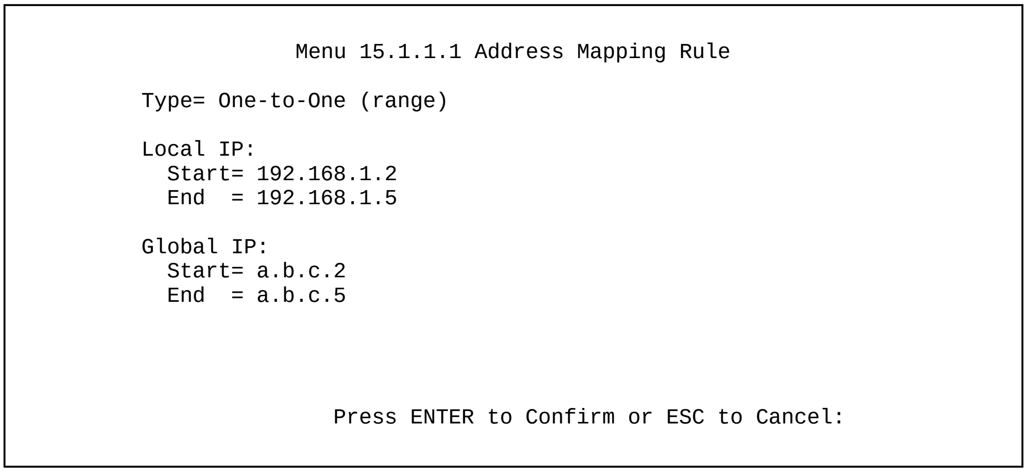
Step 1. Pick an available NAT set from Menu 15.1. Let's say set 1 is available.



```
                  Menu 15.1 - Address Mapping Sets

                          1. NAT_SET1
                          2. NAT_SET2
                          3. NAT_SET3
                          4. NAT_SET4
                        255. SUA (read only)
```

Figure 13-3 Pick An Address Mapping Set

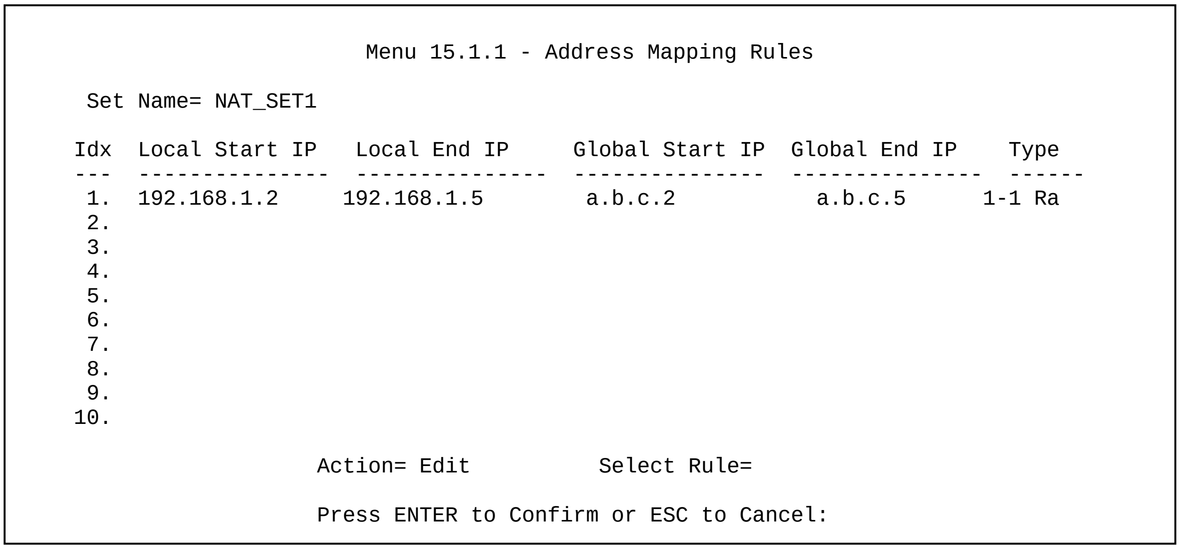
Step 2. Go to Menu 15.1.1.1 (*see the NAT chapter* for details on this) and configure the screen as shown.



```
                  Menu 15.1.1.1 Address Mapping Rule

          Type= One-to-One (range)

          Local IP:
            Start= 192.168.1.2
            End  = 192.168.1.5

          Global IP:
            Start= a.b.c.2
            End  = a.b.c.5




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

Figure 13-4 Address Mapping Rule

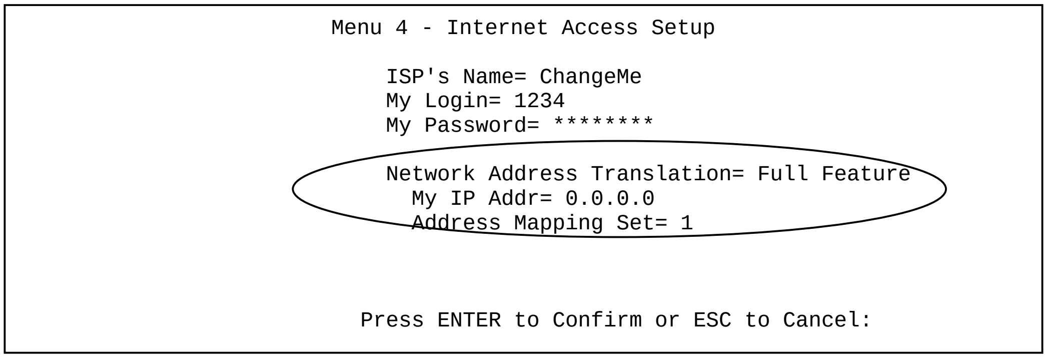
Step 3. After you configure this screen, press [ENTER] to go back to this screen.



```
                       Menu 15.1.1 - Address Mapping Rules

     Set Name= NAT_SET1

    Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
    ---  ---------------  ---------------  ---------------  ---------------  ------
     1.  192.168.1.2     192.168.1.5        a.b.c.2           a.b.c.5      1-1 Ra
     2.
     3.
     4.
     5.
     6.
     7.
     8.
     9.
    10.

                     Action= Edit          Select Rule=

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

Figure 13-5 Address Mapping Rule Summary

Step 4. Save the rule back to the Prestige, then go to Menu 4 to apply this newly configured set.



```
                        Menu 4 - Internet Access Setup

                            ISP's Name= ChangeMe
                            My Login= 1234
                            My Password= ********

                            Network Address Translation= Full Feature
                              My IP Addr= 0.0.0.0
                              Address Mapping Set= 1



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

Figure 13-6 Apply the New NAT Set

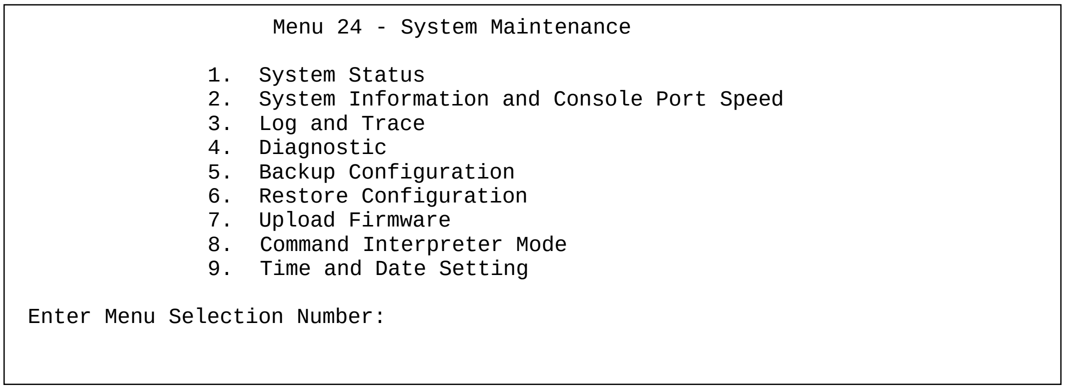
Step 5. You can now test the rule by using “telnet a.b.c.2” on a computer to connect to the Secondary 1 unit.

Chapter 14
System Information and Maintenance

This chapter provides information about the diagnostic tools that help you maintain your Prestige.

The diagnostic tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail. Information about upgrades is provided in the *Configuration & Firmware Maintenance* chapter.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown below.



```
                    Menu 24 - System Maintenance

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

Enter Menu Selection Number:
```

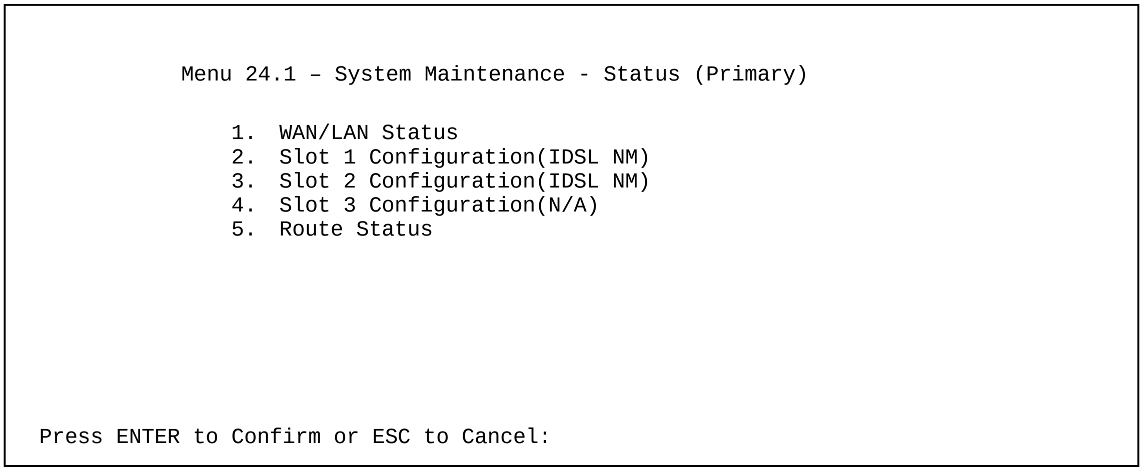
Figure 14-1 Menu 24 - System Maintenance

14.1 System Status

The first selection, System Status, gives you 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 the WAN port and the network module status, number of packets sent and number of packets received.

To get to the System Status, select number **24** to go to **Menu 24 - System Maintenance.** From this menu, select number **1, System Status.**

Depending on the **System Type** configuration in the **Menu 1 - General Setup,** you can see the respective system type status in **Menu 24.1 - System Maintenance - Status**. For example, if you chose **Primary Configuration Type** with 2 IDSL network modules installed in slots 1 and 2, you will see the following figure. It should be noted that these fields are READ-ONLY and are meant to be used for diagnostic purposes.

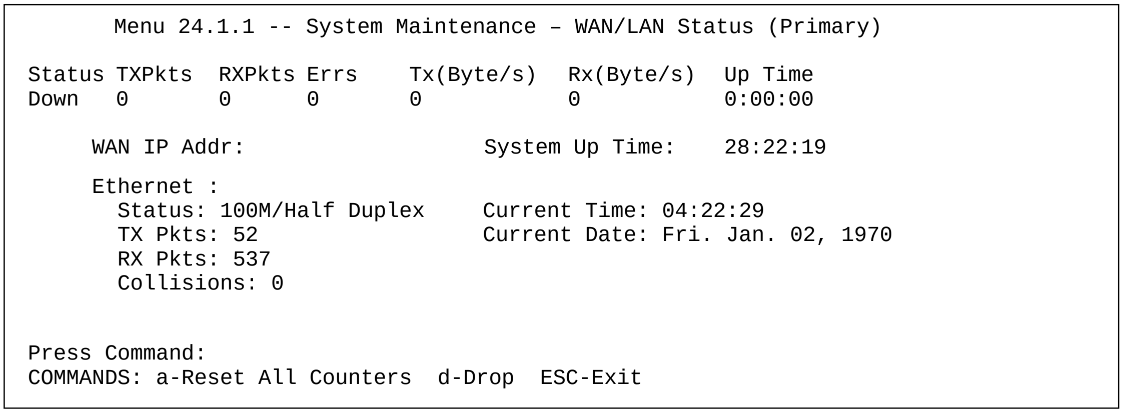


```
              Menu 24.1 – System Maintenance - Status (Primary)

                  1.  WAN/LAN Status
                  2.  Slot 1 Configuration(IDSL NM)
                  3.  Slot 2 Configuration(IDSL NM)
                  4.  Slot 3 Configuration(N/A)
                  5.  Route Status







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

Figure 14-2 Menu 24.1 - System Maintenance - Status

14.1.1 WAN/LAN Status

Type “1” in **Menu 24.1** to enter **Menu 24.1.1** for detailed WAN/LAN Status.



```
       Menu 24.1.1 -- System Maintenance – WAN/LAN Status (Primary)

Status TXPkts  RXPkts Errs    Tx(Byte/s)  Rx(Byte/s)  Up Time
Down   0       0      0       0           0           0:00:00

     WAN IP Addr:                  System Up Time:    28:22:19

     Ethernet :
       Status: 100M/Half Duplex     Current Time: 04:22:29
       TX Pkts: 52                  Current Date: Fri. Jan. 02, 1970
       RX Pkts: 537
       Collisions: 0


Press Command:
COMMANDS: a-Reset All Counters  d-Drop  ESC-Exit
```

Figure 14-3 Menu 24.1.1 - WAN/LAN Status

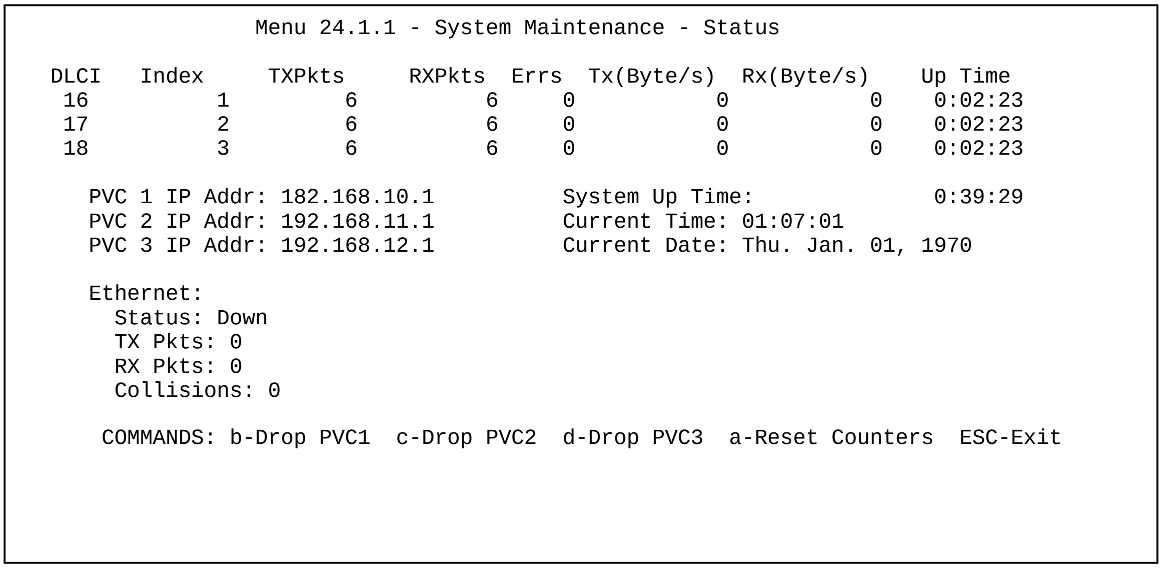
The following table describes the fields present in **Menu 24.1.1 - System Maintenance - WAN/LAN Status**.

Table 14-1 System Maintenance - Status Menu Fields

Field	Description
Status	The status of the WAN port.
TXPkts	The number of transmitted packets on this port.
RXPkts	The number of received packets on this port.
Err(or)s	The number of error packets on this port.
Tx (Byte / s)	The number of bytes transmitted in the last second.
Rx (Byte / s)	The number of bytes received in the last second.
Up Time	Elapsed time this port has been up.
WAN IP Addr	Shows the IP address of the WAN port.

Field	Description
System Up Time	Displays the total elapsed time your system has been running.
Current Time	Displays the current time according to how you have the time set in Menu 24.9 - System Maintenance - Time and Date Setting.
Current Date	Displays the current date according to how you have the date set in Menu 24.9 - System Maintenance - Time and Date Setting.
Ethernet	
Status	Shows the current speed and duplex mode of the LAN.
TX Pkts	The number of transmitted packets to LAN.
RX Pkts	The number of received packets from LAN.
Collisions	Number of collisions on the Ethernet.

You see the next 24.1.1 screen when you have Frame Relay configured. DLCI, Port and the WAN IP address are shown for each PVC configured.



```
                Menu 24.1.1 - System Maintenance - Status

DLCI   Index     TXPkts     RXPkts  Errs  Tx(Byte/s)  Rx(Byte/s)    Up Time
 16          1         6          6     0           0           0    0:02:23
 17          2         6          6     0           0           0    0:02:23
 18          3         6          6     0           0           0    0:02:23

   PVC 1 IP Addr: 182.168.10.1          System Up Time:              0:39:29
   PVC 2 IP Addr: 192.168.11.1          Current Time: 01:07:01
   PVC 3 IP Addr: 192.168.12.1          Current Date: Thu. Jan. 01, 1970

   Ethernet:
     Status: Down
     TX Pkts: 0
     RX Pkts: 0
     Collisions: 0

    COMMANDS: b-Drop PVC1  c-Drop PVC2  d-Drop PVC3  a-Reset Counters  ESC-Exit
```

Figure 14-4 Menu 24.1.1 With Frame Relay Configured

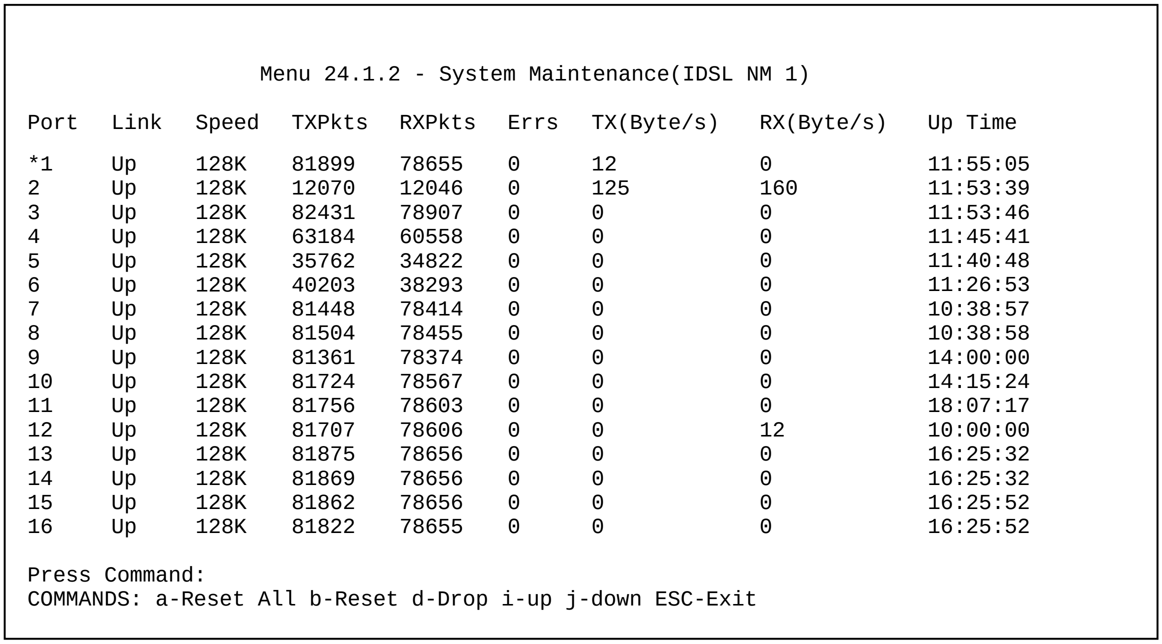
Table 14-2 Menu 24.1.1 With Frame Relay Configured

Field	Description
DLCI	This field shows you the DLCI (data link connection identifier) for the virtual circuit. The DLCI changes for each hop through the network it is not the address of the destination. It is a logical identifier with local significance.
Index	This is the virtual circuit index number.
PVC 1, 2, 3 IP Addr	This displays the IP address of the respective virtual circuit.

14.1.2 DSL Port Status

Enter 2 from **Menu 24.1** to go to **Menu 24.1.2** for detailed status information on the network module installed in slot 1. **Menus 24.1.3** and **24.1.4** offer identical information on the network modules installed in slots 2 and 3. You see a “Slot 3 is empty, please make another selection” message if a slot (3 in this case) is empty. Note the asterisk

(*) indicates the port you can reset (press "b") or drop (press "d") the counters. Press "i" to move the asterisk to the preceding port and "j" to the next port. Press "a" to reset all ports. Press [ESC] to exit this menu.



```
                  Menu 24.1.2 - System Maintenance(IDSL NM 1)

Port   Link   Speed   TXPkts   RXPkts   Errs   TX(Byte/s)   RX(Byte/s)   Up Time

*1     Up     128K    81899    78655    0      12           0            11:55:05
2      Up     128K    12070    12046    0      125          160          11:53:39
3      Up     128K    82431    78907    0      0            0            11:53:46
4      Up     128K    63184    60558    0      0            0            11:45:41
5      Up     128K    35762    34822    0      0            0            11:40:48
6      Up     128K    40203    38293    0      0            0            11:26:53
7      Up     128K    81448    78414    0      0            0            10:38:57
8      Up     128K    81504    78455    0      0            0            10:38:58
9      Up     128K    81361    78374    0      0            0            14:00:00
10     Up     128K    81724    78567    0      0            0            14:15:24
11     Up     128K    81756    78603    0      0            0            18:07:17
12     Up     128K    81707    78606    0      0            12           10:00:00
13     Up     128K    81875    78656    0      0            0            16:25:32
14     Up     128K    81869    78656    0      0            0            16:25:32
15     Up     128K    81862    78656    0      0            0            16:25:52
16     Up     128K    81822    78655    0      0            0            16:25:52

Press Command:
COMMANDS: a-Reset All b-Reset d-Drop i-up j-down ESC-Exit
```

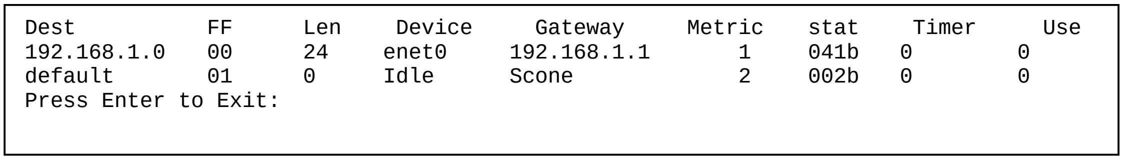
Figure 14-5 Menu 24.1.2 - NM-1 Status

Table 14-3 NM Status Fields

Field	Description
Port	The DSL Port number.
TXPkts	The number of transmitted packets on this port.
RXPkts	The number of received packets on this port.
Err(or)s	The number of error packets on this port.
Tx (Byte / s)	The number of bytes transmitted in the last second.
Rx (Byte / s)	The number of bytes received in the last second.
Up Time	Elapsed time this port has been up.

14.1.3 Route Status

Enter 3 in menu 24.1 to bring up the following screen showing detailed information on the status of the router.



```
Dest           FF      Len    Device     Gateway     Metric    stat    Timer     Use
192.168.1.0    00      24    enet0     192.168.1.1       1     041b   0        0
default        01      0     Idle      Scone             2     002b   0        0
Press Enter to Exit:
```

Figure 14-6 Menu 24.1.5 - Router Status

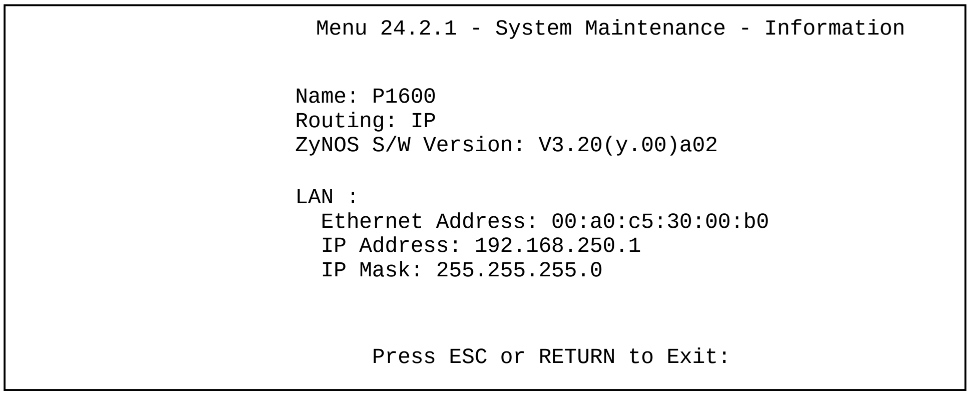
Field	Description
Dest	This is the destination IP address.
FF	This is for ZyXEL internal debugging.

Len	This is the length of the subnet mask (24 bits = 255.255.255.0)
Device	This is the physical device. Enet0 is Ethernet.
Gateway	This is the gateway IP address or the remote node name.
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks.
Stat	This is the bitmap flags of the route status.
Timer	This is the time left to route expiry. “0” means there is no expiry time, i.e., an infinite timeout.
Use	This shows how many times the route has been used.

14.2 System Information

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

Step 2 From Menu 24, select option 2 then select the first option from Menu 24.2 to view Menu 24.2.1.



```
                     Menu 24.2.1 - System Maintenance - Information


                  Name: P1600
                  Routing: IP
                  ZyNOS S/W Version: V3.20(y.00)a02

                  LAN :
                    Ethernet Address: 00:a0:c5:30:00:b0
                    IP Address: 192.168.250.1
                    IP Mask: 255.255.255.0



                      Press ESC or RETURN to Exit:
```

Figure 14-7 Menu 24. 2.1 - System Maintenance Information

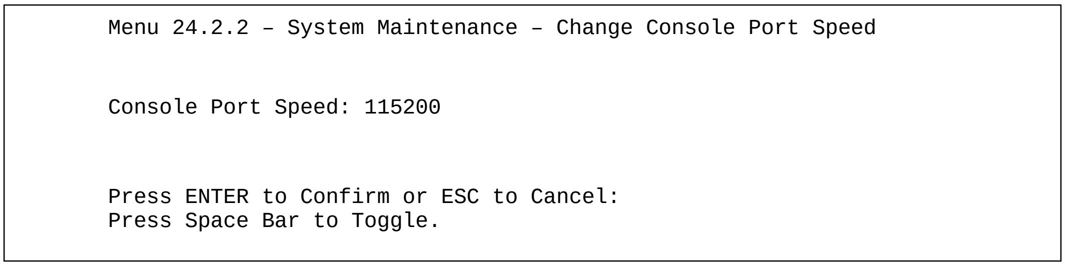
Table 14-4 Fields in System Maintenance

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 enabled.
ZyNOS S/W Version	Refers to the ZyXEL Network Operating System software version.
LAN:	
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.

14.2.1 Console Port Speed

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

Select option 24 from the Main Menu to open **Menu 24 - System Maintenance**. From Menu 24, select option 2 then select the second option from Menu 24.2 to display **Menu 24.2.2 - System Maintenance - Change Console Port Speed.**



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


        Console Port Speed: 115200



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

Figure 14-8 Menu 24.2.2 - System Maintenance - Change Console Port Speed

14.3 Log and Trace

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

14.3.1 Viewing Error Log

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

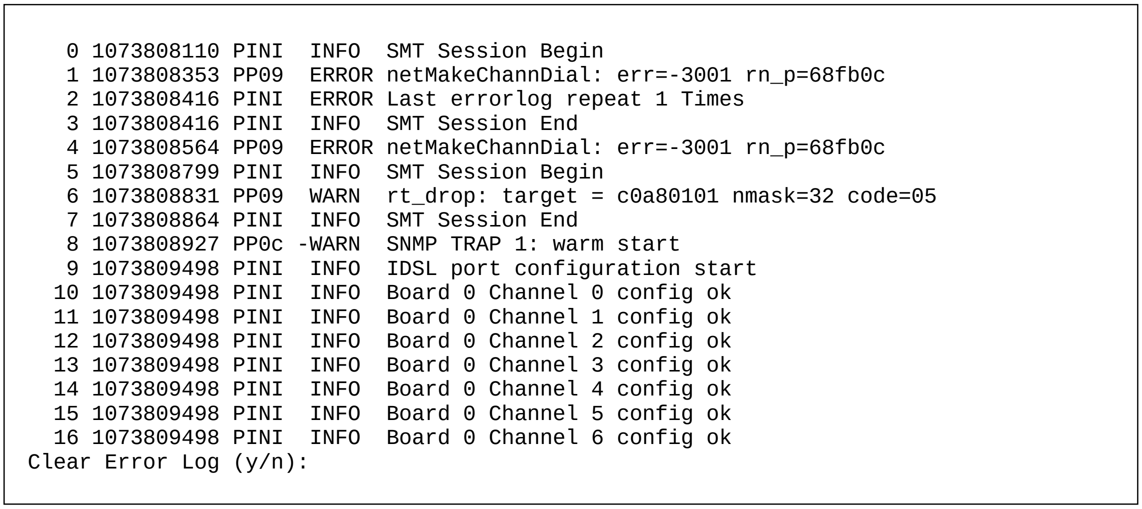
Step 1 Select option 24 from the Main Menu to open **Menu 24 - System Maintenance**.

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

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

Step 4 After the Prestige finishes displaying, you will have the option to clear the error log.

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

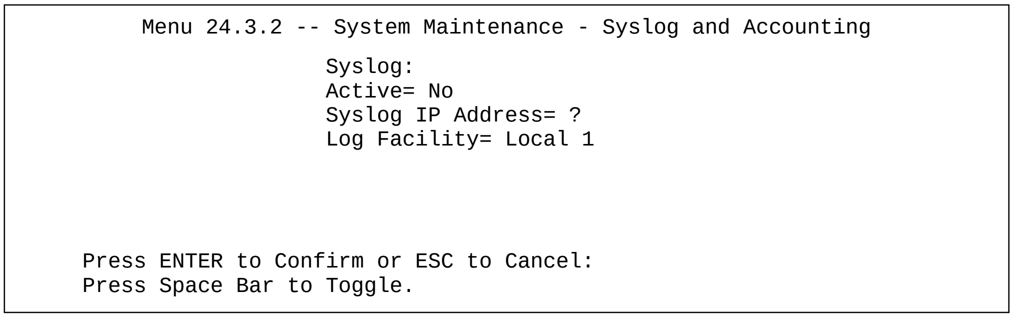


```
  0 1073808110 PINI  INFO  SMT Session Begin
  1 1073808353 PP09  ERROR netMakeChannDial: err=-3001 rn_p=68fb0c
  2 1073808416 PINI  ERROR Last errorlog repeat 1 Times
  3 1073808416 PINI  INFO  SMT Session End
  4 1073808564 PP09  ERROR netMakeChannDial: err=-3001 rn_p=68fb0c
  5 1073808799 PINI  INFO  SMT Session Begin
  6 1073808831 PP09  WARN  rt_drop: target = c0a80101 nmask=32 code=05
  7 1073808864 PINI  INFO  SMT Session End
  8 1073808927 PP0c -WARN  SNMP TRAP 1: warm start
  9 1073809498 PINI  INFO  IDSL port configuration start
 10 1073809498 PINI  INFO  Board 0 Channel 0 config ok
 11 1073809498 PINI  INFO  Board 0 Channel 1 config ok
 12 1073809498 PINI  INFO  Board 0 Channel 2 config ok
 13 1073809498 PINI  INFO  Board 0 Channel 3 config ok
 14 1073809498 PINI  INFO  Board 0 Channel 4 config ok
 15 1073809498 PINI  INFO  Board 0 Channel 5 config ok
 16 1073809498 PINI  INFO  Board 0 Channel 6 config ok
Clear Error Log (y/n):
```

Figure 14-9 Examples of Error and Information Messages

14.3.2 Syslog And Accounting

The Prestige uses the UNIX syslog facility to log 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 - Syslog and Accounting

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




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

Figure 14-10 Syslog and Accounting

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

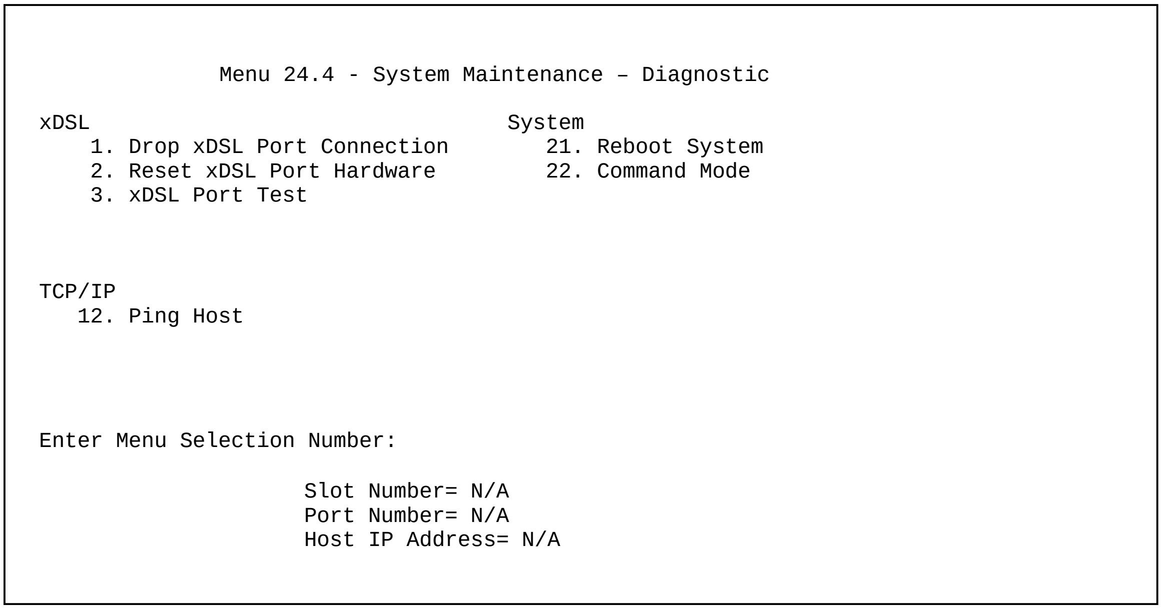
Table 14-5 System Maintenance Menu Syslog Parameters

Parameter	Description
Active	Press [SPACE BAR] to turn on or off syslog.
Syslog IP Address	Enter the IP Address of your syslog server.
Log Facility	Press [SPACE BAR] to toggle between the 7 different Local options. The log facility allows you to log the message in different files in the server. Please refer to your UNIX manual for more detail.

Note: If you want to utilize Syslog on a Windows 95,98 or NT system, you must install a Syslog client.

14.4 Diagnostic

The diagnostic facility allows you to test the different aspects of your Prestige to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown next. “xDSL” refers to the network module type, i.e., ADSL, IDSL or SDSL.



```
              Menu 24.4 - System Maintenance – Diagnostic

xDSL                                 System
    1. Drop xDSL Port Connection        21. Reboot System
    2. Reset xDSL Port Hardware         22. Command Mode
    3. xDSL Port Test



TCP/IP
   12. Ping Host




Enter Menu Selection Number:

                     Slot Number= N/A
                     Port Number= N/A
                     Host IP Address= N/A
```

Figure 14-11 Menu 24.4 - System Maintenance - Diagnostic

Follow this procedure to get to the Diagnostic screen.

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

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

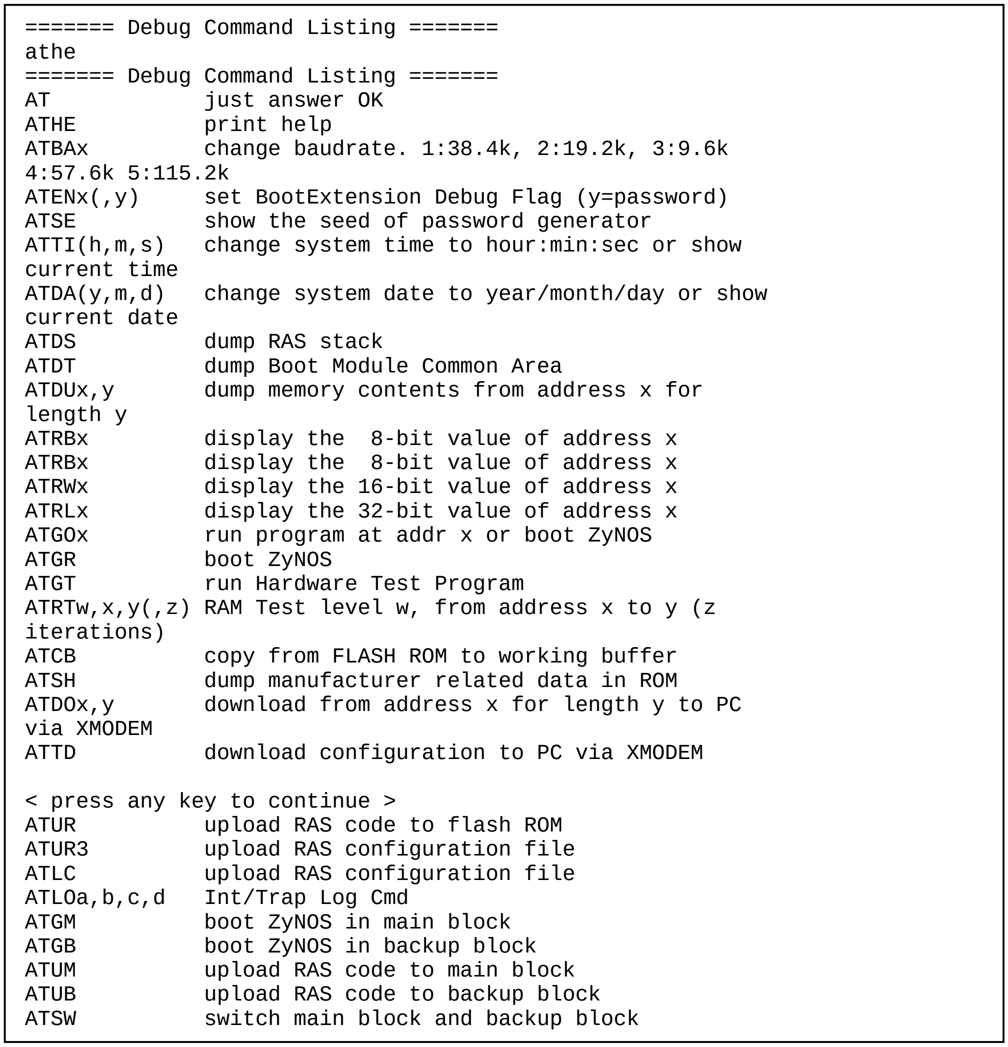
The following table describes the diagnostic tests available in **Menu 24.4** for your Prestige and the connections.

Table 14-6 System Maintenance Menu Diagnostic

Field	Description
Drop xDSL Port Connection	Drops xDSL Port connection.
Reset xDSL Port Hardware	Resets xDSL Port Hardware.
xDSL Port Test	Performs xDSL Port test.
Reboot System	This option reboots the Prestige.
Command Mode	This option allows you to diagnose and test your Prestige using a specified set of commands.
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.
Slot Number	Enter the slot number containing the port you wish to diagnose.
Port Number	Enter xDSL port number.
Host IP Address	Enter the host IP address.

14.5 Boot Module Commands

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



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

< press any key to continue >
ATUR          upload RAS code to flash ROM
ATUR3         upload RAS configuration file
ATLC          upload RAS configuration file
ATLOa,b,c,d   Int/Trap Log Cmd
ATGM          boot ZyNOS in main block
ATGB          boot ZyNOS in backup block
ATUM          upload RAS code to main block
ATUB          upload RAS code to backup block
ATSW          switch main block and backup block
```

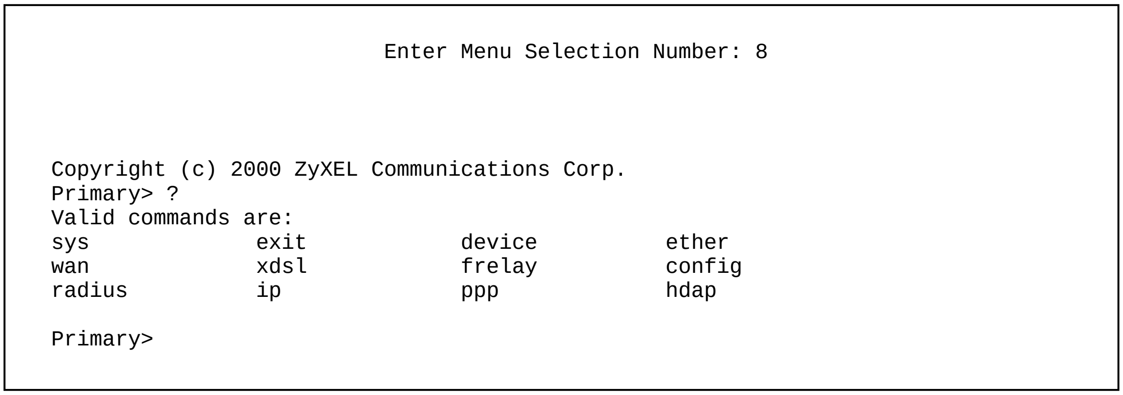
Figure 14-12 Boot Module Commands

14.6 Command Interpreter Mode

This option allows you to enter the command line interpreter mode. A CLI/CI (Command Line Interface) is a user interface to a computer's operating system or an application program in which the user responds to a visual prompt by typing in a command on a specified line, receives a response back from the system, and then enters another command, and so forth.

The list of valid commands can be found by typing **help** or **?** at the command prompt. To exit the CI mode and return to the menu mode, type **exit.**

For more detailed information, refer to the list of CI commands appended at the end of this guide, check the ZyXEL Web site.

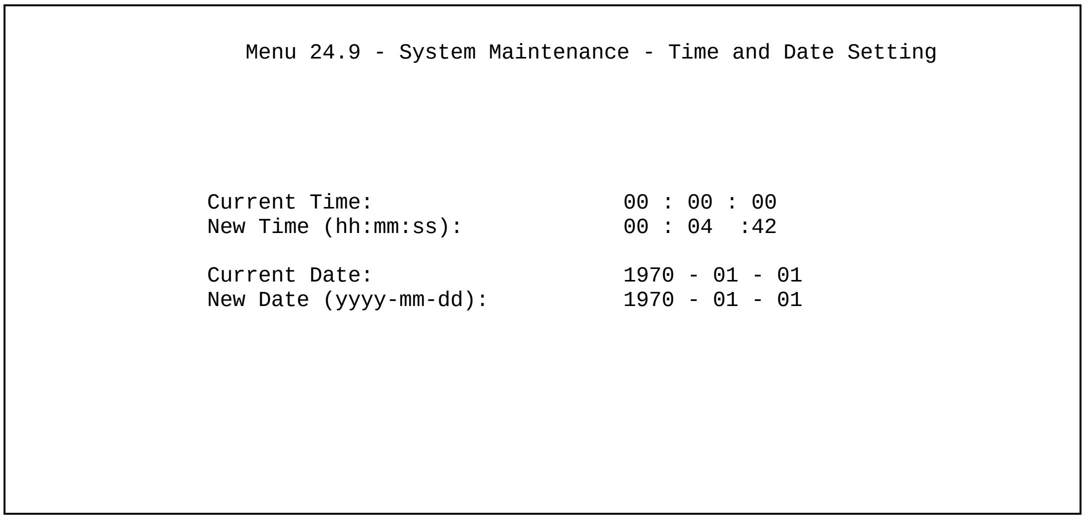


```
                              Enter Menu Selection Number: 8



   Copyright (c) 2000 ZyXEL Communications Corp.
   Primary> ?
   Valid commands are:
   sys             exit            device          ether
   wan             xdsl            frelay          config
   radius          ip              ppp             hdap

   Primary>
```

Figure 14-13 Command Mode

14.7 Time and Date Setting

The Prestige 1600 has a battery powered real time clock. Set the time and date of your Prestige in **Menu 24.9**. Real time is then displayed in the Prestige error logs and firewall logs.



```
                 Menu 24.9 - System Maintenance - Time and Date Setting




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

               Current Date:                     1970 - 01 - 01
               New Date (yyyy-mm-dd):            1970 - 01 - 01
```

Figure 14-14 System Maintenance - Time and Date Setting

Table 14-7 Time and Date Setting Fields

Field	Description
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.
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 15
Configuration & Firmware Maintenance

This chapter describes how to backup and restore your configuration file as well as upload new firmware and a new configuration file.

15.1 Filenames

The configuration file contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup etc. It arrives from ZyXEL with named “prestige.rom” or something similar. Once you have customized the Prestige's setting, they can be saved back to your computer under a filename of your choosing. Choose something meaningful, e.g., “prestige.cfg”. Rename it as “rom-spt” or “rom-0” when transferring files to the Prestige. Renaming is not necessary if you transfer files using the XMODEM protocol.

The ZyNOS firmware file (sometimes referred to as the ras file) is the file that contains the ZyXEL Network Operating System firmware and is usually named the router model name with a “bin” extension, e.g., “prestige.bin”. Rename it as “ras-m” or “ras-b” when uploading to the Prestige main block and backup block respectively using TFTP or FTP. With serial (Xmodem) transfer and many ftp and tftp clients, the filenames on the PC are your choice.

```
ftp> put prestige.bin ras
```

This is a sample ftp session showing the transfer of the "prestige.bin" file on your computer to the Prestige.

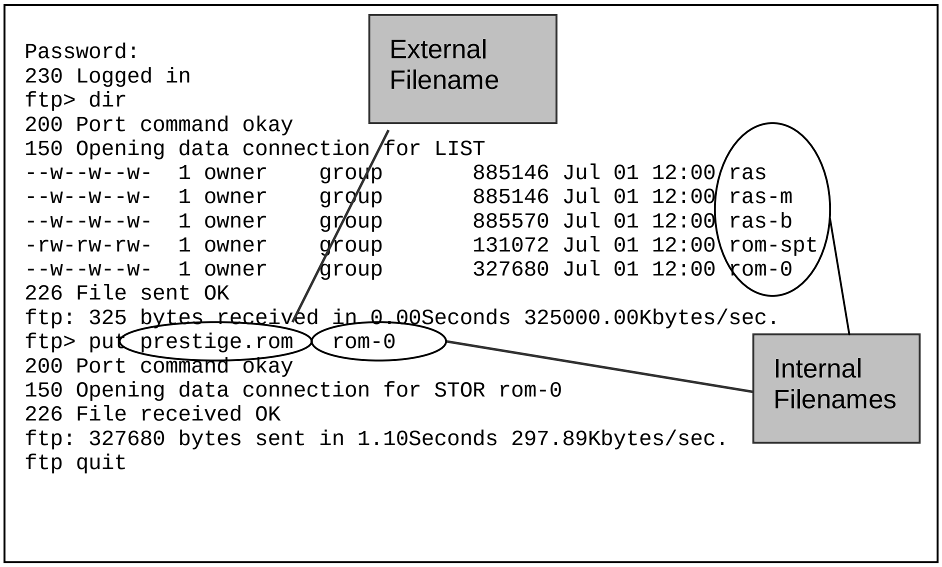
```
ftp> get rom-0 prestige.cfg
```

This is a sample ftp session saving the current configuration to the “prestige.cfg” file on your computer.

If your (t)ftp client does not allow a destination filename different from the source, then you will need to rename them. Be sure you keep unaltered copies of both files for later use.

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.

Always refer to Menu 24.2.1 to verify your current firmware version.



```
Password:
230 Logged in
ftp> dir
200 Port command okay
150 Opening data connection for LIST
--w--w--w-  1 owner    group       885146 Jul 01 12:00 ras
--w--w--w-  1 owner    group       885146 Jul 01 12:00 ras-m
--w--w--w-  1 owner    group       885570 Jul 01 12:00 ras-b
-rw-rw-rw-  1 owner    group       131072 Jul 01 12:00 rom-spt
--w--w--w-  1 owner    group       327680 Jul 01 12:00 rom-0
226 File sent OK
ftp: 325 bytes received in 0.00Seconds 325000.00Kbytes/sec.
ftp> put prestige.rom  rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
ftp: 327680 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp quit
```

Figure 15-1 Internal and External Filenames

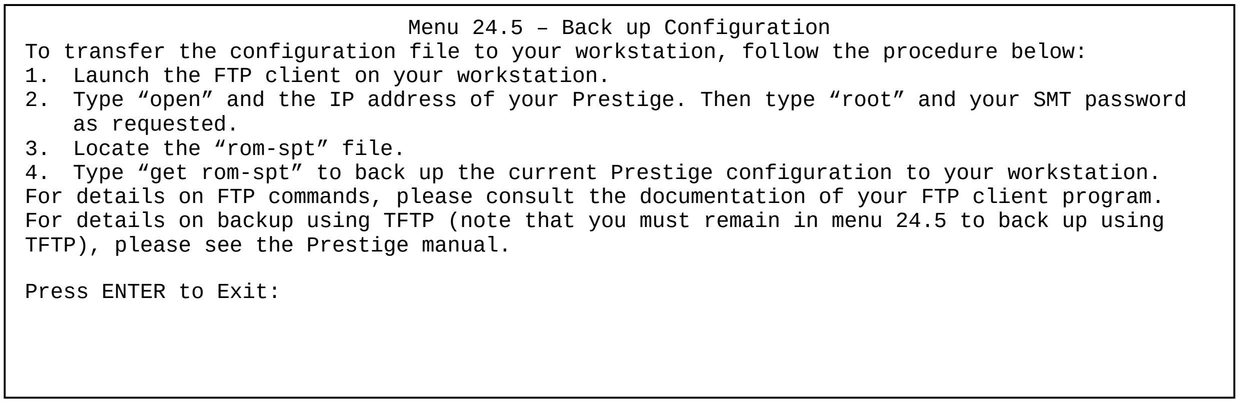
Table 15-1 Filenames

Internal Filename	Description	External Filename	FTP Command Example
rom-spt	The rom-spt file is the user configuration file. It contains your password, Prestige configurations such as IP addresses, Remote Node settings, etc.	*.rom	get rom-spt (backup) put rom-spt (restore)
rom-0	The rom-0 configuration file is the entire factory configuration file. It includes rom-spt, default settings, file system, log, etc. Uploading the rom-0 file replaces the entire ROM file system, including your Prestige configurations, system-related data (speed of the console port and default password etc.), the error log and the trace log.	*.rom	put prestige.rom rom-0 (upload)
ras	This is the firmware filename.	*.bin	
ras-m	This is the router firmware filename on the Prestige 1600 when you transfer a file to the main block.	*.bin	put prestige.bin ras-m (upload)
ras-b	This is the router firmware filename on the Prestige 1600 when you transfer a file to the backup block.	*.bin	put prestige.bin ras-b (upload)

15.2 Backup Configuration

15.2.1 Backup using FTP

To transfer the configuration file using FTP to your workstation, follow the instructions as shown in the following screen. See also the FTP example later in this chapter. For details on FTP commands, please consult the documentation of your FTP client program.



```
                              Menu 24.5 – Back up Configuration
To transfer the configuration file to your workstation, follow the procedure below:
1.  Launch the FTP client on your workstation.
2.  Type “open” and the IP address of your Prestige. Then type “root” and your SMT password
    as requested.
3.  Locate the “rom-spt” file.
4.  Type “get rom-spt” to back up the current Prestige configuration to your workstation.
For details on FTP commands, please consult the documentation of your FTP client program.
For details on backup using TFTP (note that you must remain in menu 24.5 to back up using
TFTP), please see the Prestige manual.

Press ENTER to Exit:
```

Figure 15-2 Menu 24.5 as seen using Telnet

15.2.2 Backup using TFTP

To use TFTP, your workstation must have both telnet and TFTP clients. To transfer 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 checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.

Step 2. Put the SMT in Command Interpreter (CI) mode by entering **8** in **Menu 24 - System Maintenance**.

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

Step 4. Launch the TFTP client on your workstation and connect to the Prestige.

Step 5. Go to SMT menu 24.5. You must remain in this menu until backup is complete.

Step 6. Use the TFTP client to transfer files between the Prestige and the workstation. The file name for the configuration file is “rom-spt”.

The telnet connection must be active before and during TFTP transfer.

For UNIX, use “binary” to set binary transfer mode before using “get” to transfer from the Prestige to the computer. For details on TFTP commands, please consult the documentation of your TFTP client program.

15.2.3 Backup using the Console Port

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

You can perform the backup either through FTP or TFTP (preferred methods as they are faster) or through the RS-232 console port (if the network is down). For backup via the console port any serial communications program should work fine; however, you must use the XMODEM protocol to perform the download/upload.

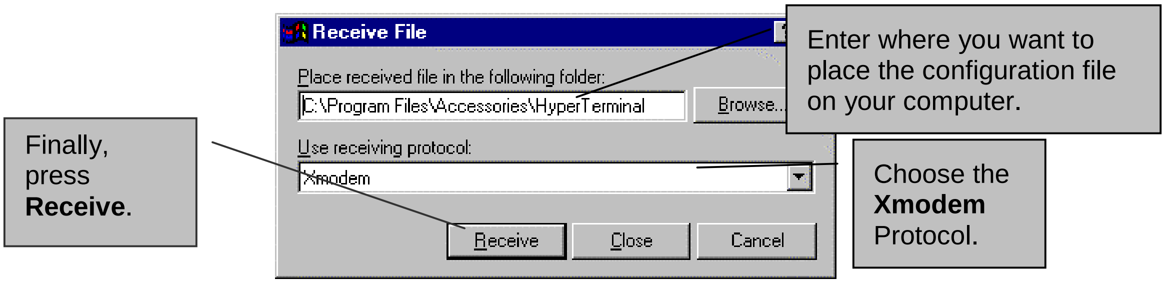
```
                         Menu 24.5 – Backup Configuration
FTP or TFTP are the preferred methods for backing up the current Prestige
configuration to your workstation since FTP or TFTP is faster.
Ready to back up Configuration via Xmodem.

Do you want to continue (Y/N):
```

Figure 15-3 Menu 24.5 - Menu 24.5 as seen using the Console Port

Step 1. Go to menu 24.5.

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

Step 3. Click **Transfer** in the HyperTerminal menu bar, then **Receive File** from the drop-down menu to display the following screen. Follow the instructions as shown in the next screen.



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

Use receiving protocol: Xmodem

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

Finally, press **Receive**.

Choose the **Xmodem** Protocol.

Figure 15-4 Backup Example Using HyperTerminal

Step 4. After a successful backup, you will see the following screen.

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

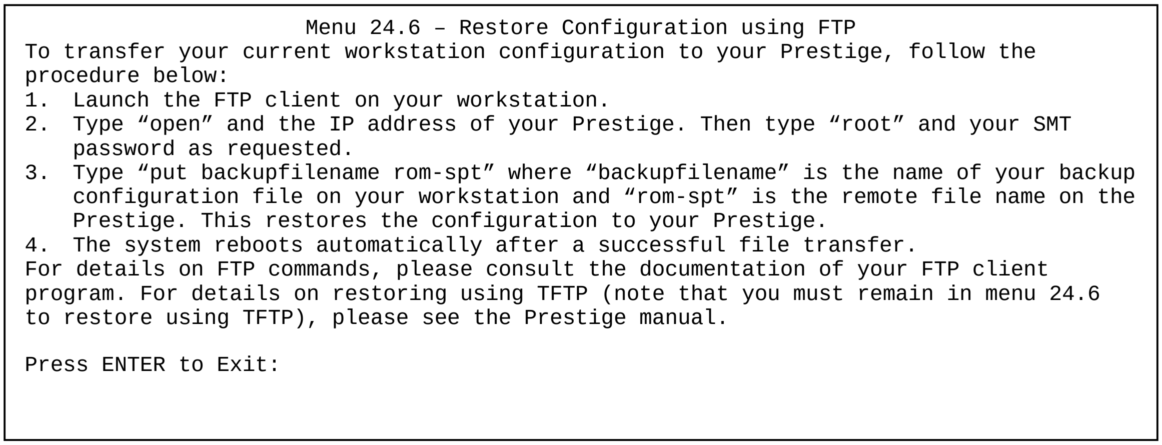
Figure 15-5 Successful Backup Confirmation Screen

15.3 Restore Configuration

Option **6** from **Menu 24 - System Maintenance** allows you to restore the current workstation backup configuration to your Prestige.

15.3.1 Restore using FTP

To transfer your current workstation configuration to your Prestige, follow the instructions as shown in the following screen. See also the FTP example later in this chapter. For details on FTP commands, please consult the documentation of your FTP client program.



```
                      Menu 24.6 – Restore Configuration using FTP
To transfer your current workstation configuration to your Prestige, follow the
procedure below:
1.  Launch the FTP client on your workstation.
2.  Type “open” and the IP address of your Prestige. Then type “root” and your SMT
    password as requested.
3.  Type “put backupfilename rom-spt” where “backupfilename” is the name of your backup
    configuration file on your workstation and “rom-spt” is the remote file name on the
    Prestige. This restores the configuration to your Prestige.
4.  The system reboots automatically after a successful file transfer.
For details on FTP commands, please consult the documentation of your FTP client
program. For details on restoring using TFTP (note that you must remain in menu 24.6
to restore using TFTP), please see the Prestige manual.

Press ENTER to Exit:
```

Figure 15-6 Menu 24.6 as seen using Telnet

15.3.2 Restore using TFTP

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 configuration file, follow the procedure below. See also the TFTP example later in this chapter. Follow steps 1 to 4 as outlined previously in *15.2.2*, then continue with the steps below.

Step 1. Go to SMT menu 24.6. You must remain in this menu until file transfer is complete.

Step 2. Use the TFTP client to transfer files between the Prestige and the workstation. The remote file name on the Prestige is “rom-spt”.

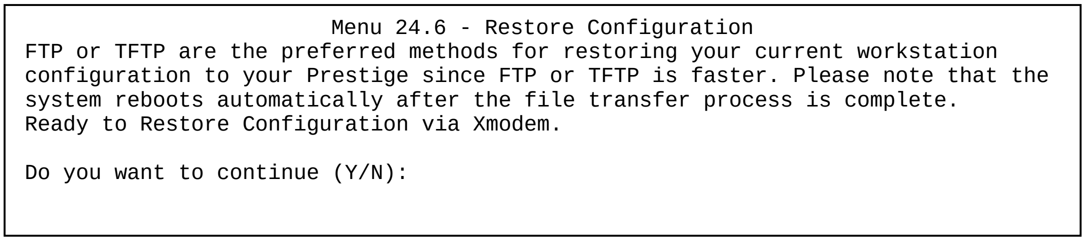
Step 3. The system reboots automatically after the file transfer process is complete.

The telnet connection must be active before and during TFTP transfer.

For UNIX, use “binary” to set binary transfer mode before using “get” to transfer from the Prestige to the computer. For details on TFTP commands, please consult the documentation of your TFTP client program.

15.3.3 Restore using the Console Port

You can restore the backup configuration on your computer either through FTP or TFTP (preferred methods as they are faster) or through the RS-232 console port (if the network is down). To restore via the console port any serial communications program should work fine; however, you must use the XMODEM protocol to perform the download/upload. The system reboots automatically after the file transfer process is complete.



```
                        Menu 24.6 - Restore Configuration
FTP or TFTP are the preferred methods for restoring your current workstation
configuration to your Prestige since FTP or TFTP is faster. Please note that the
system reboots automatically after the file transfer process is complete.
Ready to Restore Configuration via Xmodem.

Do you want to continue (Y/N):
```

Figure 15-7 Menu 24.6 as seen using the Console Port

Step 1. Go to menu 24.6.

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

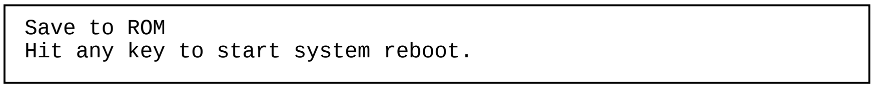
Step 3. Click **Transfer** in the HyperTerminal menu bar, then **Send File** from the drop-down menu.

Step 4. Enter the configuration filename on your computer.

Step 5. Choose the **Xmodem** Protocol.

Step 6. Finally, press **Send**.

Step 7. After a successful restoration you will see the following screen.



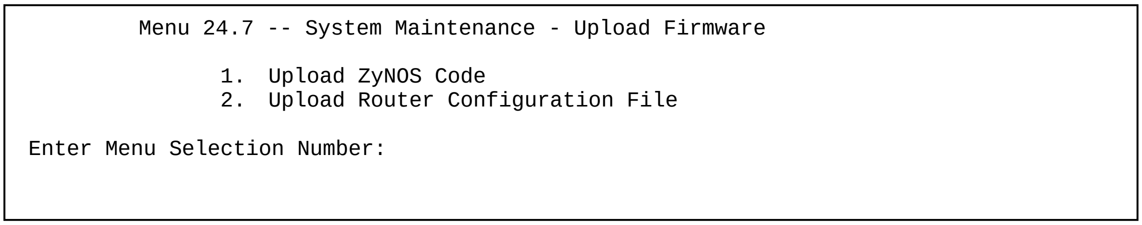
```
Save to ROM
Hit any key to start system reboot.
```

Figure 15-8 Successful Restoration Confirmation Screen

15.4 Upload Firmware

Option **7** from **Menu 24 - System Maintenance** takes you to **Menu 24.7 - System Maintenance - Upload Firmware** which allows you to upgrade the firmware. You can upgrade the firmware either through FTP or TFTP (preferred methods as they are faster) or through the RS-232 console port (if the network is down). The system reboots automatically after the file transfer process is complete.

The Prestige P1600 internal filenames are ‘ras-m’ (main block) and ‘ras-b’ (backup block).



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

               1.  Upload ZyNOS Code
               2.  Upload Router Configuration File

Enter Menu Selection Number:
```

Figure 15-9 Menu 24.7 - System Maintenance - Upload Firmware

15.4.1 Dual Firmware Block Structure

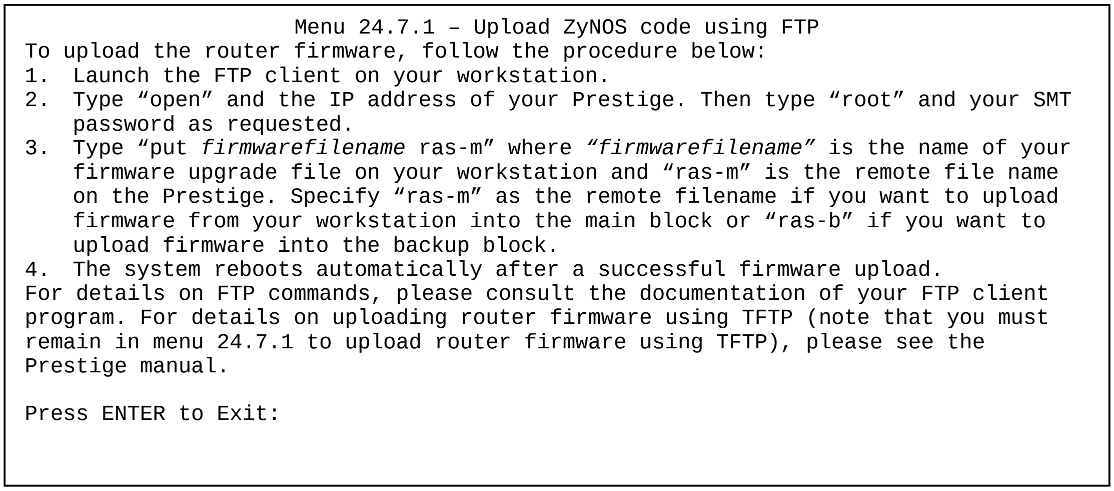
The Prestige 1600 employs a “dual firmware block structure” where one block is called the “main block” and the other block is called the “backup block”. The benefits of this approach are:

You can save the current firmware into the backup block before you upload new firmware. If the new firmware has problems, you may either revert to the old working firmware by using the “ATSW” command under Boot Extension or selectively run the old firmware in the backup block by using the “ATGB” command under Boot Extension.

If the firmware in the main block gets corrupted for some reason, the Prestige will try to boot from the backup block automatically.

15.4.2 Upload Prestige Firmware using FTP

To transfer the firmware, follow the instructions as shown in the following screen (Menu 24.7.1 using Telnet).

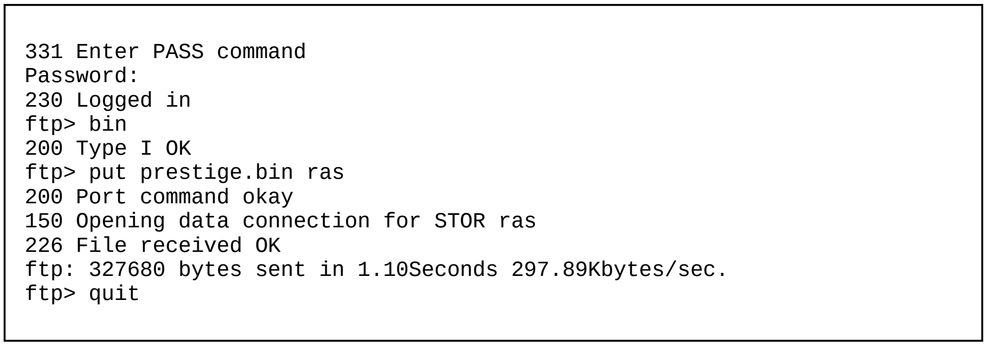


```
                     Menu 24.7.1 – Upload ZyNOS code using FTP
To upload the router firmware, follow the procedure below:
1.  Launch the FTP client on your workstation.
2.  Type “open” and the IP address of your Prestige. Then type “root” and your SMT
    password as requested.
3.  Type “put firmwarefilename ras-m” where “firmwarefilename” is the name of your
    firmware upgrade file on your workstation and “ras-m” is the remote file name
    on the Prestige. Specify “ras-m” as the remote filename if you want to upload
    firmware from your workstation into the main block or “ras-b” if you want to
    upload firmware into the backup block.
4.  The system reboots automatically after a successful firmware upload.
For details on FTP commands, please consult the documentation of your FTP client
program. For details on uploading router firmware using TFTP (note that you must
remain in menu 24.7.1 to upload router firmware using TFTP), please see the
Prestige manual.

Press ENTER to Exit:
```

Figure 15-10 Menu 24.7.1 as seen using Telnet

15.4.3 Example - Using the FTP command from the DOS Prompt

Use “put” to transfer files from the workstation to the Prestige, e.g., `put prestige.bin ras` transfers the firmware on your computer (“prestige.bin”) to the Prestige and renames it “ras”. Type “quit” to exit the ftp prompt.



```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put prestige.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 15-11 FTP Session Example

Note: The system reboots after a successful upload.

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

Table 15-2 Third Party FTP Clients - General Commands

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).

15.4.4 Upload Prestige Firmware using TFTP

To use TFTP, your workstation must have both telnet and TFTP clients. Follow steps 1 to 4 as outlined previously in *15.2.2*, then continue with the steps below.

Step 1. Go to SMT menu 24.7.1. You must remain in this menu until file transfer is complete.

Step 2. Use the TFTP client to transfer files between the Prestige and the workstation.

Step 3. Specify "ras-m" as the remote filename if you want to upload firmware from your workstation into the main block or "ras-b" if you want to upload firmware into the backup block of the Prestige.

Step 4. The system reboots automatically after a successful firmware upload.

The telnet connection must be active before and during the TFTP transfer.

For UNIX, use "binary" to set binary transfer mode before using "get" to transfer from the Prestige to the computer. For details on TFTP commands, please consult the documentation of your TFTP client program.

15.4.5 Third Party TFTP Clients - General Commands

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

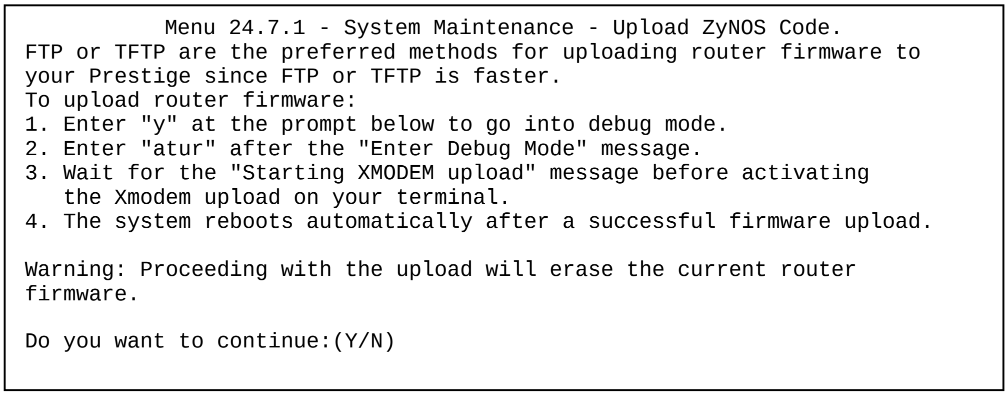
Table 15-3 Third Party TFTP Clients - General Commands

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.

15.4.6 Upload Prestige Firmware via the Console Port

You can upload Prestige firmware to your Prestige either through FTP or TFTP (preferred methods as they are faster) or through the RS-232 console port (if the network is down). To upload Prestige firmware via the console port any serial communications program should work fine; however, you must use the XMODEM protocol to perform the download/upload.

Select **1** from **Menu 24.7 - System Maintenance - Upload Firmware** to display **Menu 24.7.1 - System Maintenance - Upload ZyNOS Code**, then follow the instructions as shown in the following screen.



```
           Menu 24.7.1 - System Maintenance - Upload ZyNOS Code.
FTP or TFTP are the preferred methods for uploading router firmware to
your Prestige since FTP or TFTP is faster.
To upload router firmware:
1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atur" after the "Enter Debug Mode" message.
3. Wait for the "Starting XMODEM upload" message before activating
   the Xmodem upload on your terminal.
4. The system reboots automatically after a successful firmware upload.

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

Do you want to continue:(Y/N)
```

Figure 15-12 Menu 24.7.1 as seen using the Console Port.

You can type 'atur' to upload ras code to the P1600 main block as atur = atum. If you want to upload ras code to the backup block then you must type 'atub' instead of 'atur'.

After the "Starting XMODEM upload" message appears, activate the Xmodem protocol on your computer. The following procedure is for the HyperTerminal program. The procedure for other serial communications programs should be similar.

Step 1. Click **Transfer** in the HyperTerminal menu bar, then **Send File** from the drop-down menu.

Step 2. Enter the path and name of the firmware file (“bin” extension) on your computer.

Step 3. Choose the **Xmodem** Protocol.

Step 4. Finally, press **Send**.

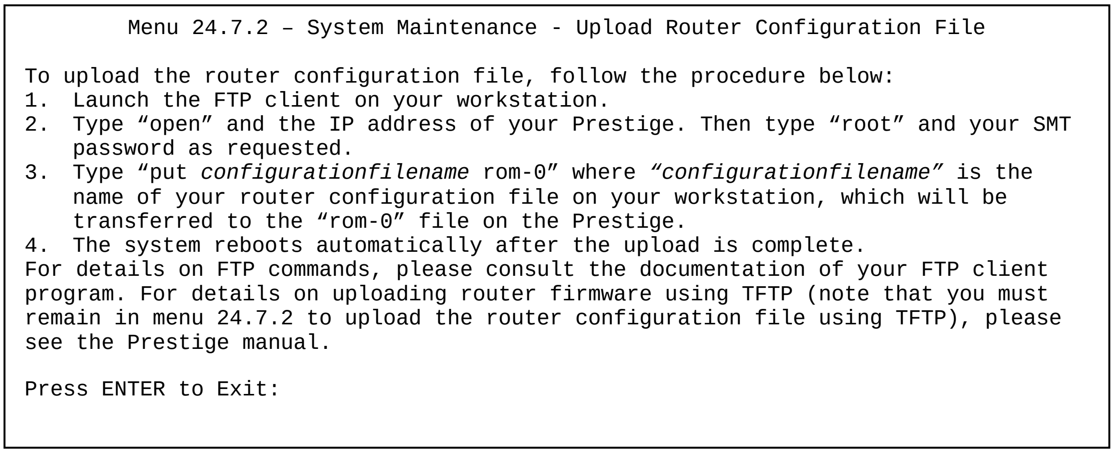
Step 5. The system reboots automatically after a successful firmware upload.

15.5 Upload Prestige Configuration File

The configuration data, system-related data, error log and trace log are all stored in the configuration file. You can upload the configuration file either through FTP or TFTP (preferred methods as they are faster) or through the RS-232 console port (if the network is down). You need to reboot the system after the configuration file upload process is complete. Uploading the configuration file replaces all previous configurations; the speed of the console port will be reset to the default of 9600 bps with 8 data bit, no parity and 1 stop bit (8n1) and the password will also be reset to the default of 1234.You will need to change your serial communication software to the defaults before you can connect to the Prestige again.

15.5.1 Upload Prestige Configuration File using FTP

To upload the router configuration file, follow the instructions as shown in the following screen (Menu 24.7.2 using Telnet). See also the FTP example earlier in this chapter.



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

To upload the router configuration file, follow the procedure below:
1.  Launch the FTP client on your workstation.
2.  Type “open” and the IP address of your Prestige. Then type “root” and your SMT
    password as requested.
3.  Type “put configurationfilename rom-0” where “configurationfilename” is the
    name of your router configuration file on your workstation, which will be
    transferred to the “rom-0” file on the Prestige.
4.  The system reboots automatically after the upload is complete.
For details on FTP commands, please consult the documentation of your FTP client
program. For details on uploading router firmware using TFTP (note that you must
remain in menu 24.7.2 to upload the router configuration file using TFTP), please
see the Prestige manual.

Press ENTER to Exit:
```

Figure 15-13 Menu 24.7.2 as seen using Telnet

15.5.2 Upload Prestige Configuration File using TFTP

To use TFTP, your workstation must have both telnet and TFTP clients. Follow steps 1 to 4 as outlined previously in and then continue with the steps below.

Step 1. Go to SMT menu 24.7.2. You must remain in this menu until file transfer is complete.

Step 2. Use the TFTP client to transfer files between the Prestige and the workstation.

Step 3. Specify “rom-0” as the remote file name on the Prestige.

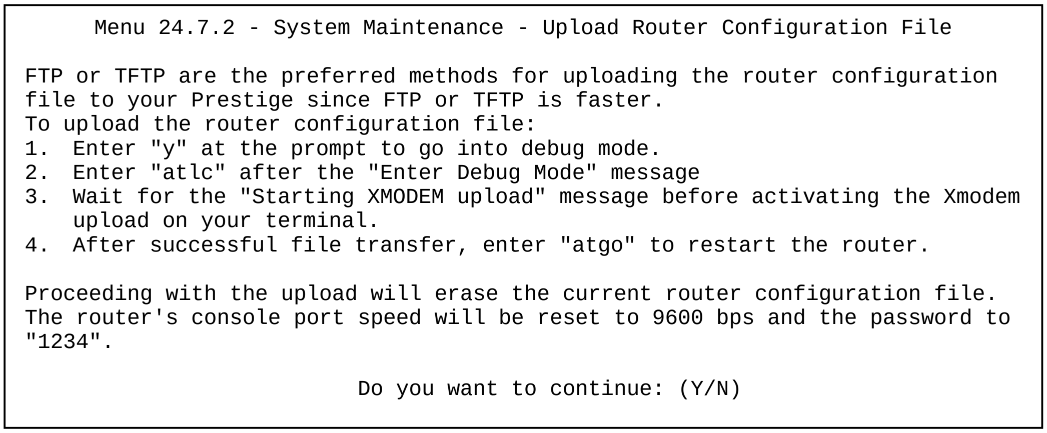
Step 4. The system reboots automatically after the upload Prestige configuration file process is complete.

The telnet connection must be active before and during the TFTP transfer.

For UNIX, use “binary” to set binary transfer mode before using “get” to transfer from the Prestige to the computer. For details on TFTP commands, please consult the documentation of your TFTP client program.

15.5.3 Upload Prestige Configuration File using the Console Port

Select **2** from **Menu 24.7 - System Maintenance - Upload Firmware** to display **Menu 24.7.2 - System Maintenance - Upload Router Configuration File**. Follow the instructions as shown in the following screen.



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

FTP or TFTP are the preferred methods for uploading the router configuration
file to your Prestige since FTP or TFTP is faster.
To upload the router configuration file:
1.  Enter "y" at the prompt to go into debug mode.
2.  Enter "atlc" after the "Enter Debug Mode" message
3.  Wait for the "Starting XMODEM upload" message before activating the Xmodem
    upload on your terminal.
4.  After successful file transfer, enter "atgo" to restart the router.

Proceeding with the upload will erase the current router configuration file.
The router's console port speed will be reset to 9600 bps and the password to
"1234".

                          Do you want to continue: (Y/N)
```

Figure 15-14 Menu 24.7.2 as seen using the Console Port

After the "Starting XMODEM upload" message appears, activate the Xmodem protocol on your computer. The following procedure is for the HyperTerminal program. The procedure for other serial communications programs should be similar.

Step 1. Click **Transfer** in the HyperTerminal menu bar, then **Send File** from the drop-down menu.

Step 2. Enter the configuration filename on your computer.

Step 3. Choose the **Xmodem** Protocol.

Step 4. Finally, press **Send**.

Chapter 16
IP Policy Routing

This chapter explains IP Policy Routing and helps you to configure IP Policy Routing.

16.1 Introduction

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

16.1.1 Benefits

Source-Based Routing - Network administrators can use policy-based routing to direct traffic from different users through different connections.

Quality of Service (QoS) - Organizations can differentiate traffic by setting the precedence or TOS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.

Cost Savings - IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.

Load Sharing - Network administrators can use IPPR to distribute traffic among multiple paths.

16.1.2 Routing Policy

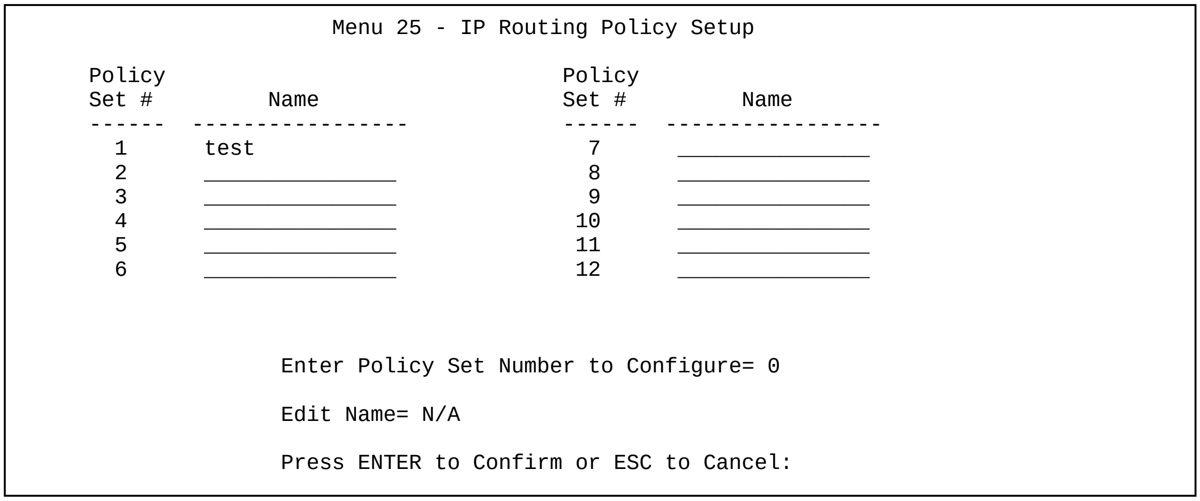
A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria include the source address and port, IP protocol (ICMP, UDP, TCP, etc.), destination address and port, TOS and precedence (fields in the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

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

IPPR follows the existing packet filtering facility of ZyNOS in style and in implementation. The policies are divided into sets, where related policies are grouped together. A user defines the policies before applying them to an interface or a remote node, in the same fashion as the filters. There are 12 policy sets with 6 policies in each set.

16.2 IP Routing Policy Setup

Menu 25 shows all the policies defined.



```
                       Menu 25 - IP Routing Policy Setup

    Policy                               Policy
    Set #        Name                    Set #        Name
    ------  -----------------            ------  -----------------
      1      test                           7     _______________
      2     _______________                 8     _______________
      3     _______________                 9     _______________
      4     _______________                10     _______________
      5     _______________                11     _______________
      6     _______________                12     _______________



                   Enter Policy Set Number to Configure= 0

                   Edit Name= N/A

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

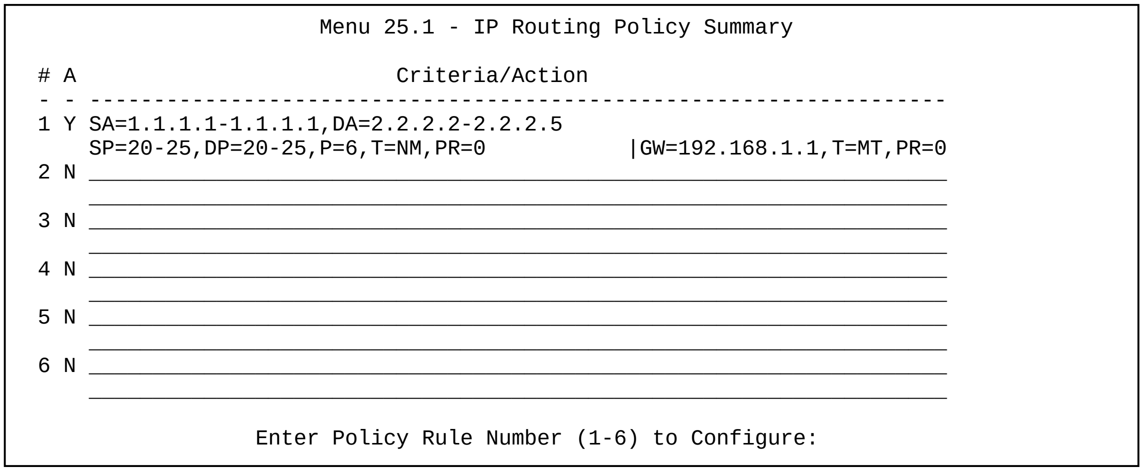
Figure 16-1 Menu 25 - IP Routing Policy Setup

To setup a routing policy, follow the procedure below:

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

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

Menu 25.1 shows the summary of a policy set, including the criteria and the action of a single policy, and whether a policy is active or not. Each policy contains two lines. The former part is the criteria of the incoming packet, and the latter is the action. Between these two parts, separator '|' means the action is taken on criteria matched and separator '=' means the action is taken on criteria not matched.



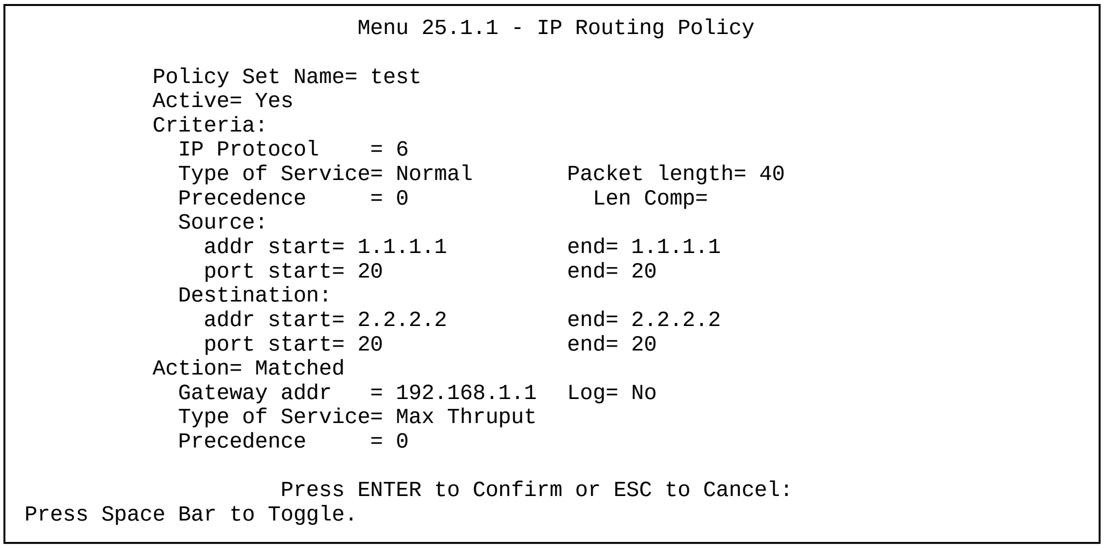
```
                      Menu 25.1 - IP Routing Policy Summary

# A                         Criteria/Action
- - -------------------------------------------------------------------
1 Y SA=1.1.1.1-1.1.1.1,DA=2.2.2.2-2.2.2.5
    SP=20-25,DP=20-25,P=6,T=NM,PR=0          |GW=192.168.1.1,T=MT,PR=0
2 N ___________________________________________________________________
    ___________________________________________________________________
3 N ___________________________________________________________________
    ___________________________________________________________________
4 N ___________________________________________________________________
    ___________________________________________________________________
5 N ___________________________________________________________________
    ___________________________________________________________________
6 N ___________________________________________________________________
    ___________________________________________________________________

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

Figure 16-2 Menu 25 - IP Routing Policy Summary

Table 16-1 IP Routing Policy Summary

Abbreviation	Meaning
Criteria	
SA	Source IP address
SP	Source port
DA	Destination IP address
DP	Destination port
P	IP layer 4 protocol number(TCP=6,UDP=17…)
T	Type Of Service of Incoming packet
PR	Precedence of incoming packet
Action	
GW	Gateway IP address
T	Outgoing Type of Service
P	Outgoing Precedence
Type Of Service	
NM	Normal
mD	Minimum Delay
MT	Maximum Throughput
MR	Maximum Reliability
MC	Minimum Cost

Enter a number from 1 to 6 to display Menu 25.1.1 - IP Routing Policy (see the next figure). This menu allows you to configure a policy rule.



```
                          Menu 25.1.1 - IP Routing Policy

          Policy Set Name= test
          Active= Yes
          Criteria:
            IP Protocol    = 6
            Type of Service= Normal       Packet length= 40
            Precedence     = 0              Len Comp=
            Source:
              addr start= 1.1.1.1         end= 1.1.1.1
              port start= 20              end= 20
            Destination:
              addr start= 2.2.2.2         end= 2.2.2.2
              port start= 20              end= 20
          Action= Matched
            Gateway addr   = 192.168.1.1  Log= No
            Type of Service= Max Thruput
            Precedence     = 0

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

Figure 16-3 Menu 25.1.1 - IP Routing Policy

Table 16-2 IP Routing Policy

Field	Description
Policy Set Name	This is the name of the policy set assigned in **Menu 25 - IP Routing Policy Setup**.
Active	Press the spacebar to select **Yes** to activate the policy.
Criteria	
IP Protocol	IP layer 4 protocol, e.g., UDP, TCP, ICMP, etc.
Type of Service	Prioritize incoming network traffic by choosing from **Don't Care/ Normal / Min Delay / Max Thruput / Max Reliability**.
Packet Length	Enter the length of incoming packets (in bytes). The operators in the **Len Comp** (next) apply to packets of this length.
Len Comp	Press the spacebar to choose from **Equal / Not Equal / Less / Greater / Less or Equal / Greater or Equal**.
Precedence	Precedence value of the incoming packet. Values range from 0 to 7 or Don't Care.
Source:	
addr start= / end=	Source IP address range from start to end.
port start= / end=	Source port number range from start to end; applicable only for TCP/UDP.
Destination:	
addr start= / end=	Destination IP address range from start to end.
port start= / end=	Destination port number range from start to end; applicable only for TCP/UDP.
Action=	Specifies whether action should be taken on criteria **Matched** or **Not Matched**.
Gateway addr	Defines the outgoing gateway address. The gateway must be on the same subnet as the Prestige if it's on the LAN, otherwise, the gateway must be the IP address of a remote node. The default gateway is specified as 0.0.0.0.
Log	Press the spacebar to select **Yes** to make an entry in the system log when a policy is executed.
Type of Service	Set the new TOS value of the outgoing packet. Choose from Prioritize incoming network traffic by choosing from **No Change / Normal / Min Delay / Max Thruput / Max Reliability**.
Precedence	Set the new precedence value of the outgoing packet. Values range from 0 to 7 or No Change.

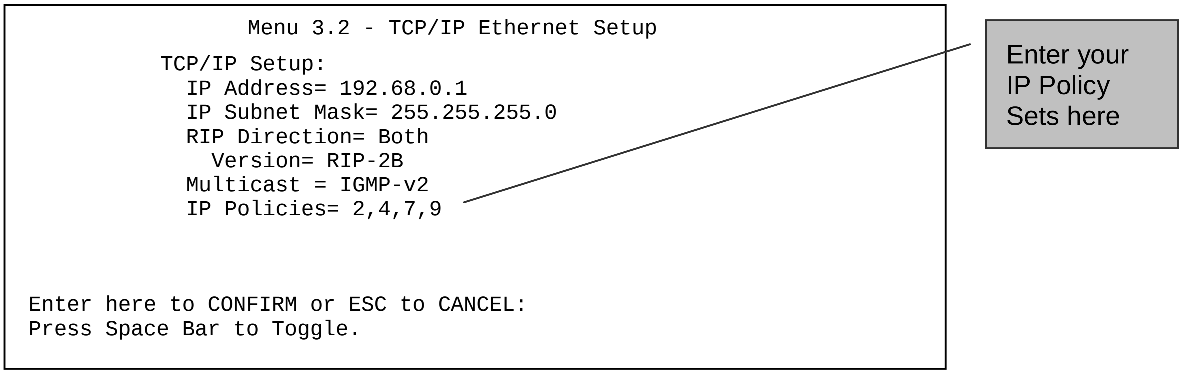
16.3 Applying an IP Policy

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

16.3.1 Ethernet IP Policies

From **Menu 3 - Ethernet Setup**, enter 2 to go to **Menu 3.2 -TCP/IP Ethernet Setup**.

You can choose up to four IP Policy sets (from twelve) by entering their numbers separated by commas, e.g., 2, 4, 7, 9.



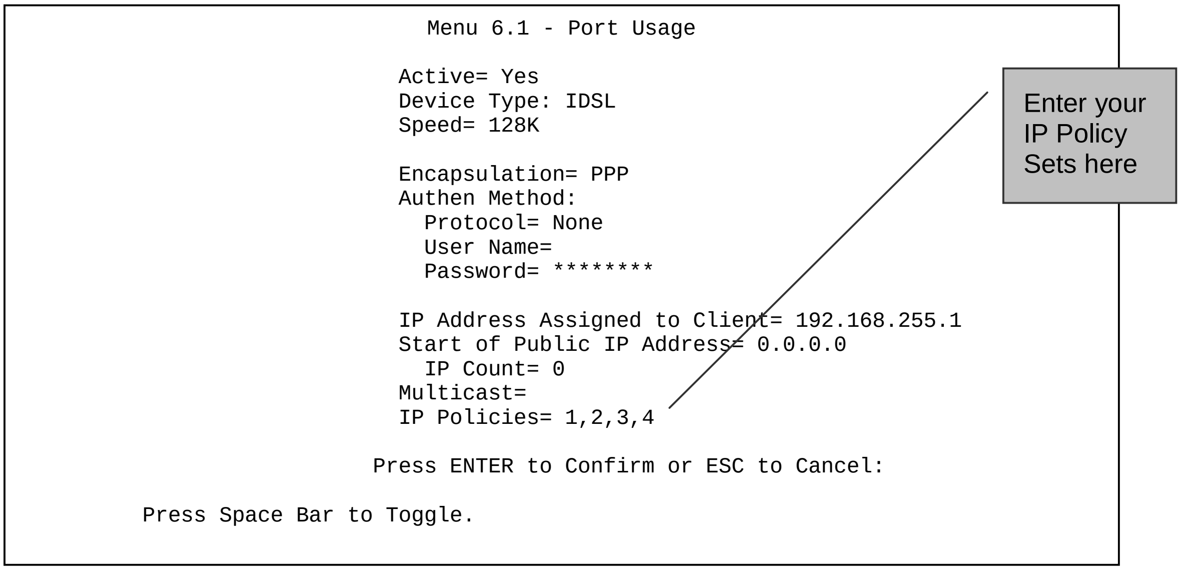
```
                 Menu 3.2 - TCP/IP Ethernet Setup

          TCP/IP Setup:
            IP Address= 192.68.0.1
            IP Subnet Mask= 255.255.255.0
            RIP Direction= Both
              Version= RIP-2B
            Multicast = IGMP-v2
            IP Policies= 2,4,7,9



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

Enter your IP Policy Sets here

Figure 16-4 Ethernet IP Policies

16.3.2 DSL IP Routing Policies

Go to **Menu 6.1** and enter the number(s) of the IP Routing Policy set(s) as appropriate. You can cascade up to four policy sets by entering their numbers separated by commas.



```
                      Menu 6.1 - Port Usage

                    Active= Yes
                    Device Type: IDSL
                    Speed= 128K

                    Encapsulation= PPP
                    Authen Method:
                      Protocol= None
                      User Name=
                      Password= ********

                    IP Address Assigned to Client= 192.168.255.1
                    Start of Public IP Address= 0.0.0.0
                      IP Count= 0
                    Multicast=
                    IP Policies= 1,2,3,4

                  Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Enter your IP Policy Sets here

Figure 16-5 IDSL IP Routing Policies

16.4 IP Policy Routing Example

If a network has both Internet and remote node connections, you can route Web packets to the Internet using one policy and route FTP packets to a remote network using another policy. See the next figure.

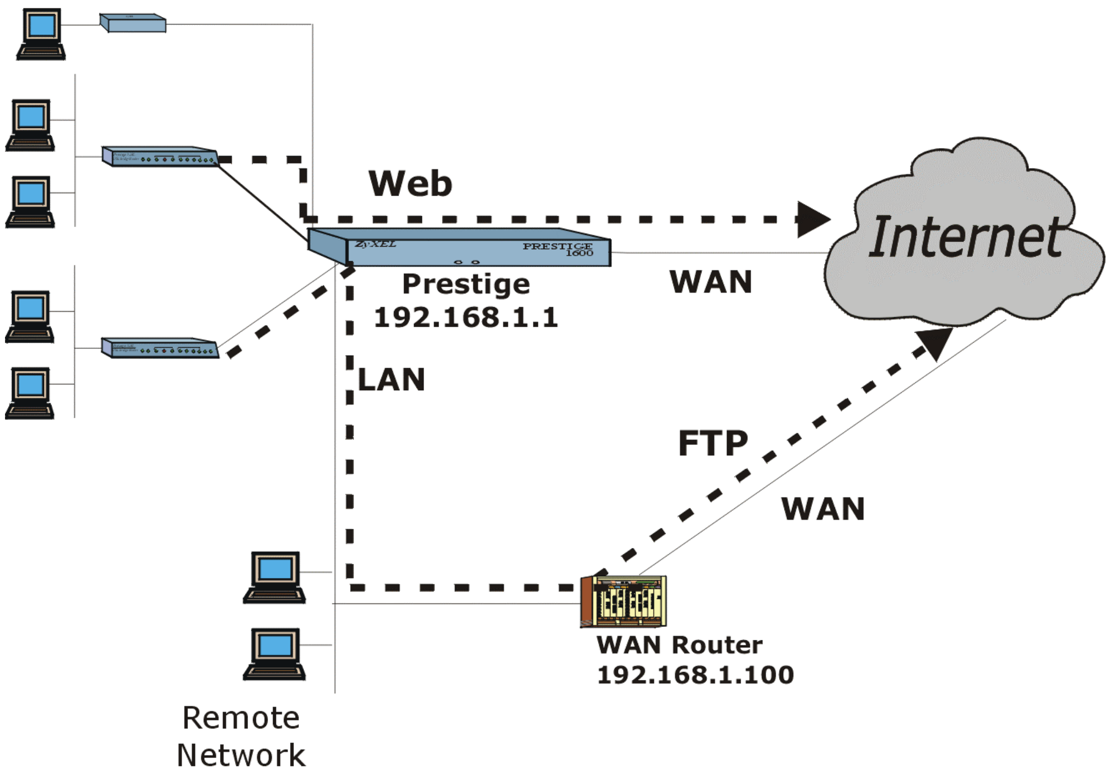
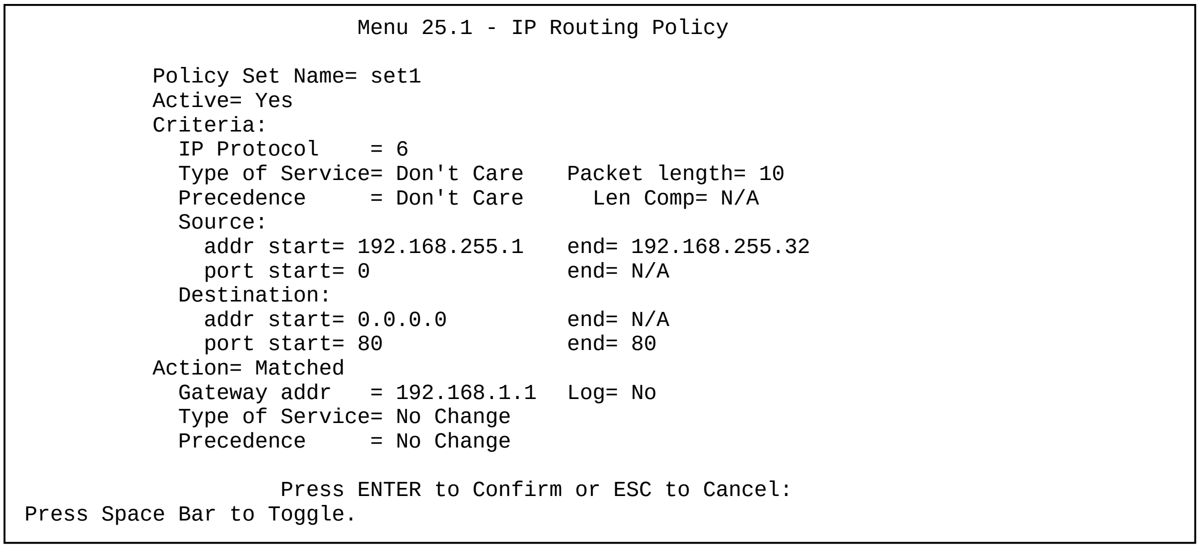


Figure 16-6 Example of IP Policy Routing

To force Web packets coming from clients with IP addresses of 192.168.255.1 to 192.168.255.32 to be routed to the Internet via the WAN port of the P1600, follow the steps mentioned next.

Step 1. Create a routing policy set in Menu 25.

Step 2. Create a rule for this set in **Menu 25.1 - IP Routing Policy** as shown next.



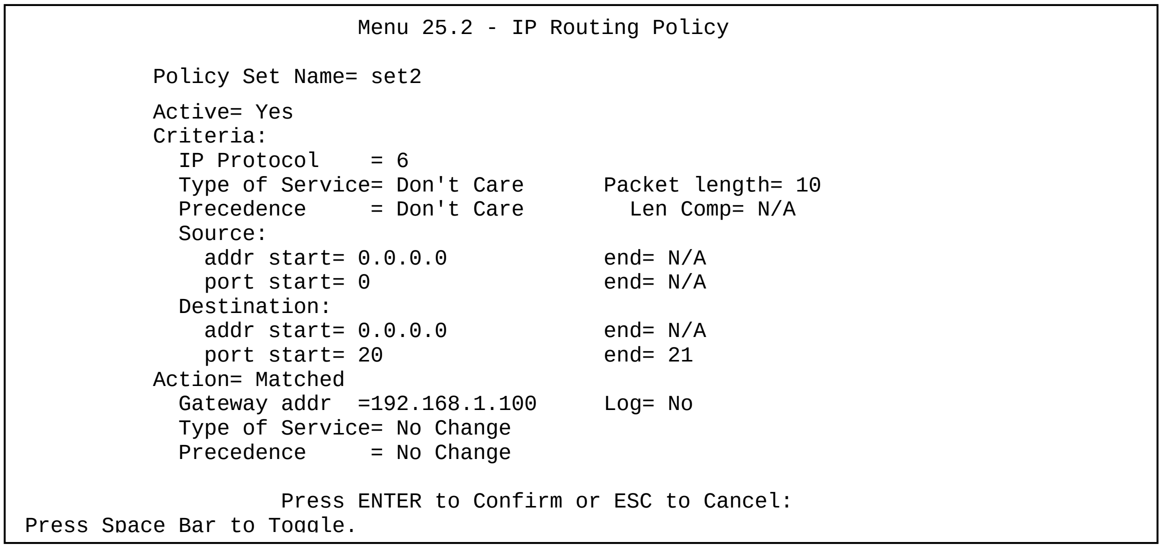
```
                          Menu 25.1 - IP Routing Policy

          Policy Set Name= set1
          Active= Yes
          Criteria:
            IP Protocol    = 6
            Type of Service= Don't Care   Packet length= 10
            Precedence     = Don't Care     Len Comp= N/A
            Source:
              addr start= 192.168.255.1   end= 192.168.255.32
              port start= 0               end= N/A
            Destination:
              addr start= 0.0.0.0         end= N/A
              port start= 80              end= 80
          Action= Matched
            Gateway addr   = 192.168.1.1  Log= No
            Type of Service= No Change
            Precedence     = No Change

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

Figure 16-7 IP Routing Policy Example

Step 3. Check **Menu 25.1 - IP Routing Policy Setup** to see if the rule is added correctly.

Step 4. Create another policy set in **Menu 25**.

Step 5. Create a rule this set in Menu 25.2 to route packets from any host (IP=0.0.0.0 means any host) with protocol TCP and port FTP access through another gateway (192.168.1.100).

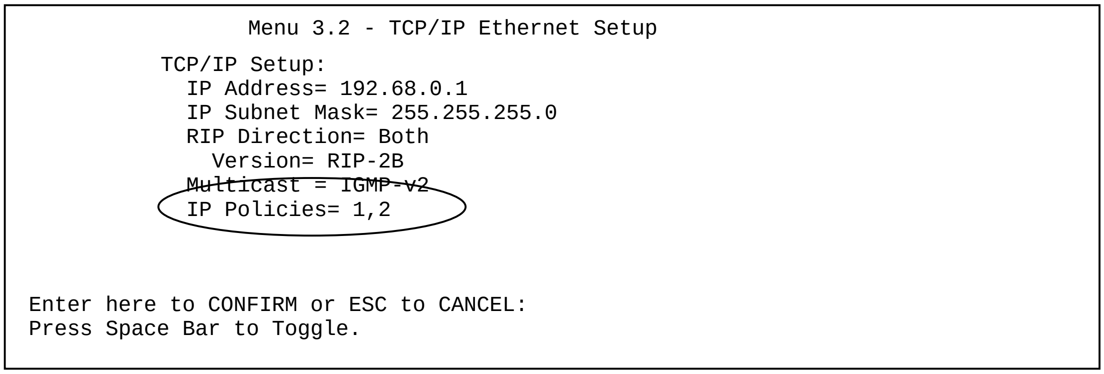


```
                          Menu 25.2 - IP Routing Policy

          Policy Set Name= set2
          Active= Yes
          Criteria:
            IP Protocol    = 6
            Type of Service= Don't Care      Packet length= 10
            Precedence     = Don't Care        Len Comp= N/A
            Source:
              addr start= 0.0.0.0            end= N/A
              port start= 0                  end= N/A
            Destination:
              addr start= 0.0.0.0            end= N/A
              port start= 20                 end= 21
          Action= Matched
            Gateway addr  =192.168.1.100     Log= No
            Type of Service= No Change
            Precedence     = No Change

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

Figure 16-8 IP Policy Routing

Step 6. Check **Menu 25.1 - IP Routing Policy Setup** to see if the rule is added correctly.

Step 7. Apply both policy sets in **Menu 3.2** as shown next.



```
                   Menu 3.2 - TCP/IP Ethernet Setup

          TCP/IP Setup:
            IP Address= 192.68.0.1
            IP Subnet Mask= 255.255.255.0
            RIP Direction= Both
              Version= RIP-2B
            Multicast = IGMP-v2
            IP Policies= 1,2



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

Figure 16-9 Applying IP Policies

Chapter 17
Troubleshooting

17.1 Problems Starting Up the Prestige 1600

Table 17-1 Troubleshooting the Start-Up of your Prestige 1600

<table>
<tr><th>Troubleshooting</th><th colspan="2">Corrective Action</th></tr>
<tr><td>None of the LEDs are on when you power on the Prestige 1600.</td><td colspan="2">Check the connection between the power cord and your Prestige 1600.
If the error persists you may have a hardware problem. In this case you should contact technical support.</td></tr>
<tr><td rowspan="5">Cannot access the Prestige 1600 via the console port.</td><td colspan="2">Check to see if the Prestige 1600 is connected to your computer's serial port.</td></tr>
<tr><td rowspan="4">Check to see if the communications program is configured correctly. The communications software should be configured as mentioned here.</td><td>VT100 terminal emulation</td></tr>
<tr><td>9600 Baud</td></tr>
<tr><td>No parity, 8 Data bits, 1 Stop bit</td></tr>
<tr><td>Flow Control set to None</td></tr>
</table>

17.2 Problems With the xDSL Port

Table 17-2 Troubleshooting an xDSL Port Connection

Troubleshooting	Corrective Action
Cannot connect to the xDSL Client	Check Menu 24.1 to verify the line status. If it indicates [down], then refer to the section on the line problems.

17.3 Problems with the WAN Port

Table 17-3 Troubleshooting the WAN Port Connection

Troubleshooting	Corrective Action
Cannot connect to WAN device.	Check if the WAN port is connected to an external WAN device.
	Check if the power of the external WAN device is turned on.

17.4 Problems with the LAN Interface

Table 17-4 Troubleshooting the LAN Interface

Troubleshooting	Corrective Action
Can’t ping any station on the LAN	Check the Ethernet LED on the front panel of your Prestige 1600. If it is off, check the cables connecting your Prestige 1600 to the hub.
	Verify that the IP address and the subnet mask in Menu 3.2 are consistent between the Prestige 1600 and the workstations.

17.5 Problems Connecting to a Remote Node or ISP

Table 17-5 Troubleshooting a Connection to a Remote Node or ISP

Troubleshooting	Corrective Action
Can’t connect to a remote node or ISP	Check Menu 24.1 to verify the line status. If it indicates [down], then refer to the section on the line problems.
	Check the error log in Menu 24.3.1. If it does indicate that something has gone wrong, it may be an IP address configuration error.

17.6 General Instructions

If you have other problems, you can try the following options.

- Check the **Menu 24.1 System Maintenance - Status**, **Menu 24.2.1 - System Information** and **Menu 24.3 System Maintenance - Log and Trace** in order to locate the problem.
- Check the Troubleshooting section in the Support Notes.
- Use Debug commands to diagnose problems. In general, ZyXEL recommends that you use these commands with the direction of your customer support representative.

CI Commands

Use **Menu 24.8** to enter command line mode. Please refer to the section 14.6 *Command Interpreter Mode* for details about the SMT menu. The following table describes the syntax used to configure your Prestige using Command Interface (CI) commands. For details on other CI commands to configure your Prestige, please consult the supporting CD.

ZyXEL recommends that you use CI Commands for debugging purposes only. You are advised to configure the Prestige through menu interface.

Command Syntax

CI user interface uses the following syntax:

command < iface **|** device > subcommand [*Parma*]

command subcommand [*Parma*]

command ? **|** help

command subcommand ? **|** help

[channel-name]: enet0 for Ethernet port, wan00 for WAN port (only available in P1600 primary), xdsln (n=00~31) for xDSL port

[iface-name]: enif0 for Ethernet port, wanif0 for WAN port (only available in P1600 primary), wanifn (n=01~32) for IDSL port

System Related Commands

CI Command			Options	Description
sys				
	cbuf			
		cnt	disp	Display cbuf static
			clear	Clear cbuf static
		disp	[a|f|u]	Display cbuf a: all f: free u: used
	cpu	disp		Display CPU utilization
	dir			Display file directory
	edit		<filename>	Edit a text file
	errctl		[level]	Set the error control level
				0:crash no save, not in debug mode (default)
				1:crash no save, in debug mode
				2:crash save, not in debug mode
				3:crash save, in debug mode
	event			
		display		Display tag flags information
		trace	[display|clear]	Display system event information
	feature			Display feature bit
	fid	display		Display function id list

CI Command			Options	Description
	filter			
		disp		Display filter statistic counters
		clear		Clear filter statistic counter
		sw	[on|off]	
	hostname			Display system hostname
	iface	disp		Display iface list
	log			
		disp		Display log error
		clear		Clear log error
		online	[on|off]	Turn on/off error log online display
	mbuf			
		cnt	[disp|cl]	Display or clear system mbuf count
		link	link	List system mbuf link
		pool	[id] [type]	List system mbuf pool
		status		Display system mbuf status
		disp	<address>	Display mbuf status
	memutil			
		usage		Display memory allocate and heap status
		mq	<address> <len>	Display memory queues
		mcell	mid [f|u]	Display memory cells by given ID
		msecs		Display memory sections
	pro			
		disp		Display all process information
		stack	[TAG]	Display process's stack by a give TAG
		ps	[TAG]	Display process's status by a give TAG
	queue			
		disp	[a|f|u] [start#] [end#]	Display queue by given status and range numbers
		ndisp	[#]	Display a queue by a given number
	quit			Quit CI command mode
	reboot		[code]	Reboot system
				code = 0 cold boot,
				= 1 immediately boot
				= 2 bootModule debug mode
	reslog		[disp|clear]	Display resources trace
	roadrun	disp	<iface-name>	Display roadrunner information
				iface-name: enif0, wanif0, wanifn (n=01~32)

CI Command			Options	Description
		debug	<level>	Enable/disable roadrunner service
				0: diable <default>
				1: enable
		restart	<iface-name>	
	socket			
	spt	dump	[root|rn|user|slot]	Dump spt raw data
		size		Display spt record size
	stdio		[second]	Change terminal timeout value
	timer			
		disp	[a|f|u]	Display timer cell
	trcdisp			Monitor packets
.	.	brief	.	Online display packet content briefly
.	.	parse	.	Online parse packet content
	trcl			
		call		Display call event
		clear		Clear trace
		disp		Display trace log
		level	[#]	Set trace level of trace log #:1-10
		online	[on|off]	Set on/off trace log online
		switch	[on|off]	Set system trace log
		type	<bitmap>	Set trace type of trace log
	trcp			
		chann	<channel name> [none|incoming|outgoing|bothway]	Set packet trace direction for a given channel
				<channel name>=enet0, wan00, idsln (n=00~31)
		create	<entry> <size>	Create packet trace buffer
		destroy		Packet trace related commands
		disp		Display packet trace
		string		
		switch	[on|off]	Turn on/off the packet trace
		udp	[sw|addr|port]	Send packet trace to other system
		brief		Display packet content briefly
		parse	[[begin_idx], end_idx]	Parse packet content
	version			Display RAS code and driver version
	view		<filename>	View a text file
	wdog			
		switch	[on|off]	Set on/off wdog
		cnt	<value>	Display watchdog counts value: 0-34463

DSL related CI Commands

CI Command			Options			Description
xdsl	cnt	disp	chann name|scc2|scc4			Display idsl channel/line counter
		clear	chann name|scc2|scc4			Clear idsl channel/line counter
	test	disp	packet	0|1|2		Set packet display mode in testing
			event	chann name	on|off	Set event display mode in testing
		inernal	chann name	cnt		Do internal loopback
		external	chann name	cnt		Do external loopback
	event	disp				Display ZyNOS event
		clear				Clear ZyNOS event
	netstat	chann name				Display network state
	reset	chann name				Reset channel
	drop	chann name				Drop channel
	version					Display NDIS version
	debug	on|off				Enable/disable debug. If enable and system crash, system will reboot and stop at BootExt
	dpram	system	line name			Display system descriptor
		parameter	line name			Display channel parameters
		inttable	line name			Display interrupt table
		bd	chann name			Display buffer descriptor
		bf	chann name			Display buffer
	idsl	rci	chann name|all			Read layer1 CI code
		wci	chann name	CI code	[up]	Write layer 1 CI code (up for upstream)
		rmon	chann name|all			Read layer1 Monitor code
		wmon	chann name	mon code 1	mon code 2	Write layer1 Monitor code
		status	chann name			Display layer1 near-end and far-end error count
		setbw	chann name	1:128K, 2:64K		Set layer1 bandwidth
		parameter	scc2|scc4			Display SCC parameters
		inttable	scc2|scc4			Display interrupt table
		chantable	chann name			Display channel parameter table
		bd	chann name			Display buffer descriptor
		bf	chann name			Display buffer
	modem	xx				Modem related CI command
	xdsl	xx				xDSL related CI command

IP related CI Commands

CI Command			Options	Description
ip	address			display host ip address
	arp			
		add	<hostid> ether <ether addr>	add arp
		drop	<hostid> [ether]	drop arp
		flush		flush arp
		publish		add proxy arp
		resolve	<hostid>	
		status		display ip arp status
	dhcp			set dhcp configuration
		arpcount	<num>	
		dnsserver	<dnsIP1> <dnsIP2>	
		gateway	<gateway IP>	
		hostname	<hostname>	
		leasetime	<period>	
		netmask	<netmask>	
		pool	<start IP> <num>	
		rebindtime	<period>	
		renewaltime	<period>	
		reset		
		status		
		<iface-name>	st	display iface DHCP information iface-name wanif2, wanif1, wanif0, enif1, enif0
			client release	release DHCP client IP
			client renew	renew DHCP client IP
	dns			
		table		display dns table
		stats	[disp|clear]	display or clear dns statistics
	icmp			
		check	[cmd|rsp|indication]	
		data		
		echo	[on|off]	
		status		display icmp statistic counter
		trace	[on|off]	turn on/off trace for debugging

	ifconfig			display ifconfig
	ping		<hostid>	ping remote host
	pong		<hostid> [<size> <time-interval>]	pong remote host
	rip			
		accept	<gateway>	
		activate		
		dialin_user	[show|in|out|both|none]	
		merge	[on|off]	RIP merging
		mode	<iface> [in|out] [mode]	mode: 0 - 3
		refuse	<gateway>	
ip	rip	request		
		reverse	[on|off]	RIP Poisoned Reverse
		status		display rip statistic counters
		trace		
	route			
		add	<dest addr>[/<bits>] <gateway> [<metric>]	add route
		addprivate		add private route
		drop	<host address> [/bits]	drop a route
		errcnt	[disp|clear]	display|clear routing statistic counters
		flush		flush route table
		lookup		
		status		display routing table
	status			display ip statistic counters
	sua			
		iface	<iface>	
		disp		display single user account statistic
		set	<IP addr> <Port #>	
	tcp			
		ceiling	<value>	TCP maximum round trip time
		floor	<value>	TCP minimum rtt
		kick		
		irtt	<value>	TCP default init rtt
		limit	<value>	
		mss	<size>	TCP input MSS
		reset		
		rtt		
		status		display TCP statistic counters
		syndata	[on|off]	TCP syndata piggyback

		trace	[on|off]	turn on/off trace for debugging
		window	[size]	TCP input window size
	tftp			
		stats		
		support		
	udp	status		

Ethernet Related CI Command

CI Command			Options	Description
ether				
	config			display LAN configuration information
	driver			
		cnt	disp <ch-name>	display ether driver counters
			clear <ch-name>	ch-name: enet0, enet1
		mac	<macaddr>	Set LAN Mac address
		reg		display LAN hardware related registers
		status	<ch-name>	ch-name: enet0, enet1
ether	driver	rxmod	<mode>	set LAN receive mode. mode: 1: turn off receiving 2: receive only packets of this interface 3: mode 2+ broadcast 5: mode 2 + multicast 6: all packets
	debug			display ethernet debug infomation
		disp	<ch-name>	display ethernet debug infomation
		level	<ch-name> <level>	set the ethernet debug level
				level 0: disable debug log
				level 1:enable debug log (default)
		arp	[ip-addr]	
		disp event	[ch-name] [on|off]	
		disp packet	[1|2|3]	
		sap		
	version			

Glossary

10BaseT	The 10-Mbps baseband Ethernet specification that uses two pairs of twisted-pair cabling (Category 3 or 5): one pair for transmitting data and the other for receiving data.
ADSL	Asymmetric Digital Subscriber Line. A digital subscriber line (DSL) technology in which the transmission of data from server to client is much faster than the transmission from the client to the server.
ARP	Address Resolution Protocol is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.
ATU-C and ATU-R	ADSL Transmission Unit, Central or Remote: the device at the end of an ADSL line that stands between the line and the first item of equipment in the subscriber premises or telephone switch. It may be integrated within an access node.
Backbone	A high-speed line or series of connections that forms a major pathway within a network.
Bandwidth	This is the capacity on a link usually measured in bits-per-second (bps).
bandwidth-on-demand	The ability of a user to dynamically set upstream and downstream line speeds to a particular rate of speed.
Bit	(Binary Digit) -- A single digit number in base-2, in other words, either a one or a zero. The smallest unit of computerized data.
bps	Bits per second. A standard measurement of digital transmission speeds.
Byte	A set of bits that represent a single character. There are 8 bits in a Byte.
Call Filtering	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.
CDR	Call Detail Record. This is a name used by telephone companies for call related information.
CHAP	Challenge Handshake Authentication Protocol is an alternative protocol that avoids sending passwords over the wire by using a challenge/response technique.
CI/CLI Commands	CI/CLI (Command Interface/Command Line Interface) commands can be accessed via Menu 24.8. For details on CI commands to configure your Prestige, please consult the supporting CD. ZyXEL recommends use of the CI Commands only for debugging purposes.
CIR	See Committed Information Rate.
Client	A software program that is used to contact and obtain data from a Server software program on another computer. Each Client program is designed to work with one or more specific kinds of Server programs and each Server requires a specific kind of Client. A Web Browser is a specific kind of Client.
Committed Information Rate	The carrier programs virtual circuits into the network between your sites and charges you for a specific level of service called the committed information rate (CIR). The CIR is a negotiated rate and is basically a guarantee that the carrier will always have that bandwidth available. The CIR limit for the Prestige is 8000Kbps. The sum of CIRs from all channels in a line cannot exceed 8000Kbps due to the processing limit of the P1600 CPU.
CPE	Customer Premises Equipment: that portion of the ADSL system residing within the customer's premises.
crossover Ethernet cable	A cable that wires a pin to its opposite pin, for example, RX+ is wired to TX+. This cable connects two similar devices, for example, two data terminal equipment (DTE) or data communications equipment (DCE) devices.
CSU/DSU	Channel Service Unit/Data Service Unit. CSUs (channel service units) and DSUs (data service units) are actually two separate devices, but they are used in conjunction and often combined into the same box. The devices are part of the hardware you need to connect computer equipment to digital transmission lines. The Channel Service Unit device connects with the digital communication line and provides a termination for the digital signal. The Data Service Unit device, sometimes called a digital service unit, is the hardware component you need to transmit digital data over the hardware channel. The device converts signals from bridges, routers and multiplexors into the bipolar digital signals used by the digital lines. Multiplexors mix voice signals and data on the same line.
Data Filtering	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 LAN side.
DCE	Data Communications Equipment is typically a modem or other type of communication device. The DCE sits between the DTE (data terminal equipment) and a transmission circuit such as a phone line.
Device Filter Rules	For Device 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.
DHCP	Dynamic Host Configuration Protocol automatically assigns IP addresses to clients when they log on. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses for a period of time which means that addresses are made available to assign to other systems.
DLCI	For Frame Relay connections, DLCI (Data Link Connection Identifier) is a path number of a portion of the PVC (the DLCI changes for each hop through the network). It is a logical identifier with local significance only and is not the address of the destination.
DNS	Domain Name System links names to IP addresses. When you access Web sites on the Internet, you can type the IP address of the site or the DNS name. When you type a domain name in a Web browser, a query is sent to the primary DNS server defined in your Web browser’s configuration dialog box. The DNS server converts the name you specified to an IP address and returns this address to your system. From then on, the IP address is used in all subsequent communications.
Domain Name	The unique name that identifies an Internet site. Domain Names always have two or more parts, separated by dots. The part on the left is the most specific and the part on the right is the most general.
DRAM	Dynamic RAM that stores information in capacitors that must be refreshed periodically.
DSL	Digital Subscriber Line technologies enhances the data capacity of the existing twisted-pair wire that runs between the local telephone company switching offices and most homes and offices. There are actually seven types of DSL service, ranging in speeds from 16 Kbits/sec to 52 Mbits/sec. The services are either symmetrical (traffic flows at the same speed in both directions), or asymmetrical (the downstream capacity is higher than the upstream capacity). DSL connections are point-to-point dedicated circuits, meaning that they are always connected. There is no dial-up. There is also no switching, which means that the line is a direct connection into the carrier’s frame relay, ATM (Asynchronous Transfer Mode), or Internet-connect system.
DSLAM	A Digital Subscriber Line Access Multiplexer (DSLAM) is a network device, usually at a telephone company central office, that receives signals from multiple customer Digital Subscriber Line connections and puts the signals on a high-speed backbone line using multiplexing techniques. Depending on the product, DSLAM multiplexers connect DSL lines with some combination of asynchronous transfer mode ATM, frame relay, or IP networks.
DTE	Originally, the DTE (data terminal equipment) was a dumb terminal or printer, but today it is a computer, or a bridge or router that interconnects local area networks.
Dual Firmware Block Structure	The Prestige 1600 employs a “dual firmware block structure” where one block is called the “main block” and the other block is called the “backup block”. You can save the current firmware into the backup block before you try to upload new firmware. If the firmware in the main block gets corrupted, the Prestige will try to boot from the backup block automatically so the service will not get interrupted.
E1	European basic multiplex rate which packs thirty voice channels into a 256 bit frame and transmitted at 2.048 Mbps.
EIR (Excess Information Rate)	This is the burst capability of the connection, i.e., the maximum allowable data transfer rate.
EMI	ElectroMagnetic Interference. The interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.
Ethernet	A very common method of networking computers in a LAN. There are a number of adaptations to the IEEE 802.3 Ethernet standard, including adaptations with data rates of 10 Mbits/sec and 100 Mbits/sec over coaxial cable, twisted-pair cable and fiber-optic cable. The latest version of Ethernet, Gigabit Ethernet, has a data rate of 1 Gbit/sec.
FAQ	(Frequently Asked Questions) -- FAQs are documents that list and answer the most common questions on a particular subject.

FCC	The FCC (Federal Communications Commission) is in charge of allocating the electromagnetic spectrum and thus the bandwidth of various communication systems.
Filters	Your Prestige uses filters to decide whether to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering.
Flash memory	The nonvolatile storage that can be electrically erased and reprogrammed so that data can be stored, booted and rewritten as necessary.
Frame Relay	Frame relay is a metropolitan and wide area networking solution that implements a form of packet-switching technology. It routes frames of information from source to destination over a switching network.
FTP	File Transfer Protocol. The Internet protocol (and program) used to transfer files between hosts.
Gateway	A gateway is a computer system or other device that acts as a translator between two systems that do not use the same communication protocols, data formatting structures, languages, and/or architecture.
HDLC	HDLC (High-level Data Link Control) is a bit-oriented (the data is monitored bit by bit), link layer protocol for the transmission of data over synchronous networks.
hop count	A measure of distance between two points on the Internet. It is equivalent to the number of gateways that separate the source and destination.
Host	Any computer on a network that is a repository for services available to other computers on the network. It is quite common to have one host machine provide several services, such as WWW and USENET.
IANA	Internet Assigned Number Authority acts as the clearinghouse to assign and coordinate the use of numerous Internet protocol parameters such as Internet addresses, domain names, protocol numbers, and more. The IANA Web site is at http://www.isi.edu/iana.
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and are not directly apparent to the application user.
IDSL	Uses ISDN transmission technology to deliver data at 128kbps into an IDSL "modem bank" connected to a router.
IGMP	IGMP (Internet Group Management Protocol) is a session-layer protocol used to establish membership in a multicast group - it is not used to carry user data.
Internet	(Lower case i) Any time you connect two or more networks together, you have an internet.
Internet	(Upper case I) The vast collection of inter-connected networks that all use the TCP/IP protocols and that evolved from the ARPANET of the late 60's and early 70's.
Intranet	A private network inside a company or organization that uses the same kinds of software that you would find on the public Internet, but that is only for internal use.
IP	Internet Protocol (currently IP version 4, or IPv4), is the underlying protocol for routing packets on the Internet and other TCP/IP-based networks.
IP Multicast	Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). IP Multicast is a third way to deliver IP packets to a group of hosts on the network - not everybody.
IP Policy Routing (IPPR)	IPPR provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis prior to the normal routing.
IPCP (PPP)	IP Control Protocol allows changes to IP parameters such as the IP address.
ISO	International Standards Organization. A voluntary, non-treaty organization founded in 1946, responsible for creating international standards in many areas, including computers and communications.
ISP	Internet Service Provider: an organization offering and providing Internet services to the public and having its own computer servers to provide the services offered.
ITU-T	International Telecommunications Union, Standardization Sector. ITU-T is the telecommunication standardization sector of ITU and is responsible for making technical

	recommendations about telephone and data (including fax) communications systems for service providers and suppliers.
LAN	Local Area Network is a shared communication system to which many computers are attached. A LAN, as its name implies, is limited to a local area. This has to do more with the electrical characteristics of the medium than the fact that many early LANs were designed for departments, although the latter accurately describes a LAN as well. LANs have different topologies, the most common being the linear bus and the star configuration.
LEC	Local Exchange Carrier: one of the new U.S. telephone access and service providers that have grown up with the recent U.S. deregulation of telecommunications.
MAC	On a local area network (LAN) or other network, the MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it is the same as your Ethernet address.) The MAC layer frames data for transmission over the network, then passes the frame to the physical layer interface where it is transmitted as a stream of bits.
NAT	Network Address Translation is the translation of an Internet Protocol address used within one network to a different IP address known within another network - see also SUA.
NAT Server Set	A NAT server set is a list of inside servers (behind NAT on the LAN) that you can make visible to the outside world.
NDIS	Network Driver Interface Specification is a Windows® specification for how communication protocol programs (such as TCP/IP) and network device drivers should communicate with each other.
Network	Any time you connect two or more computers together so that they can share resources, you have a computer network. Connect two or more networks together and you have an internet.
NIC	Network Interface Card. A board that provides network communication capabilities to and from a computer system. Also called an adapter.
Node	Any single computer connected to a network.
PAP	Password Authentication Protocol PAP is a security protocol that requires users to enter a password before accessing a secure system. The user’s name and password are sent over the wire to a server, where they are compared with a database of user account names and passwords. This technique is vulnerable to wiretapping (eavesdropping) because the password can be captured and used by someone to log onto the system.
Port	An Internet port refers to a number that is part of a URL, appearing after a colon (:) right after the domain name. Every service on an Internet server listens on a particular port number on that server. Most services have standard port numbers, e.g. Web servers normally listen on port 80.
POTS	Plain Old Telephone Service is the analog telephone service that runs over copper twisted-pair wires and is based on the original Bell telephone system. Twisted-pair wires connect homes and businesses to a neighborhood central office. This is called the local loop. The central office is connected to other central offices and long-distance facilities.
PPP	Point to Point Protocol. PPP encapsulates and transmits IP (Internet Protocol) datagrams over serial point-to-point links. PPP works with other protocols such as IPX (Internetwork Packet Exchange). The protocol is defined in IETF (Internet Engineering Task Force) RFC 1661 through 1663. PPP provides router-to-router, host-to-router and host-to-host connections.
Primary	The P1600 in primary mode provides concentration, network management, Internet access and routing functions as well as uses the FlexWan port as the interface to the trunk.
PSTN	Public Switched Telephone Network was put into place many years ago as a voice telephone call-switching system. The system transmits voice calls as analog signals across copper twisted cables from homes and businesses to neighborhood COs (central offices); this is often called the local loop. The PSTN is a circuit-switched system, meaning that an end-to-end private circuit is established between caller and callee.
PTT	The generic European name is usually used to refer to state-owned telephone companies.
PVC	Permanent Virtual Circuit. A PVC is a logical point-to-point circuit between customer sites. PVCs are low-delay circuits because routing decisions do not need to be made along the way. Permanent means that the circuit is preprogrammed by the carrier as a path through the network. It does not need to be set up or torn down for each session.
RADIUS	Remote Authentication Dial-In User Service (RADIUS). A client/server security protocol created by Livingston Enterprises. Security information is stored in a central location, known as the RADIUS server.

RADIUS Accounting	This facility logs information about dial-in connections. It can be used independently of RADIUS Authentication. It allows data to be sent at the start and the end of sessions, indicating the amount of resources (time, packets, bytes, etc.) used during the session. An ISP could use this function for special security and billing needs.
RADIUS Authentication	An external RADIUS server can provide authentication service for an unlimited number of DSL users.
RFC	An RFC (Request for Comments) is an Internet formal document or standard that is the result of committee drafting and subsequent review by interested parties. Some RFCs are informational in nature. Of those that are intended to become Internet standards, the final version of the RFC becomes the standard and no further comments or changes are permitted. Change can occur, however, through subsequent RFCs.
RIP	Routing Information Protocol is an interior or intra-domain routing protocol that uses the distance-vector routing algorithms. RIP is used on the Internet and is common in the NetWare environment as a method for exchanging routing information between routers.
RS-232	An EIA standard which is the most common way of linking data devices together.
SDSL	Symmetrical Digital Subscriber Line is a symmetrical, bi-directional DSL service that operates on one twisted-pair wire. It can provide data rates up to the T1 rate of 1.544 Mbits/sec and it operates above the voice frequency, so voice and data can be carried on the same wire.
Secondary	The P1600 secondary provides concentration, network management, Internet access and routing functions as well but only through the LAN interface.
Server	A computer, or a software package that provides a specific kind of service to client software running on other computers.
SMT	The SMT (System Management Terminal) is the interface that you use to configure your Prestige.
SNMP	System Network Management Protocol is a popular management protocol defined by the Internet community for TCP/IP networks. It is a communication protocol for collecting information from devices on the network.
Splitter	A filter to separate ADSL signals from POTS signals to prevent mutual interference.
Standalone	Standalone SMT configurations are the same as a secondary, but in this configuration mode, it does not have to work with a primary. You can connect a router to its LAN port.
STP	Twisted-pair cable consists of copper-core wires surrounded by an insulator. Two wires are twisted together to form a pair and the pair form a balanced circuit. The twisting prevents interference problems. STP (shielded twisted-pair) provides protection against external crosstalk.
Straight-through Ethernet Cable	A cable that wires a pin to its equivalent pin. This cable connects two dissimilar devices, for example, a data terminal equipment (DTE) device and a data communications equipment (DCE) device. A straight-through Ethernet cable is the most common cable used.
SUA	SUA (Single User Account) is a proprietary ZyXEL implementation of a subset of NAT that supports two types of mapping, Many-to-One and Server - see also NAT.
Subnet Mask	A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion.
SYSLOG	SYSLOG allows you to log significant system information to a remote server.
T1	Twenty-four voice channels packed into a 193 bit frame and transmitted at 1.544 Mbps. The unframed version, or payload, is 192 bits at a rate of 1.536 Mbps.
TCP	Transmission Control Protocol. The major transport protocol in the Internet suite of protocols providing reliable, connection-oriented full-duplex streams.
TCP/IP Filter Rules	TCP/IP filter rules allow you to base the rule on the fields in the IP and the upper layer protocol, e.g., UDP and TCP headers.
Telco	The generic name for telephone companies throughout the world which encompasses RBOCs, LECs and PTTs.
Telnet	The virtual terminal protocol in the Internet suite of protocols. Allows users of one host to log into a remote host and act as normal terminal users of that host.

Terminal	A device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard and a display screen and some simple circuitry.
Terminal Software	Software that pretends to be (emulates) a physical terminal and allows you to type commands to a computer somewhere else.
TFTP	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP (File Transfer Protocol), but it is scaled back in functionality so that it requires fewer resources to run. TFTP uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
UDP	UDP is a connectionless transport service that dispenses with the reliability services provided by TCP. UDP gives applications a direct interface with IP and the ability to address a particular application process running on a host via a port number without setting up a connection session.
URL	(Uniform Resource Locator) URL is an object on the Internet or an intranet that resides on a host system. Objects include directories and an assortment of file types, including text files, graphics, video and audio. A URL is the address of an object that is normally typed in the Address field of a Web browser. The URL is basically a pointer to the location of an object.
Virtual Connection (VC)	A link that seems and behaves like a dedicated point-to-point line or a system that delivers packets in sequence, as happens on an actual point-to-point network. In reality, the data is delivered across a network via the most appropriate route. The sending and receiving devices do not have to be aware of the options and the route is chosen only when a message is sent. There is no pre-arrangement, so each virtual connection exists only for the duration of that one transmission.
WAN	Wide Area Network s link geographically dispersed offices in other cities or around the globe. Just about any long-distance communication medium can serve as a WAN link, including switched and permanent telephone circuits, terrestrial radio systems and satellite systems.
WWW	(World Wide Web) - Frequently used when referring to "The Internet", WWW has two major meanings - First, loosely used: the whole constellation of resources that can be accessed using Gopher, FTP, HTTP, telnet, USENET, WAIS and some other tools. Second, the universe of hypertext servers (HTTP servers).

Index