Prestige 202H

ISDN Router

User's Guide

Version 3.40

August 2003

ZyXEL

Unleash Networking Power

Copyright

Copyright © 2003 by ZyXEL Communications Corporation.

Disclaimer

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

This publication is subject to change without notice.

Trademarks

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

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:
This device may not cause harmful interference.
This device must accept any interference received, including interference that may cause undesired operations.
This equipment has been tested and found to comply with the limits for a CLASS B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.
If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
Reorient or relocate the receiving antenna.
Increase the separation between the equipment and the receiver.
Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
Consult the dealer or an experienced radio/TV technician for help.

Notice 1

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

Certifications

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

Information for Canadian Users

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

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

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

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

Caution

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

Note

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

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two 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 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. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Online Registration

Register online registration at www.zyxel.com for free future product updates and information.

Customer Support

When you contact your customer support representative please have the following information ready:
Please have the following information ready when you contact customer support.

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

METHOD LOCATION	E-MAIL SUPPORT/SALES	TELEPHONE/FAX	WEB SITE/ FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu 300, Taiwan
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-714-632-0882 800-255-4101 +1-714-632-0858	www.zyxel.com ftp.zyxel.com	ZyXEL Communications Inc., 1650 Miraloma Avenue, Placentia, CA 92870, U.S.A.
SCANDINAVIA	support@zyxel.dk sales@zyxel.dk	+45-3955-0700 +45-3955-0707	www.zyxel.dk ftp.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen, Germany

Table of Contents

List of Figures

List of Tables

Preface

Congratulations on your purchase of the Prestige 202H ISDN router.

About This User's Manual

This manual is designed to guide you through the configuration of your Prestige for its various applications. This manual may refer to the Prestige 202H ISDN router as the Prestige.

You may use the System Management Terminal (SMT), web configurator or command interpreter interface to configure your Prestige. Not all features can be configured through all interfaces. This *User's Guide* primarily shows SMT configuration but includes the other interfaces where appropriate.

Related Documentation

- Support Disk
  Refer to the included CD for support documents.
- Quick Start Guide
  The Quick Start Guide is designed to help you get up and running right away. It contains general connection and initial configuration instructions.
- Web Configurator Online Help
  Embedded web help for descriptions of individual screens and supplementary information.
- Packing List Card
  The Packing List Card lists all items that should have come in the package.
- Certifications
  Refer to the product page at www.zyxel.com for information on product certifications.
- ZyXEL Glossary and Web Site
  Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

User Guide Feedback

Help us help you. E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

Syntax Conventions

- "Enter" means for you to type one or more characters and press the carriage return. "Select" or "Choose" means for you to use one of the predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** 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 and [SPACE BAR] means the space bar. [UP] and [DOWN] are the up and down arrow keys.
- Mouse action sequences are denoted using a comma. For example, "click the Apple icon, **Control Panels** and then **Modem**" means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity's sake, we will use "e.g." as shorthand for "for instance" and "i.e." for "that is" or "in other words" throughout this manual.

Part I:

Getting Started

This part is structured as a step-by-step guide to help you connect, install and setup your router to operate on your network and access the Internet.

Chapter 1
Getting to Know Your Prestige

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

1.1 Introducing the Prestige 202H

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

By integrating NAT, firewall, VPN capability and a four-port switch, the Prestige 202H is a complete security solution that protects your Intranet and efficiently manages data traffic on your network.

The embedded web configurator is easy to operate and totally independent of your operating system platform. You can also manage the router via the SMT (System Management Terminal), a menu-driven interface that you can access from either a terminal emulator or telnet.

1.2 Features

This section describes the router's key features.

IPSec VPN Capability

Establish Virtual Private Network (VPN) tunnels to connect (home) office computers to your company network using data encryption and the Internet; thus providing secure communications without the expense of leased site-to-site lines. The router's VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products.

Firewall

The Prestige has a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The Prestige firewall supports TCP/UDP inspection, DoS detection and protection, real time alerts, reports and logs.

4-Port Switch

A combination of switch and router makes your router a cost-effective and viable network solution. You can connect up to four computers to the router without the cost of a hub. Use a hub to add more than four computers to your LAN.

Auto-negotiating 10/100 Mbps Ethernet LAN

The LAN interfaces automatically detect if they are on a 10 or a 100 Mbps Ethernet.

Auto-crossover 10/100 Mbps Ethernet LAN

The LAN interfaces automatically adjust to either a crossover or straight-through Ethernet cable.

Call Scheduling

Configure call time periods to restrict and allow access for users on remote nodes.

Network Address Translation (NAT)

NAT (Network Address Translation - NAT, RFC 1631) allows the translation of multiple IP addresses used within one network to different IP addresses known within another network.

SNMP (Simple Network Management Protocol – Versions 1 and 2)

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

SNMP is only available if TCP/IP is configured on your router.

IP Alias

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

ISDN Data Link Connections

The router supports two types of ISDN Data Link Connections: point-to-multipoint and point-to-point.

ISDN Basic Rate Interface (BRI) Support

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

Incoming Call Support

In addition to making outgoing calls, you can configure the router to act as a remote access server for telecommuting employees.

Outgoing Data Call Bumping Support

Call bumping is a feature that allows the router to manage an MP (Multilink Protocol) bundle dynamically, dropping or reconnecting a channel in a bundle when necessary. Previously, the router did this for voice calls only, but now with this new feature, the router can drop a channel in an MP bundle if there is a data packet to another remote node.

CLID Callback Support For Dial-In Users

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

TCP/IP and PPP Support

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

Dial-on-Demand

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

PPP Multilink

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

Bandwidth-On-Demand

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

Full Network Management

- You can access the SMT (System Management Terminal) through a telnet connection.
- The embedded web configurator is an all-platform web-based utility that allows you to easily access the Prestige's management settings and configure the firewall.

Logging and Tracing

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

PAP and CHAP Security

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

DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) allows the individual client computers to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The Prestige has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to all systems that support the DHCP client. The Prestige can also act as a surrogate DHCP server (**DHCP Relay**) where it relays IP address assignment from another DHCP server to the clients.

Call Control

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

Data Compression

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

Networking Compatibility

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

Upgrade Firmware via LAN

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

1.3 Internet Access With the Prestige

These sections provide example applications for your Prestige.

1.3.1 Internet Access

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

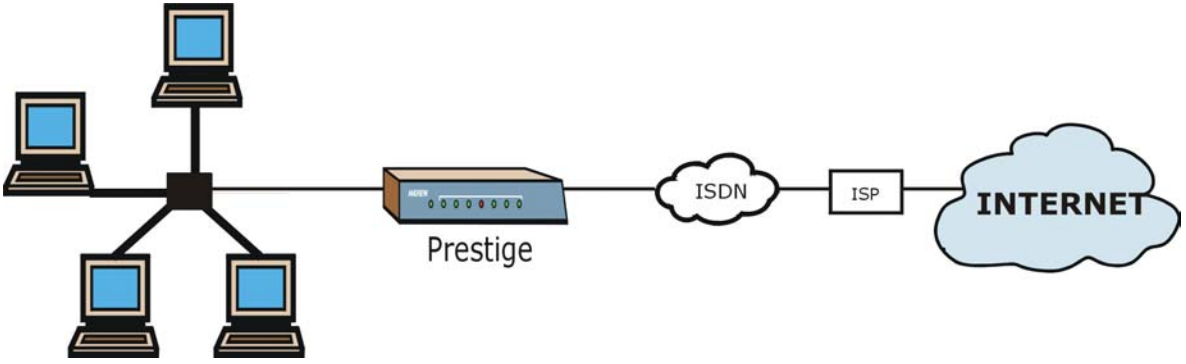


Figure 1-1 Internet Access Application

Internet Single User Account

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

1.3.2 LAN-to-LAN Connection

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

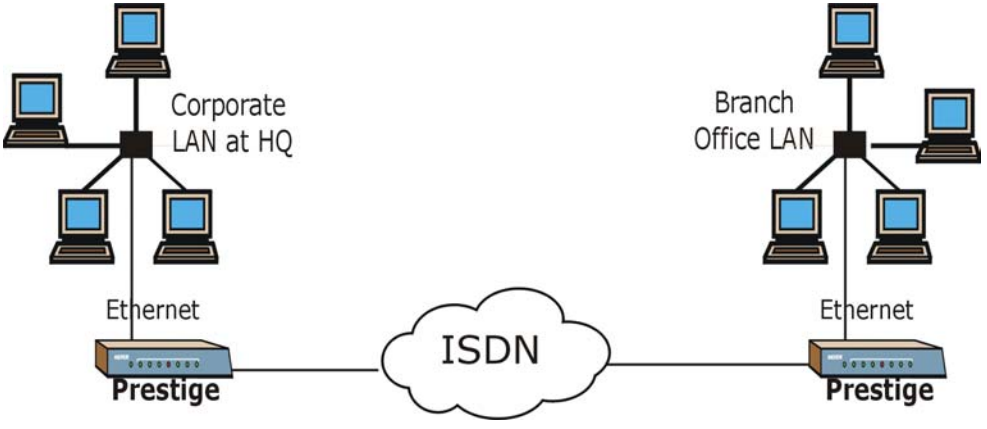


Figure 1-2 LAN-to-LAN Connection Application

1.3.3 Remote Access Server

Your router allows remote users to dial-in and gain access to your LAN. This feature enables individuals that have computers with remote access capabilities to dial in to access the network resources without physically being in the office. Either PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) authentication can be used to control remote access. You can also use callback for security and/or accounting purposes.

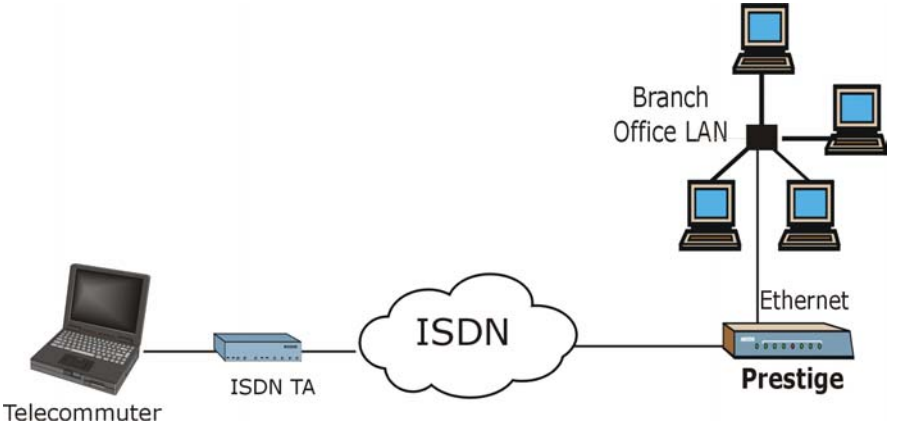


Figure 1-3 Remote Access

1.3.4 Secure Broadband Internet Access and VPN

The Prestige provides IP address sharing and a firewall-protected local network with traffic management.

Prestige VPN is an ideal cost-effective way to connect branch offices and business partners over the Internet without the need (and expense) of leased lines between sites. The LAN computers can use VPN tunnels for secure connections to remote computers.

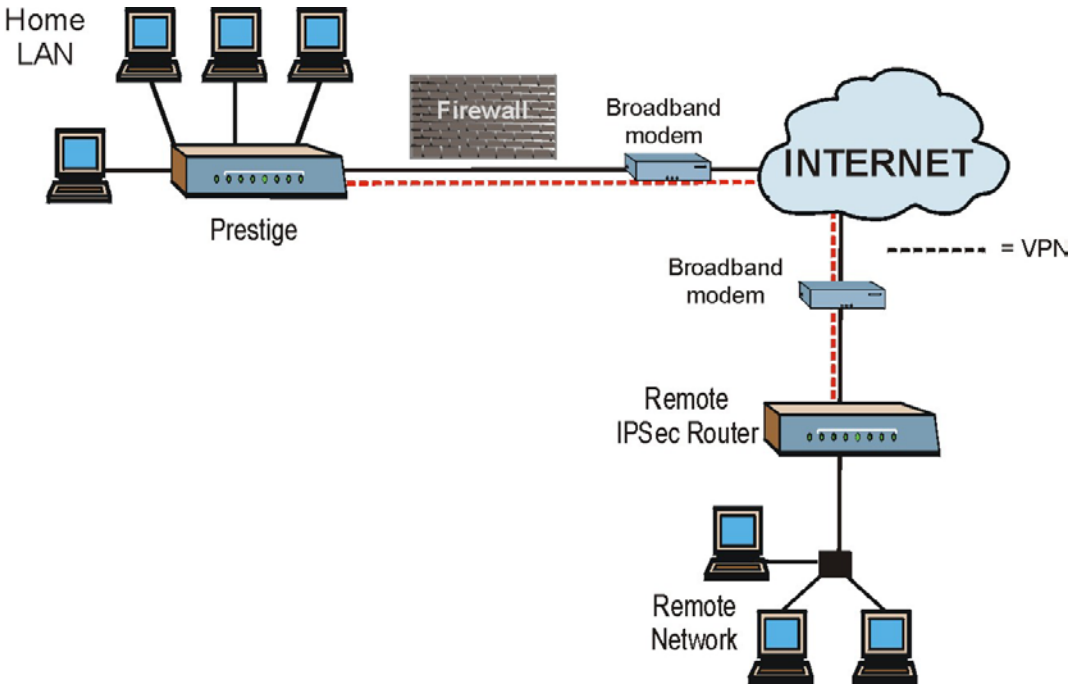


Figure 1-4 Secure Internet Access and VPN Application

Chapter 2
Hardware Installation

This chapter shows you how to make the cable connections to your router.

2.1 Front Panel

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

Figure 2-1 Front Panel

Table 2-1 LED Functions

LED	DESCRIPTION
PWR/SYS	The PWR/SYS (power/system) LED turns steady on *green* when power is applied to the router and it has boot up properly. A *green* blinking PWR/SYS LED indicates the router is performing a system test or rebooting. When the router senses low voltage power, the PWR/SYS LED turns steady on *red*.
LAN 1-4	A steady green light indicates a successful 10Mbs Ethernet connection, while an orange light indicates a successful 100Mbs connection. The LEDs will blink when data is being sent/received.
ISDN LNK, B1, B2	The LNK LED is on when the router is connected to an ISDN switch and the line has been successfully initialized. The B1 (B2) LED remains steady on when data is being sent/received on the B1 (B2) bearer channel.

2.2 Rear Panel and Connections

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

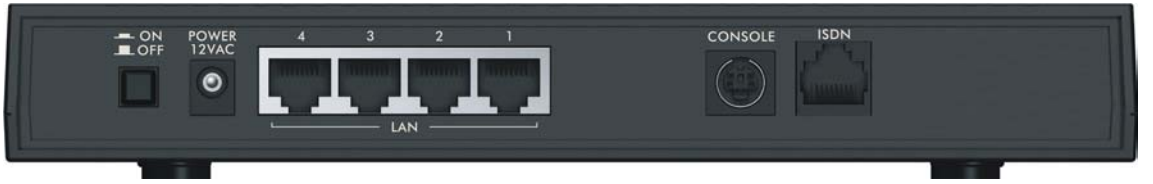


Figure 2-2 Rear Panel

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

2.2.1 Connecting the ISDN Line

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

2.2.2 Connecting the Console Port

You can configure the router via terminal emulator software on a computer that is connected it to the router through the console port. Connect the male end of the console cable to the console port of the router and the female end to a serial port (COM1, COM2 or other COM port) of your computer.

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

2.2.3 Connecting a Computer to the Router

Ethernet 10Base-T/100Base-T networks use Unshielded Twisted Pair (UTP) cable with RJ-45 connectors that look like a bigger telephone plug with 8 pins. Use crossover cable to connect your router to a computer directly or use straight-through Ethernet cable to connect to an external hub.

2.2.4 Connecting the Power Adaptor to your Router

Connect the power adaptor to the port labeled **POWER** on the rear panel of your router.

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

2.3 Turn On Your Router

At this point, you should have connected the console port, the ISDN port, the Ethernet port(s) and the power port to the appropriate devices or lines. You can now turn on the router by pushing the power button in to the on position (in is ON, out is OFF).

Chapter 3
Introducing the SMT

This chapter explains how to access the System Management Terminal and gives an overview of its menus.

3.1 Introduction to the SMT

The Prestige's SMT (System Management Terminal) is a menu-driven interface that you can access from a terminal emulator through the console port or over a telnet connection. This chapter shows you how to access the SMT (System Management Terminal) menus via console port, how to navigate the SMT and how to configure SMT menus.

3.2 Accessing the Prestige via the Console Port

Make sure you have the physical connection properly set up as described in the hardware installation chapter.

When configuring using the console port, you need a computer equipped with communications software configured to the following parameters:

- VT100 terminal emulation.
- 9600 Baud.
- No parity, 8 data bits, 1 stop bit, flow control set to none.

3.3 Initial Screen

When you turn on your router, it performs several internal tests as well as line initialization.

3.3.1 Entering the Password

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

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

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

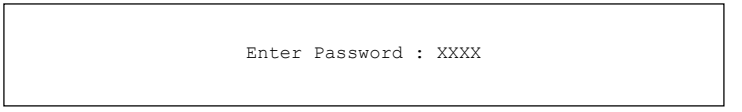


Figure 3-1 Login Screen

3.4 Navigating the SMT Interface

The SMT (System Management Terminal) interface allows you to configure and manage your router.

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

Table 3-1 Main Menu Commands

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 [SPACE BAR] to change **No** to **Yes** then press [ENTER].	Fields beginning with "Edit" lead to hidden menus and have a default setting of **No**. Press [SPACE BAR] to change **No** to **Yes**, and 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.
Entering information	Fill in, or press [SPACE BAR], then press [ENTER] to select from choices.	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<? >	All fields with the symbol <?> must be filled in order be able to save the new configuration.

Table 3-1 Main Menu Commands

OPERATION	KEYSTROKES	DESCRIPTION
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message "Press ENTER to confirm or ESC to cancel". Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

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

```
            Copyright (c) 1994 - 2003 ZyXEL Communications Corp.
                        Prestige 202H DSS1 Main Menu

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

Advanced Applications                     26. Schedule Setup
  11. Remote Node Setup                   27. VPN/IPSec Setup
  12. Static Routing Setup
  13. Default Dial-in Setup
  14. Dial-in User Setup                  99. Exit
  15. NAT Setup


                        Enter Menu Selection Number:
```

Figure 3-2 SMT Main Menu

3.4.1 System Management Terminal Interface Summary

Table 3-2 Main Menu Summary

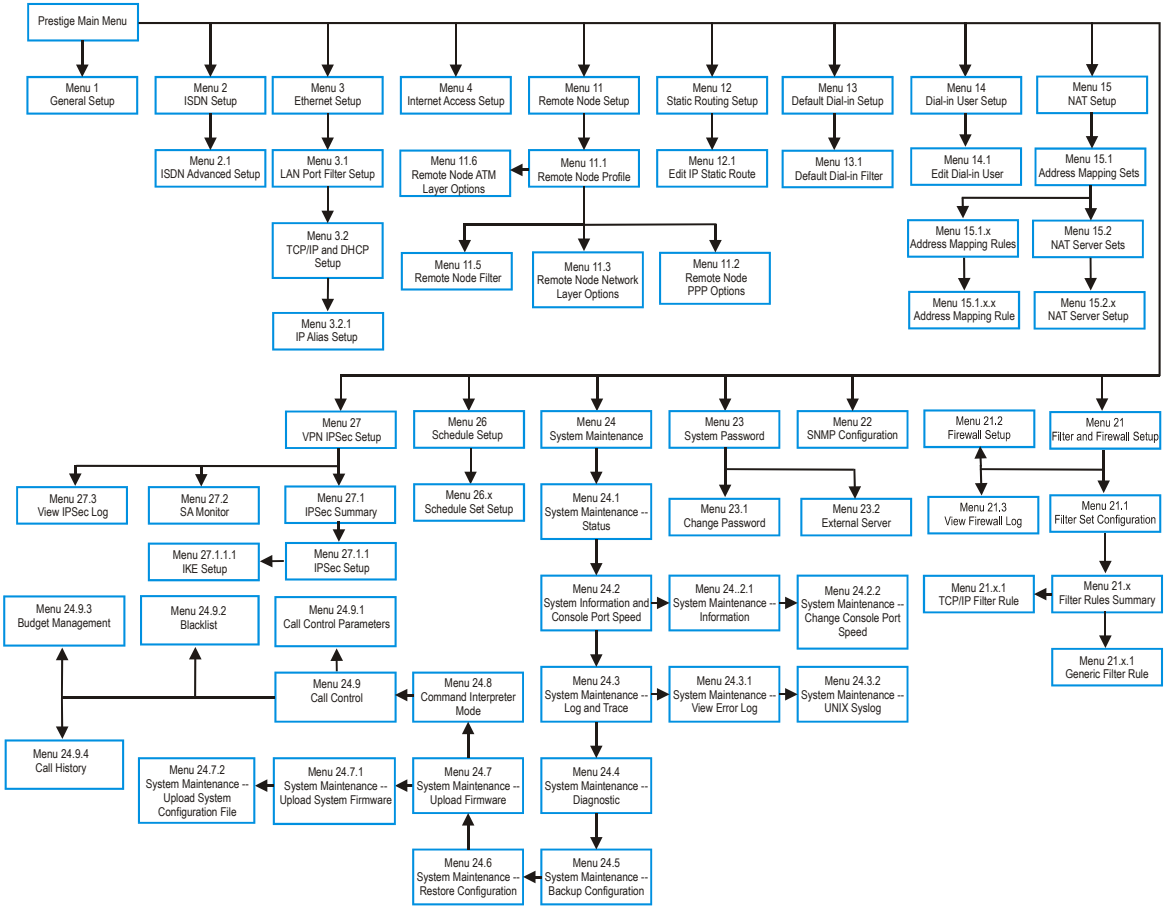
NO.	Menu Title	FUNCTION
1	General Setup	Use this menu to set up administrative information.
2	ISDN Setup	Use this menu to set up the ISDN.

Table 3-2 Main Menu Summary

NO.	Menu Title	FUNCTION
3	Ethernet Setup	Use this menu to apply LAN filters, configure LAN DHCP and TCP/IP settings and configure the wireless LAN port (not available on all models).
4	Internet Access Setup	Configure your Internet Access setup (Internet address, gateway, login, etc.) with this menu.
11	Remote Node Setup	Use this menu to configure detailed remote node settings (your ISP is also a remote node) as well as apply WAN filters.
12	Static Routing Setup	Configure IP static routes in this menu.
13	Default Dial-in Setup	Use this menu to set up default dial-in parameters so that your router can be used as a dial-in server.
14	Dial-in User Setup	Use this menu to configure settings for remote dial-in users.
15	NAT Setup	Use this menu to configure Network Address Translation.
21	Filter Set Configuration	Use this menu to setup filters to provide security, call control, etc.
22	SNMP Configuration	Use this menu to configure SNMP-related parameters.
23	System Security	Use this menu to set up security-related parameters.
24	System Maintenance	From displaying system status to uploading firmware, this menu provides comprehensive system maintenance.
26	Schedule Setup	Use this menu to schedule outgoing calls.
27	VPN /IPSec Setup	Use this menu to configure VPN connections.
99	Exit	Use this menu to exit (necessary for remote configuration).

3.5 SMT Menu Overview

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



3.6 Changing the System Password

The first thing you should do is to change the system password by performing the following steps.

Step 1. Enter 23 in the Main Menu to open **Menu 23 - System Security** as shown below.

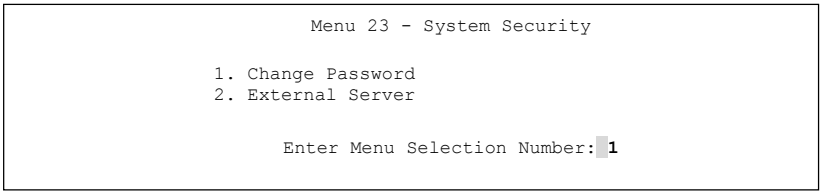


Figure 3-3 Menu 23.1 System Password

Step 2. Enter 1 in Menu 23 to open **Menu 23.1 - System Security - Change Password.**

When **Menu 23.1- System Security-Change Password** appears, as shown in the figure below, type in your existing system password, i.e., 1234, and press [ENTER].

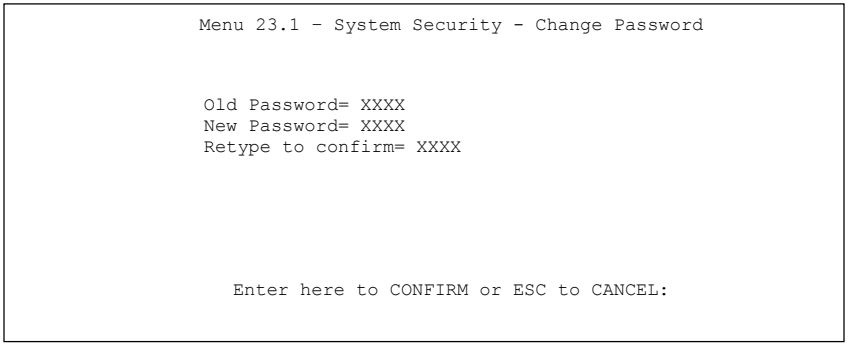


Figure 3-4 Menu 23.1 - System Security - Change Password

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

Step 4. Re-type your new system password for confirmation and press [ENTER].

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

3.7 Resetting the Prestige

If you forget your password or cannot access the SMT menu, you will need to reload the factory-default configuration file. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously 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 set to none. The password will be reset to "1234", also.

3.7.1 Uploading a Configuration File Via Console Port

Step 1. Download the default configuration file from the ZyXEL FTP site, unzip it and save it in a folder.

Step 2. Turn off the Prestige, begin a terminal emulation software session and turn on the Prestige again. When you see the message "Press Any key to enter Debug Mode within 3 seconds", press any key to enter debug mode.

Step 3. Enter "atlc" after "Enter Debug Mode" message.

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

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

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

Figure 3-5 Resetting the Router

Step 4. Wait for the "Starting XMODEM upload" message before activating Xmodem upload on your terminal. This is an example Xmodem configuration upload using HyperTerminal.

Step 5. Click **Transfer**, then **Send File** to display the following screen.

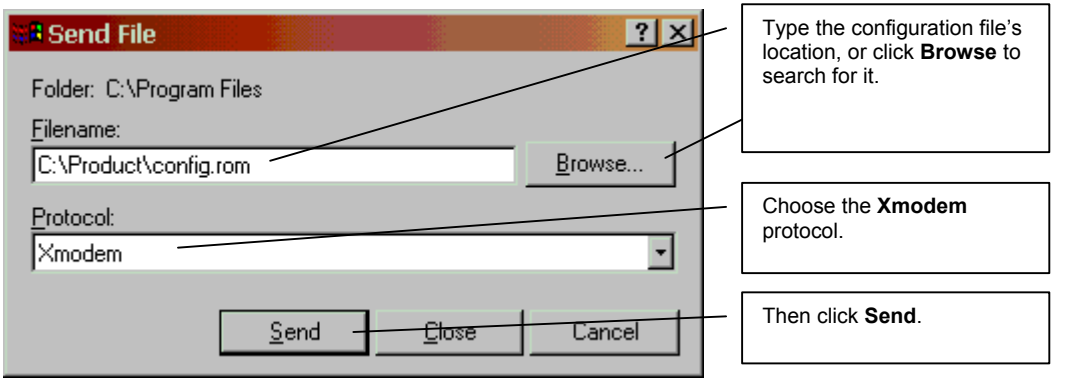


Figure 3-6 Example Xmodem Upload

Step 6. After successful firmware upload, enter "atgo" to restart the router.

Chapter 4
SMT Menu 1 General Setup

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

4.1 General Setup Overview

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

4.1.1 General Setup and System Name

General Setup contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the Prestige **System Name**.

4.2 Configuring General Setup

Enter 1 in the Main Menu to open **Menu 1 – General Setup** as shown. Fill in the required fields and turn on the individual protocols for your applications, as explained in the following table.

```
                        Menu 1 - General Setup

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



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

Figure 4-1 Menu 1 General Setup

Table 4-1 Menu 1 – General Setup

FIELD	DESCRIPTION	EXAMPLE
System Name	Choose a descriptive name, up to 30 alphanumeric characters long (no spaces, but dashes "–" and underscores "_" are accepted) for identification purposes. It is recommended you enter your computer's "Computer name" (*see section 4.1.1)* in this field. This name can be retrieved remotely via SNMP, used for CHAP authentication, and displayed at the prompt in the Command Mode.	Name
Location (optional)	Enter the geographic location (up to 31 characters) of your router.	branch
Contact Person's Name (optional)	Enter the name (up to 30 characters) of the person in charge of your router.	JohnDoe
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.		

4.3 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a DNS-like address (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a DNS name. The Dynamic DNS service provider will give you a password or key.

4.3.1 DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

4.4 Configuring Dynamic DNS

To configure Dynamic DNS, go to **Menu 1: General Setup** and press [SPACE BAR] to select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1— Configure Dynamic DNS** (shown next). Not all models have every field shown.

```
                    Menu 1.1 - Configure Dynamic DNS

Service Provider= WWW.DynDNS.ORG

Active= Yes

EMAIL=

USER=

Password= ********

Enable Wildcard= No


                Press ENTER to confirm or ESC to cancel:
```

Figure 4-2 Configure Dynamic DNS

Follow the instructions in the next table to configure Dynamic DNS parameters.

Table 4-2 Configure Dynamic DNS Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Service Provider	This is the name of your Dynamic DNS service provider.	WWW.DynDNS.ORG (default)
Active	Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active.	**Yes**
EMAIL	Enter your e-mail address.	mail@mailserver
USER	Enter your user name.	
Password	Enter the password assigned to you.	
Enable Wildcard	Your Prestige supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** This field is **N/A** when you choose DDNS client as your service provider.	**No**
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.		

Chapter 5
ISDN Setup

This chapter tells you how to configure the ISDN Setup menus for your Internet connection.

5.1 ISDN Setup Overview

Menu 2 - ISDN Setup allows you to enter the information about your ISDN line.

5.1.1 IDSN Setup

Enter 1 in the main menu to open menu 2 as shown next.

```
                    Menu 2 - ISDN Setup

Switch Type: DSS-1
B Channel Usage= Switch/Switch

Incoming Phone Numbers:
  ISDN Data     = 5551212

Edit Advanced Setup = No



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

Figure 5-1 Menu 2 ISDN Setup

Table 5-1 Menu 2 ISDN Setup

FIELD	DESCRIPTION
Switch Type	This read only field displays your switch type, DSS-1.
B Channel Usage	In general, this will be **Switch/Switch** (default). If you are only using one B channel (e.g., your router is sharing the ISDN BRI line with another device), then select **Switch/Unused**. If your second B channel is a leased line, select **Switch/Leased.** Press [SPACE BAR] to toggle through all the options. The options are below.

Table 5-1 Menu 2 ISDN Setup

FIELD	DESCRIPTION	
	♦ **Switch/Unused** ♦ **Switch/Switch** ♦ **Switch/Leased** ♦ **Leased/Switch**	♦ **Leased/Unused** ♦ **Unused/Leased** ♦ **Leased/Leased**
Telephone Number(s) IDSN Data	Enter the telephone number(s) assigned to your ISDN line by your telephone company. Some switch types only have one telephone number. Note that the router only accepts digits; please do not include '–' or spaces in this field. This field should be no longer than 25 digits.	
Edit Advanced Setup	Advanced Setup features are configured when you select **Yes** to enter **Menu 2.1-ISDN Advanced Setup** (see ahead). Refer to the Advanced Phone Services Chapter for detailed information.	
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.		

5.2 ISDN Advanced Setup Menus

Select **Yes** in the **Edit Advanced Setup** field of **Menu 2 – ISDN Setup** to display Menu 2.1 as shown later.

Switch Type

The only switch available with your Prestige is DSS-1.

Calling Line Indication

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

PABX Outside Line Prefix

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

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

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

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

Outgoing Calling Party Number

If these fields are not blank, the router will use these values as the *calling party number* for "ISDN Data", "A/B Adapter 1" and "A/B Adapter 2" outgoing calls. Otherwise, the individual entries for "ISDN Data", "A/B Adapter 1" and "A/B Adapter 2" will be used as the calling party number. You only need to fill in these fields if your switch or PABX requires a specific calling party number for outgoing calls, otherwise, leave them blank.

The following diagram illustrates the **PABX Number (with S/T Bus Number) for Loopback** and **Outgoing Calling Party Number** fields for a router behind an ISDN PABX.

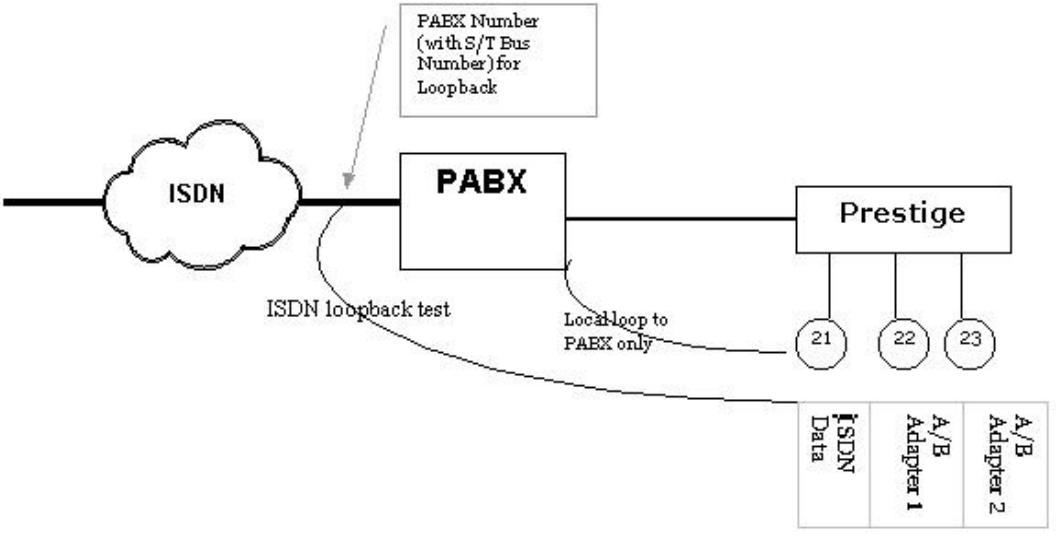


Figure 5-2 Router Behind a PABX

Data Link Connection

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

5.2.1 Configuring Advanced Setup

```
                          Menu 2.1 - ISDN Advanced Setup

Calling Line Indication= Enable

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

 Outgoing Calling Party Number:
   ISDN Data     = 80010029

 Data Link Connection= point-to-multipoint

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

Figure 5-3 Menu 2 ISDN Setup for DSS1

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

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

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

Figure 5-4 Loopback Test

5.3 NetCAPI

5.3.1 Overview

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

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

CAPI

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

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

ISDN-DCP

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

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

5.3.2 Configuring the Prestige as a NetCAPI Server

This section describes how to configure your Prestige to be a NetCAPI server.

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

The following figure illustrates the configuration used in this example.

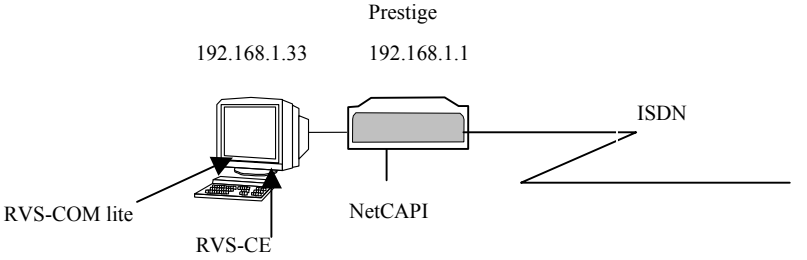


Figure 5-5 Configuration Example

Before entering any configurations, you must install the CAPI driver (RVS-CE) and communication program such as RVS-COM Lite on your computer.

5.3.3 RVS-COM

RVS-COM includes an ISDN CAPI driver with its communication program. RVS-CE (Core Engine) is an ISDN-CAPI 2.0 driver for Windows 95/98/NT that can be used by different ISDN communication programs (such as AVM Fritz or RVS-COM) to access the ISDN on the Prestige.

NetCAPI can carry out CAPI applications only if the CAPI driver is installed on your computer. In addition to the CAPI driver, you will need a communication software program such as RVS-COM Lite, Fritz etc., for users to access CAPI.

The ISDN router is a shared device and can be used by several different client computers at the same time: e.g. one computer sending a fax, another computer doing a file transfer. RVS-COM has to be installed on each client computer in order to share the ISDN lines.

Example of Installing CAPI driver and Communication Software

Please uninstall previous versions of "RVS-CAPI" and "RVS-COM lite" before you install the new versions. Click the Windows "START, Settings, Control Panel, Add/Remove Programs" to uninstall RVS-CAPI and RVS-COM.

To install the CAPI driver and the communication software, enter one of the license keys of your RVS-COM Lite CD-ROM and follow the instructions on the configuration wizard. When you install RVS-Lite, RVS-COM AUTOMATICALLY installs CAPI driver before installing RVS-Lite.

If you did not install RVS-Lite and want to use other programs such as AVM Fritz to access the ISDN router, you must first install the CAPI driver - RVS-CE using the

If you did not install RVS-Lite and want to use other programs such as AVM Fritz to access the ISDN router, you must first install the CAPI driver - RVS-CE using the English version installation wizard (in \DISKs\CEPE\DISK1\) and start the SETUP.EXE.

5.3.4 Configuring NetCAPI

Press the [SACEBAR] to select **Yes** in **Edit NetCAPI Setup** field in **Menu 2** and press [ENTER] to go to **Menu 2.2 - NetCAPI Setup**.

```
                        Menu 2.2 - NetCAPI Setup

Active= Yes

Max Number of Registered Users= 1
Incoming Data Call Number Matching= NetCAPI

Access List:
  Start IP          End IP              Operation
  192.168.1.132     192.168.1.145       Both
  192.168.14.1      192.168.14.32       Imcoming
  192.168.20.7      192.168.20.12       Outgoing
  192.168.30.1      192.168.30.3        Both
  10.0.0.0          10.255.255.255      Incoming
  ________________  ____________        _______
  ________________  ____________        _______
  ________________  ____________        _______
  default                               Both

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

Figure 5-6 Menu 2.2 NetCAPI Setup

The following table describes the fields in this screen.

Table 5-2 Configuring NetCAPI

FIELD	DESCRIPTION
Active	This field allows you to enable or disable NetCAPI. Press the [SPACEBAR] to select **Yes** or **No**

Table 5-2 Configuring NetCAPI

FIELD	DESCRIPTION
Max Number of Registered Users	When you want to use NetCAPI to place outgoing calls or to listen to incoming calls, you must start RVSCOM on your computer, and RVSCOM will register itself to the Prestige. This option is the maximum number of clients that the Prestige supports at the same time. The default value is **4**.
Incoming Data Call Number Matching	This field determines how incoming calls are routed. Select **NetCAPI** if you want to direct all incoming data calls to NetCAPI. Select **Subscriber Number (MSN)** if you want to direct all incoming call to the Prestige only when the incoming phone number matches the ISDN DATA number. If the incoming phone number does not match the ISDN DATA number, then the call will be routed to NetCAPI. Select **Called Party Subaddress** if you want to direct all incoming calls to the Prestige only when the incoming call matches the subaddress of ISDN DATA. If the incoming call does not match the subaddress of ISDN DATA, then the call will be routed to NetCAPI.
Start IP	Refers to the first IP address of a group of NetCAPI clients. Each group contains contiguous IP addresses
End IP	Refers to the last IP address in a NetCAPI client group.
Operation	Select **Incoming** if you wish to grant incoming calls permission. Select **Outgoing** if you wish to grant outgoing calls permission. Select **Both** if you wish to grant both incoming calls and outgoing calls permissions. Select **None** if you wish to deny all calls.
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.	

Chapter 6
Ethernet Setup

This chapter shows you how to configure the LAN settings for your Prestige.

6.1 Ethernet Setup

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

```
                    Menu 3 - Ethernet Setup

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

                    Enter Menu Selection Number:
```

Figure 6-1 Menu 3 Ethernet Setup

6.1.1 General Ethernet Setup

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

```
                Menu 3.1 - General Ethernet Setup

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

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

Figure 6-2 Menu 3.1 General Ethernet Setup

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

6.2 Ethernet TCP/IP and DHCP Server

The Prestige has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability. For remote node TCP/IP configuration, refer to the chapter on Remote Node Configuration.

6.2.1 Factory Ethernet Defaults

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

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

These parameters should work for the majority of installations. If the parameters are satisfactory, you can skip to section *6.3* to enter the DNS server address(es) if your ISP gives you explicit DNS server address(es).

6.2.2 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the Prestige. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your Prestige, but make sure that no other device on your network is using that IP address.

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

6.2.3 Private IP Addresses

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

Table 6-1 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

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

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

6.2.4 RIP Setup

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

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

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

By default, **RIP direction** is set to **Both** and the **Version** set to **RIP-1**.

6.2.5 DHCP Configuration

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The router has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to Windows® 95, Windows® NT and other systems that support the DHCP client. The router can also act as a surrogate DHCP server where it relays IP address assignment from the actual DHCP server to the clients.

IP Pool Setup

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

DNS Server Address

DNS (Domain Name System) maps 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 computer before you can access it.

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

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

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

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

6.3 Configuring TCP/IP Ethernet and DHCP

You will now use **Menu 3.2-TCP/IP and DHCP Ethernet Setup** to configure your router for TCP/IP.

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

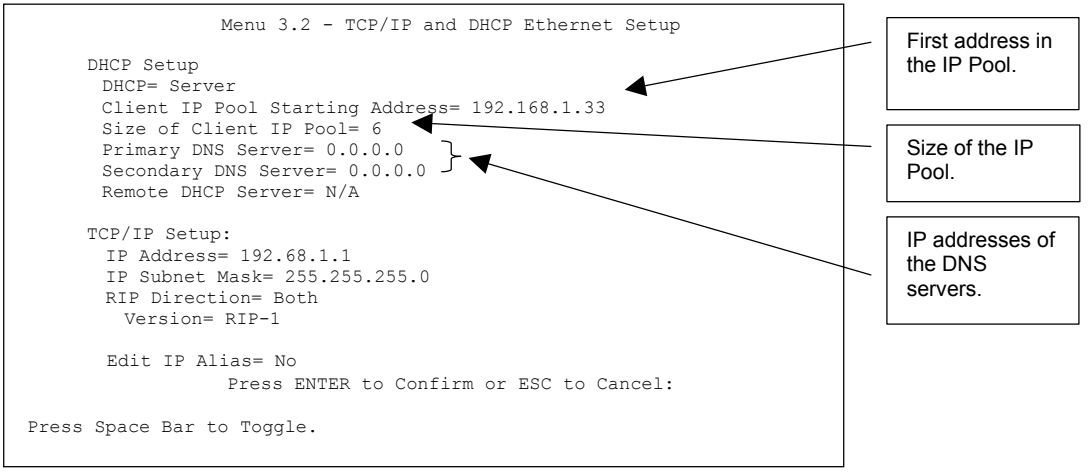


Figure 6-3 Menu 3.2 TCP/IP and DHCP Ethernet Setup

Table 6-2 Menu 3.2 TCP/IP and DHCP Ethernet Setup

FIELD	DESCRIPTION	EXAMPLE
DHCP Setup		
DHCP	This field enables/disables the DHCP server. If set to **Server**, your router will act as a DHCP server. If set to **None**, the DHCP server will be disabled. If set to **Relay,** the router acts as a surrogate DHCP server and relays requests and responses between the remote server and the clients. When set to **Server**, the following four items need to be set:	**Server** (default)
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size, or count of the IP address pool.	6

Table 6-2 Menu 3.2 TCP/IP and DHCP Ethernet Setup

FIELD	DESCRIPTION	EXAMPLE
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	
Remote DHCP Server	If **Relay** is selected in the **DHCP** field above, then enter the IP address of the actual, remote DHCP server here.	

Use the instructions in the following table to configure TCP/IP parameters for the LAN port.

Table 6-3 TCP/IP Ethernet Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
TCP/IP Setup		
IP Address	Enter the IP address of your router in dotted decimal notation.	192.168.1.1 (default)
IP Subnet Mask	Your router will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the router.	255.255.255.0
RIP Direction	Press [SPACE BAR] to select the RIP direction from **Both/None/In Only/ Out Only.**	**Both** (default)
Version	Press [SPACE BAR] to select the RIP version from **RIP-1/RIP-2B/ RIP-2M.**	**RIP-1** (default)
Edit IP Alias	The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network. Press [SPACE BAR] to select **Yes** and then press [ENTER] to display menu 3.2.1	**Yes**
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.		

6.4 IP Alias

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

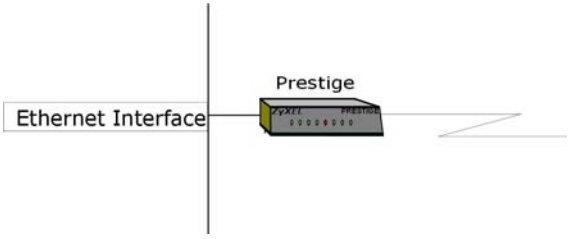


Figure 6-4 Physical Network ➔

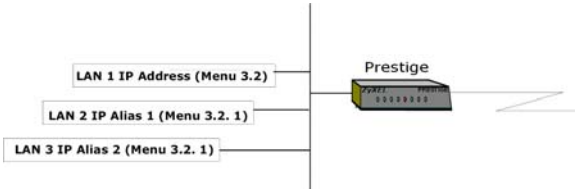


Figure 6-5 Partitioned Logical Networks

Use menu 3.2.1 to configure IP Alias on your router.

6.5 IP Alias Setup

You must use menu 3.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.

Press [ENTER] to open **Menu 3.2.1 - IP Alias Setup**, as shown next.

```
                        Menu 3.2.1 - IP Alias Setup

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

                     Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 6-6 Menu 3.2.1 IP Alias Setup

Table 6-4 IP Menu 3.2.1 – IP Alias Setup

FIELD	DESCRIPTION	EXAMPLE
IP Alias 1 or 2	Choose **Yes** to configure the LAN network for the router.	**Yes**
IP Address	Enter the IP address of your router in dotted decimal notation.	**192.168.2.1**
IP Subnet Mask	Your router will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the router.	**255.255.255.0**
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction from **Both/In Only/Out Only.**	**Both**
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1/RIP-2B/RIP-2M.**	**RIP-1**
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the router.	
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the router.	
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.		

Chapter 7
Internet Access Setup

This chapter shows you how to configure your router for Internet access

7.1 Internet Access Overview

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

Table 7-1 Internet Account Information

INTERNET ACCOUNT INFORMATION
Your device's WAN IP Address (if given): _____
DNS Server IP Address (if given): Primary _____, Secondary _____
Your ISDN Phone Number: _____
ISP Name: _____
ISP Telephone Number: _____
Login Name: _____
Password: _____
DNS Server Address(es): _____

From the Main Menu, enter option **Internet Access Setup** to go to **Menu 4 – Internet Access Setup**, as shown in the following figure.

7.2 Internet Access Setup

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

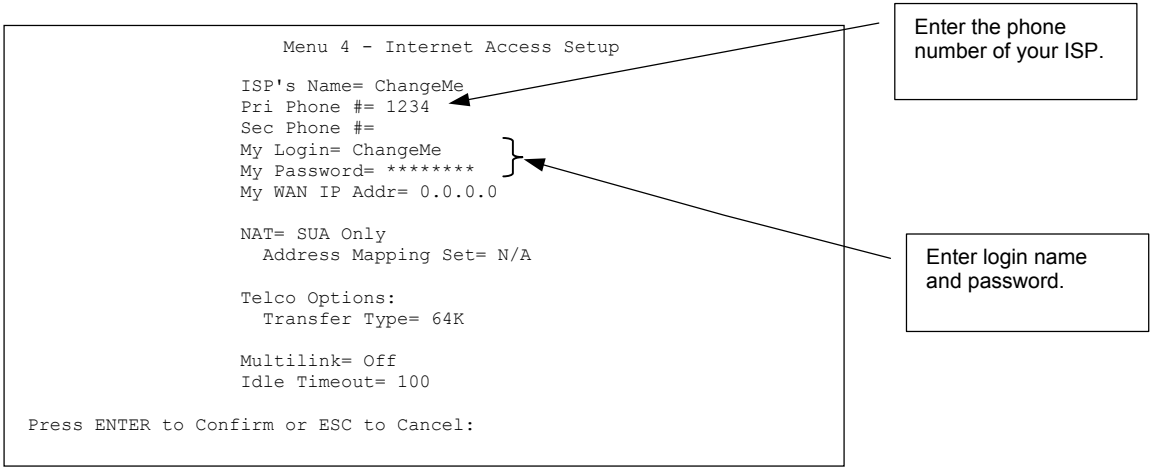


Figure 7-1 Menu 4 Internet Access Setup

Table 7-2 Menu 4 Internet Access Setup

FIELD	DESCRIPTION
ISP's Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.
Pri Phone and Sec Phone #	Both the Primary and the Secondary Phone number refer to the number that the router dials to connect to the ISP.
My Login	Enter the login name given to you by your ISP.
My Password	Enter the password associated with the login name above.
My WAN IP Addr	Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your router. NOTE: This is the address assigned to your local router WAN, not the remote router. If the remote router is a router, then this entry determines the local router **Rem IP Addr** in Menu 11.1.

Table 7-2 Menu 4 Internet Access Setup

FIELD	DESCRIPTION
NAT	Choose from **None**, **Full Feature** or **SUA Only**. When you select **Full Feature** you must configure at least one address mapping set. See the chapter on NAT for a full discussion of this new feature.
Address Mapping Set	A NAT Server Set is a list of LAN side servers mapped to external ports (similar to the old SUA menu). You may enter any server set number up to 10, but the first one is used for SUA only.
Telco options: Transfer Type	This field specifies the type of connection between the router and this remote node. Select 64K, or Leased.
Multilink	The router uses the PPP Multilink Protocol (PPP/MP) to bundle multiple links in a single connection to boost the effective throughput between two nodes. This option is only available if the transfer type is 64K. Options for this field are: **Off**, **BOD** and **Always**.
Idle Timeout	This value specifies the number of idle seconds that elapses before the remote node is automatically disconnected. Idle seconds is the period of time when no data is transmitted from your router. Administrative packets such as RIP are not counted as data.

Idle Timeout only applies when the router initiates the call.

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

Part II:

Advanced Applications

This part describes the advanced applications of your Prestige, such as Remote Node Configuration, Dial-in Configuration and NAT.

Chapter 8
Remote Node Configuration

This chapter covers the configuration of remote nodes.

8.1 Remote Node Overview

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use Menu 4 to set up Internet access, you are actually configuring one of the remote nodes. Once a remote node is configured correctly, traffic to the remote network will trigger your Prestige to make a call automatically, i.e., Dial on Demand.

8.1.1 Minimum Toll Period

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

8.2 Remote Node Setup

To configure a remote node, follow these steps:

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

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

```
                        Menu 11 - Remote Node Setup


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

Enter Node # to Edit:
```

Figure 8-1 Menu 11 Remote Node Setup

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

```
                    Menu 11.1 - Remote Node Profile

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

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

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

Edit PPP Options in menu 11.2.

Edit IP Options in menu 11.3.

Edit Filter Sets in menu 11.5.

Figure 8-2 Menu 11.1 Remote Node Profile

Table 8-1 Menu 11.1 Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	This is a required field [?]. Enter a descriptive name for the remote node, for example, Corp. This field can be up to eight characters. This name must be unique from any other remote node name or remote dial-in user name.	
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** (activate remote node) or **No** (deactivate remote node).	**Yes**
Call Direction	If this parameter is set to **Both**, your Prestige can both place and receive calls to/from this remote node. If set to **Incoming**, your Prestige will not place a call to this remote node. If set to **Outgoing**, your Prestige will drop any incoming calls from this remote node. Several other fields in this menu depend on this parameter. For example, in order to enable **Callback**, the **Call Direction** must be set to **Both**.	**Outgoing**
Incoming: Rem Login	Enter the login name that this remote node will use when it calls your Prestige. The login name in this field combined with the Rem Password will be used to authenticate this node.	
Rem Password	Enter the password used when this remote node calls your Prestige.	
Rem CLID	This field is applicable only if **Call Direction** is either set to **Both** or **Incoming**. Otherwise, a **N/A** appears in the field. This is the Calling Line ID (the telephone number of the calling party) of this remote node. If you enable the CLID Authen field in Menu 13 – Default Dial-In Setup, your Prestige will check the CLID in the incoming call against the CLIDs in the database. If no match is found and CLID Authen is set to Required, the call will be dropped.	

Table 8-1 Menu 11.1 Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Call Back	This field is applicable only if **Call Direction** is set to **Both**. Otherwise, a **N/A** appears in the field. This field determines whether or not your Prestige will call back after receiving a call from this remote node. If this option is enabled, your Prestige will disconnect the initial call from this node and call it back at the Outgoing Primary Phone Number (see section *10.4 Callback Overview*).	**Yes**
Outgoing: My Login	This is a required field [?] if **Call Direction** is either **Both** or **Outgoing**. Enter the login name for your Prestige when it calls this remote node.	
My Password	This is a required field [?] if **Call Direction** is either **Both** or **Outgoing**. Enter the password for your Prestige when it calls this remote node.	
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP/PAP** – Your Prestige will accept either CHAP or PAP when requested by this remote node. **CHAP** – accept CHAP only. **PAP** – accept PAP only.	**CHAP/PAP**
Pri(mary) Sec(ondary) Phone #	Your Prestige always calls this remote node using the Primary Phone number first for a dial-up line. If the Primary Phone number is busy or does not answer, your Prestige will dial the Secondary Phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. A # symbol may be included at the beginning of the phone numbers as required.	
Edit PPP Options	To edit the PPP options for this remote node, move the cursor to this field. Press [SPACE BAR] and then [ENTER] 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 *section 8.6*.	**No**
Rem IP Addr	This is a required field [?] if **Route** is set to **IP**. Enter the IP address of the remote gateway.	
Edit IP	Press [SPACE BAR] to select **Yes** and press [ENTER] to go to Menu 11.3 – Remote Node Network Layer Options.	**No**

Table 8-1 Menu 11.1 Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Telco Options: Transfer Type	This field specifies the type of connection between the Prestige and this remote node. When set to **Leased**, the **Allocated Budget** and **Period** do not apply.	**64k**
Allocated Budget (min)	This field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 for no budget control.	Default = **0**
Period (hr)	This field sets the time interval to reset the above outgoing call budget control.	
Schedules	Apply up to 4 schedule sets, separated by commas to your remote node here. Please see ahead for a full discussion on schedules.	
Carrier Access Code	In some European countries, you need to enter the access code number of your preferred telecommunications service provider. Your telephone company should supply you with this number.	
Nailed-up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. See the following section for more details.	**No**
Toll Period	This is the basic unit of time for charging purposes, e.g., 25 cents every 3 minutes – 3 minutes is the Toll Period.	
Session Options: Edit Filter Sets	Press [SPACE BAR] and then [ENTER] to select **Yes** to open Menu 11.5 to edit the filter sets. See the Remote Node Filter section for more details.	Default = **No**
Idle Timeout (sec)	This value specifies the number of idle seconds that elapses before the remote node is automatically disconnected. Idle seconds is the period of time when no data is transmitted from your Prestige. Administrative packets such as RIP are not counted as data. The default is 300 seconds (5 minutes). Idle timeout only applies when the Prestige initiates the call**.** 0 sec means the remote node will never be automatically disconnected.	Default = 300 secs
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.		

8.3 Outgoing Authentication Protocol

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

8.4 PPP Multilink

The Prestige uses the PPP Multilink Protocol (PPP/MP) to bundle multiple links in a single connection to boost the effective throughput between two nodes.

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

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

8.5 Bandwidth on Demand

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

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

Table 8-2 BTR vs MTR for BOD

BTR AND M' R SETTING	No. of :hannel(s) sed	Ma No. of Chanr el(s) Used	BANDWI)TH ON DEM ND
BTR = 64, MTR = 64	1	1	Off
BTR = 64, MTR = 128	1	2	On
BTR = 128, MTR = 128	2	2	Off

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

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

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

8.6 Editing PPP Options

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

```
                    Menu 11.2 - Remote Node PPP Options

                Encapsulation= Standard PPP
                Compression= No
                BACP= Enable

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

                  Add Persist(sec)= 5
                  Subtract Persist(sec)= 5


                 Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 8-3 Menu 11.2 Remote Node PPP Options

Table 8-3 Menu 11.2 Remote Node PPP Options

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Select **CISCO PPP** only when this remote node is a Cisco machine; otherwise, select **Standard PPP**.	**Standard PPP**
Compression	Turn on/off Stac Compression. The default for this field is **No**.	**No**
BACP	Your Prestige negotiates the Secondary Phone number for a dial-up line from the peer when BACP (Bandwidth Allocation Control Protocol) is enabled; otherwise it uses the Secondary Phone number set in Menu 11.1.	**Enable** (default)
Multiple Link Options:		
BOD Calculation	Select the direction of the traffic you wish to use in determining when to add or subtract a link. Options for this field are: **Transmit or Receive**, **Transmit**, **Receive**.	**Transmit or Receive** (default**)**
Base Trans Rate (Kbps)	Select the base data transfer rate for this remote node in Kbps. There are two choices for this field: **64** where only one channel is used or, **128** where two channels are used as soon as a packet triggers a call.	**64**
Max Trans Rate (Kbps)	Enter the maximum data transfer rate allowed for this remote node. This parameter is in kilobits per second.	**64**

Table 8-3 Menu 11.2 Remote Node PPP Options

Target Utility (Kbps)	Enter the two thresholds separated by a [–] for subtracting and adding the second port.	Default = **32–48**
Add Persist	This parameter specifies the number of seconds where traffic is above the adding threshold before the Prestige will bring up the second link.	Default = **5** sec
Subtract Persist	This parameter specifies the number of seconds where traffic is below the subtraction threshold before your Prestige drops the second link.	Default = **5** sec
Once you have configured this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

8.7 LAN-to-LAN Application

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

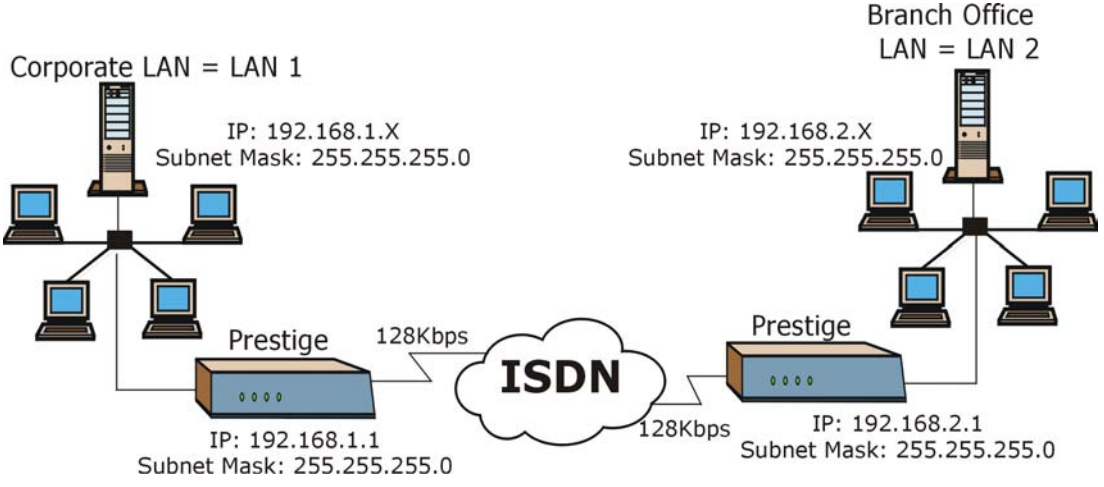


Figure 8-4 TCP/IP LAN-to-LAN Application

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

LAN 1 Setup

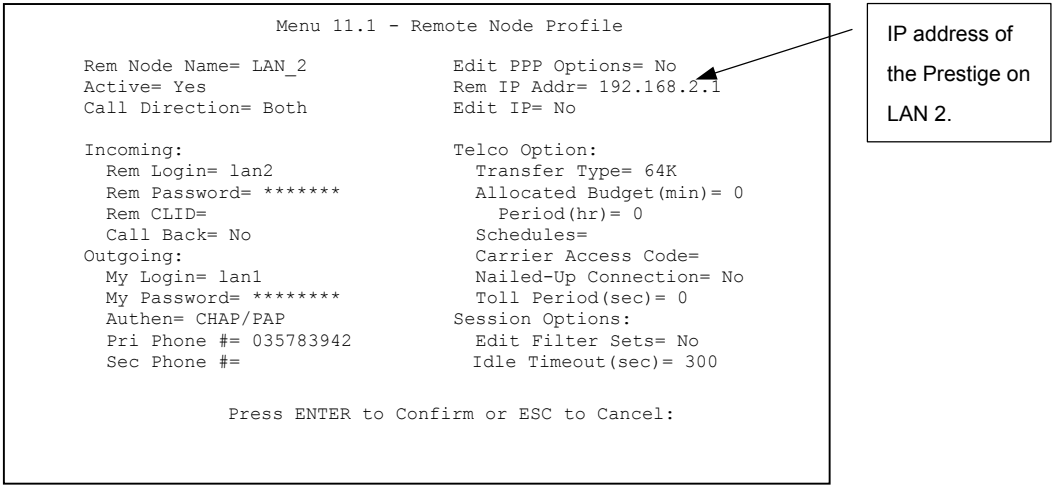


Figure 8-5 LAN 1 Setup

LAN 2 Setup

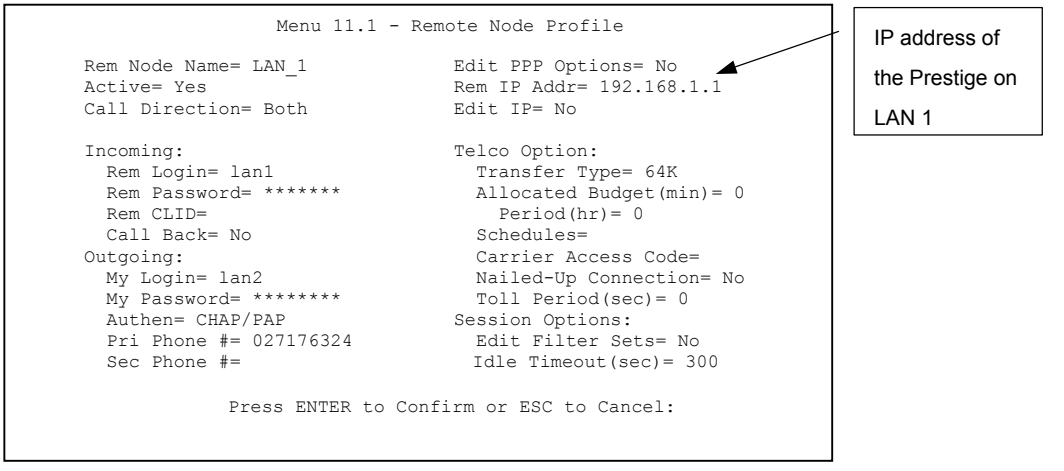


Figure 8-6 LAN 2 Setup

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

8.8 Configuring Network Layer Options

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

Step 1. To configure the TCP/IP parameters of a remote node, first configure the three fields in **Menu 11.1 – Remote Node Profile**, as shown in the following table.

Table 8-4 TCP/IP-related Fields in Remote Node Profile

FIELD	DESCRIPTION
Rem IP Addr	Enter the IP address of the remote gateway in **Menu 11.1 – Remote Node Profile**. You must fill in either the remote Prestige WAN IP address or the remote Prestige LAN IP address. This depends on the remote router's WAN IP i.e., for the (remote) Prestige, the **My WAN IP Addr** settings in **Menu 4**. For example, if the remote WAN IP is set to 172.16.0.2 (the remote router's WAN IP), then you should enter 172.16.0.2 in the **Rem IP Add** field. If the remote WAN IP is 0.0.0.0, then enter 192.168.1.1(the remote router's LAN IP) in the **Rem IP Addr** field).
Edit IP	Press [SPACE BAR] and then [ENTER] to select **Yes** and press [ENTER] to go to Menu 11.3 – Remote Node Network Layer Options menu.

Step 2. Move the cursor to the **Edit IP** field in **Menu 11** – **Remote Node Profile**, and then press [SPACE BAR] to toggle and set the value to **Yes**. Press [ENTER] to open **Menu 11.3** – **Network Layer Options**.

```
            Menu 11.3 - Remote Node Network Layer Options

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

          NAT= None
            Address Mapping Set= Full Feature

          Metric= 2
          Private= No
          RIP Direction= Both
            Version= RIP-2B

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

Table 8-5 Remote Node Network Layer Options

Table 8-6 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
Rem IP Addr	This will show the IP address you entered for this remote node in the previous menu.	
Rem Subnet Mask	Enter the subnet mask for the remote network.	
My WAN Addr	Some implementations, especially the UNIX derivatives, require the ISDN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the ISDN port of your Prestige. **NOTE**: This is the address assigned to your local Prestige WAN, not the remote router. If the remote router is a Prestige, then this entry determines the local Prestige **Rem IP Addr** in Menu 11.1.	
NAT Address Mapping Set	Choose from **None**, **Full Feature**, or **SUA Only**. When you select **Full Feature** you must configure at least one address mapping set! For more information about NAT and the choices listed refer to the NAT Chapter. A NAT Server Set is a list of LAN side servers mapped to external ports (similar to the old SUA Menu 15.1 before). You may enter any server set number up to 10 but the first one is used for SUA only.	**Full Feature**

Table 8-6 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	**2**
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.	**No**
RIP Direction	Press [SPACE BAR] and then [ENTER] to select from **Both**/**In Only**/**Out Only/None**.	**None** (default)
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1/RIP-2B/RIP-2M.**	**RIP-2B** (default)
Once you have completed filling in **Menu 11.3 Remote Node Network Layer Options**, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11, or press [ESC] at any time to cancel.		

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

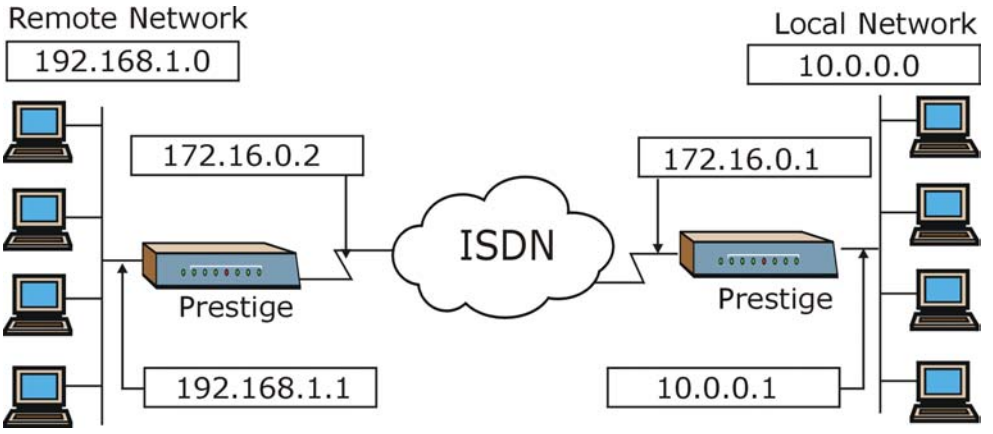


Figure 8-7 Sample IP Addresses for LAN-to-LAN Connection

8.9 Configuring Filter

Use **Menu 11.5 – Remote Node Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige and also to preve.nt certain packets from triggering calls. You can specify up to 4 filter sets separated by comma, e.g., 1, 5, 9, 12, in each **filter** field. The default is no filters.

Note that spaces are accepted in this field. The Prestige comes with a prepackaged filter set, NetBIOS_WAN, that blocks NetBIOS packets (call protocol filter = 1). You can include this in the call filter sets if you wish to prevent NetBIOS packets from triggering calls to a remote node.

To specify remote node filters, move the cursor to the **Edit Filter Sets** field in **Menu 11.1** – **Remote Node Profile**, and use [SPACE BAR] to select **Yes**. Press [ENTER] to open Menu 11.5, as shown next.

```
                Menu 11.5 - Remote Node Filter

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

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

Figure 8-8 Menu 11.5 Remote Node Filter

Chapter 9
Static Route Setup

This chapter shows how to set up static routes.

9.1 Static Route Overview

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

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

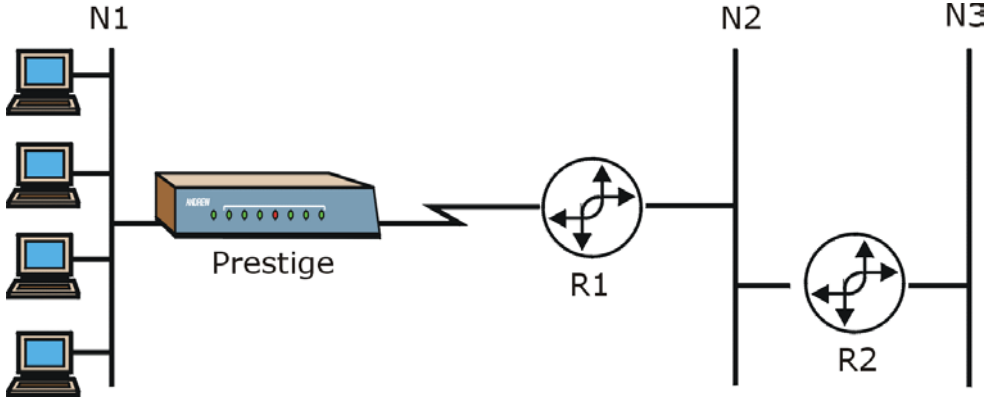


Figure 9-1 Sample Static Routing Topology

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

```
                Menu 12 - IP Static Route Setup

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

                  Enter selection number:
```

Figure 9-2 Menu 12 IP Static Route Setup

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

```
            Menu 12.1 - Edit IP Static Route


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

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

Figure 9-3 Menu 12.1 Edit IP Static Route

Table 9-1 Menu 12.1 Edit IP Static Route

FIELD	DESCRIPTION
Route Name	Enter a descriptive name for this route. This is for identification purposes only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.

Table 9-1 Menu 12.1 Edit IP Static Route

FIELD	DESCRIPTION
IP Subnet Mask	Enter the subnet mask for this destination. Follow the discussion on IP subnet mask in this chapter.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Prestige that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Prestige; over WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and is not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
Once you have completed filling in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel.	

Chapter 10
Dial-in Setup

This chapter shows you how to configure your Prestige to receive calls from remote dial-in users including telecommuters and remote nodes. This is done in SMT menus 13 and 14.

10.1 Dial-in Users Overview

There are several differences between dial-in users and remote nodes, as summarized in the next table.

Table 10-1 Remote Dial-in Users/Remote Nodes Comparison Chart

REMOTE DIAL-IN USERS	REMOTE NODES
Your Prestige will only answer calls from remote dial-in users; it will not make calls to them.	Your Prestige can make calls to and receive calls from the remote node.
All remote dial-in users share one common set of parameters, as defined in the **Menu 14 Default Dial-in User Setup**.	Each remote node can have its own set of parameters such as Bandwidth On Demand, Protocol, Security, etc.

10.2 Default Dial-in User Setup

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

10.2.1 CLID Callback Support For Dial-In Users

CLID (Calling Line IDentification) authentication affords you the security of limiting a user to only initiate connections from a fixed location. The Prestige uses the caller ID sent by the switch to match against the CLIDs in the database. Please note that for CLID authentication to work on the Prestige, your telephone company must support caller ID. If the remote node requires mutual authentication, please fill in the **O/G Username** and **O/G Password** fields. You must also fill in these fields when a dial-in user to whom we are calling back requests authentication.

10.3 Setting Up Default Dial-in

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

```
                    Menu 13 - Default Dial-in Setup

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

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

                Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 10-1 Menu 13 Default Dial-in Setup

Table 10-2 Menu 13 Default Dial-in Setup

FIELD	DESCRIPTION	EXAMPLE
Telco Options: CLID Authen	This field sets the CLID authentication parameter for all incoming calls. There are three options for this field: **None** – No CLID is required. **Required** – CLID must be available, or the Prestige will not answer the call. **Preferred** – If the CLID is available then CLID will be used; otherwise, authentication is performed in PPP negotiation.	**Required**
PPP Options:		

Table 10-2 Menu 13 Default Dial-in Setup

FIELD	DESCRIPTION	EXAMPLE
Recv Authen	This field sets the authentication protocol for incoming calls. For security reason, setting authentication to **None** is strongly discouraged. Options for this field are: **CHAP/PAP** – Your Prestige will try CHAP first, but PAP will be used if CHAP is not available. **CHAP** – Use CHAP only. **PAP** – Use PAP only. **None** – Your Prestige tries to acquire CHAP/PAP first, but no authentication is required if CHAP/PAP is not available.	**CHAP/PAP**
Compression	Turn on/off Stac Compression. The default for this field is **No**.	**Yes**
Mutual Authen	Some vendors, e.g., Cisco, require mutual authentication, i.e., the node that initiates the call will request a user name and password from the far end that it is dialing to. If the remote node requires mutual authentication, set this field to **Yes**.	**No**
O/G Username	Enter the login name to be used to respond to the peer's authentication request.	
O/G Password	Enter the outgoing password to be used to respond to the peer's authentication request.	
Multiple Link Options:		
Max Trans Rate(Kbps)	Enter the maximum data transfer rate between your Prestige and the remote dial-in user. 64 – At most, one B channel is used. 128 – A maximum of two channels can be used. When the Prestige calls back to the remote dial-in user, the maximum data transfer rate is always 64.	128
Callback Budget Management:		
Allocated Budget (min)	This field sets the budget callback time for all the remote dial-in users. The default for this field is **0** for no budget control.	**0** (default)
Period (hr)	This field sets the time interval to reset the above callback budget control.	
IP Address Supplied By:		

Table 10-2 Menu 13 Default Dial-in Setup

FIELD	DESCRIPTION	EXAMPLE
Dial-in User	If set to **Yes**, the Prestige will allow a remote host to specify its own IP address. If set to **No**, the remote host must use the IP address assigned by your Prestige from the IP pool, configured below. This is to prevent the remote host from using an invalid IP address and potentially disrupting the whole network.	**Yes** (default)
IP Pool	This field tells your Prestige to provide the remote host with an IP address from the pool. This field is required if **Dial-In IP Address Supplied By: Dial-in User** is set to **No**. You can configure this field even if Dial-in User is set to **Yes**, in which case your Prestige will accept the IP address if the remote peer specifies one; otherwise, an IP address is assigned from the pool.	**No** (default)
IP Start Addr	This field is applicable only if you selected **Yes** in the Dial-In IP Address Supplied By: IP Pool field. The IP pool contains contiguous IP addresses and this field specifies the first one in the pool. The IP start address is the start of a series of consecutive IP addresses.	
IP Count (1, 2)	In this field, enter the number (**1** or **2**) of addresses in the IP Pool. For example, if the starting address is 192.168.135.5 and the count is 2, then the pool will have 192.68.135.5 and 192.68.135.6. The IP count is the number of consecutive IP addresses allowed.	**1**
Session Options: Edit Filter Sets	Press [SPACE BAR] and then [ENTER] to select **Yes** to edit the filter sets. Keep in mind that the filter set(s) will only apply to remote dial-in users but not the remote nodes. **NOTE:** Spaces and [–] symbol are accepted in this field. For more information on customizing your filter sets, *see Chapter 9 – Filter Configuration*. The default is blank, i.e., no filters.	**No** (default)
Once you have completed filling in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel.		

10.3.1 Default Dial-in Filter

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

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

Spaces are accepted in this field. For more information on defining the filters, see the filters chapter.

```
                    Menu 13.1 - Default Dial-in Filter

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

              Press ENTER to Confirm or ESC to Cancel:


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

Figure 10-2 Menu 13.1 Default Dial-in Filter

10.4 Callback Overview

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

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

10.5 Dial-In User Setup

This section provides steps on how to set up a remote dial-in user.

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

```
                Menu 14 - Dial-in User Setup

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

                Enter Menu Selection Number:
```

Figure 10-3 Menu 14 Dial-in User Setup

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

```
                Menu 14.1 - Edit Dial-in User

            User Name= johndoe
            Active= Yes
            Password= ?
            Callback= No
              Phone # Supplied by Caller= N/A
              Callback Phone #= N/A
            Rem CLID=
            Idle Timeout= 100


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

Figure 10-4 Menu 14.1 Edit Dial-in User

Table 10-3 Edit Dial-in User

FIELD	DESCRIPTION	EXAMPLE
User Name	This is a required field. This will be used as the login name for authentication. Choose a descriptive word for login, for example, johndoe.	**johndoe**
Active	You can disallow dial-in access to this user by setting this field to inactive. Inactive users are displayed with a [–] (minus sign) at the beginning of the name in Menu 14.	**Yes**
Password	Enter the password for the remote dial-in user.	

Table 10-3 Edit Dial-in User

FIELD	DESCRIPTION	EXAMPLE
Callback	This field determines if your Prestige will allow call back to this user upon dial-in. If this option is enabled, your Prestige will call back to the user if requested. In such a case, your Prestige will disconnect the initial call from this user and dial back to the specified callback number (see ahead). **No** – The default is no callback. **Optional** – The user can choose to disable callback. **Mandatory** – The user cannot disable callback.	**No** (default)
Phone # Supplied by Caller	This option allows the user to specify the call back telephone number on a call-by-call basis. This is useful when your Prestige returns a call back to a mobile user at different numbers, e.g., a sales rep. in a hotel. If the setting is **Yes**, the user can specify and send to the Prestige the callback number of his/her choice. The default is **No**, i.e., your Prestige always calls back to the fixed callback number.	**No** (default)
Callback Phone #	If **Phone # Supplied by Caller** is **No**, then this is a required field. Otherwise, a **N/A** will appear in the field. Enter the telephone number to which your Prestige will call back.	
Rem CLID	If you enable **CLID Authen** field in Menu 13, then you need to specify the telephone number from which this user calls. Your Prestige will check the CLID in the incoming call against the CLIDs in the database. If they do not match and **CLID Authen** is **Required**, your Prestige will not answer the call.	
Idle Time-out	Enter the idle time (in seconds). This time-out determines how long the dial-in user can be idle before your Prestige disconnects the call when the Prestige is calling back. Idle time is defined as the period of time where there is no data traffic between the dial-in user and your Prestige. The default is 100 seconds.	**100** seconds
Once you have completed filling in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel.		

10.6 Telecommuting Application With Windows Example

Telecommuting enables people to work at remote sites and yet still have access to the resources in the business office. Typically, a telecommuter will use a client workstation with TCP/IP and dial-out capabilities, e.g., a Windows® PC or a Macintosh. For telecommuters to call in to your Prestige, you need to configure a

dial-in user profile for each telecommuter. Additionally, you need to configure the Default Dial-in User Setup to set the operational parameters for all dial-in users.

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

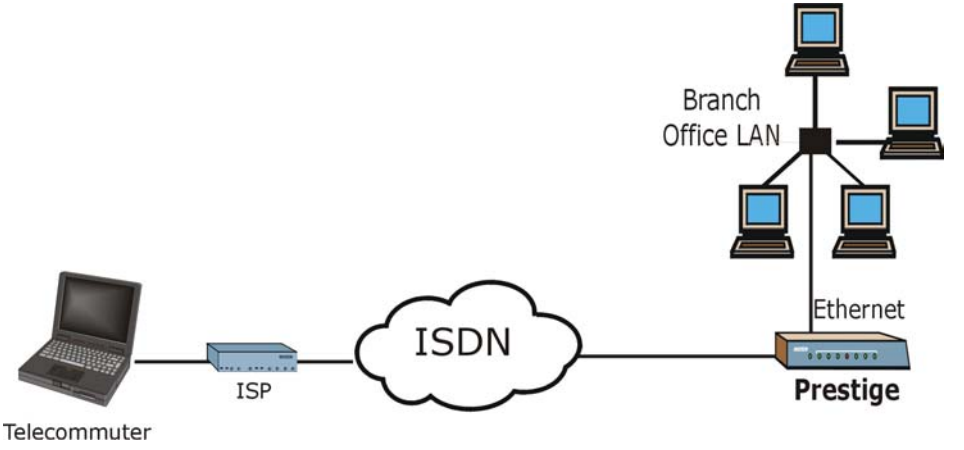


Figure 10-5 Example of Telecommuting

See the following screens on how to configure your Prestige if a remote user's computer is running Windows®.

Configuring Menu 13:

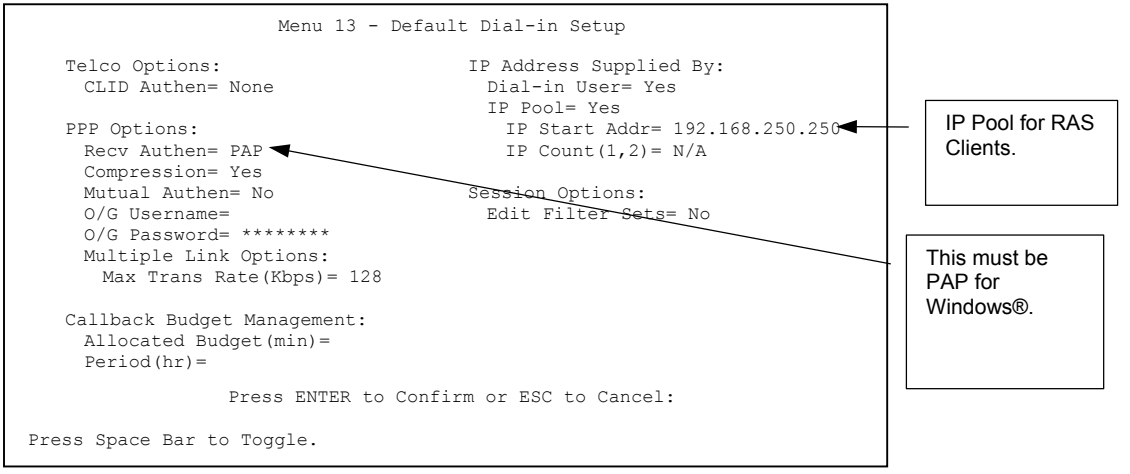


Figure 10-6 Configuring Menu 13 for Remote Access

Configuring Menu 14.1

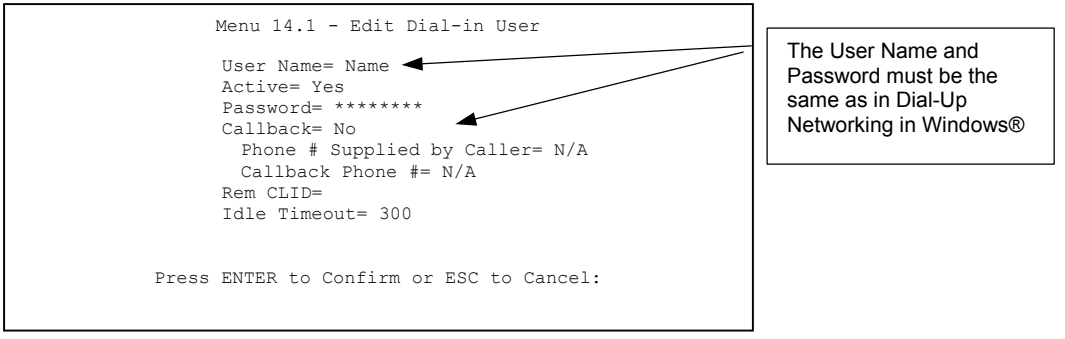


Figure 10-7 Edit Dial-in-User

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

10.7 LAN-to-LAN Server Application Example

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

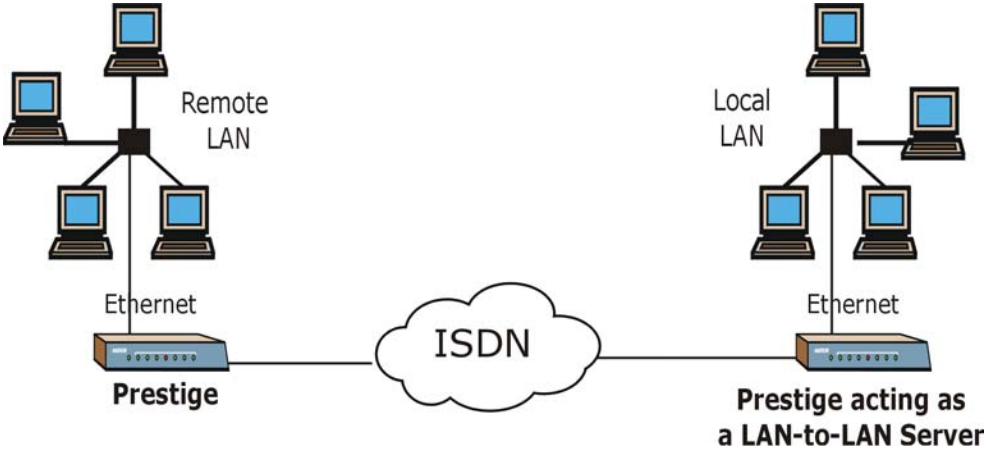


Figure 10-8 Example of a LAN-to-LAN Server Application

10.7.1 Configuring Callback in LAN-to-LAN Application

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

LAN 1

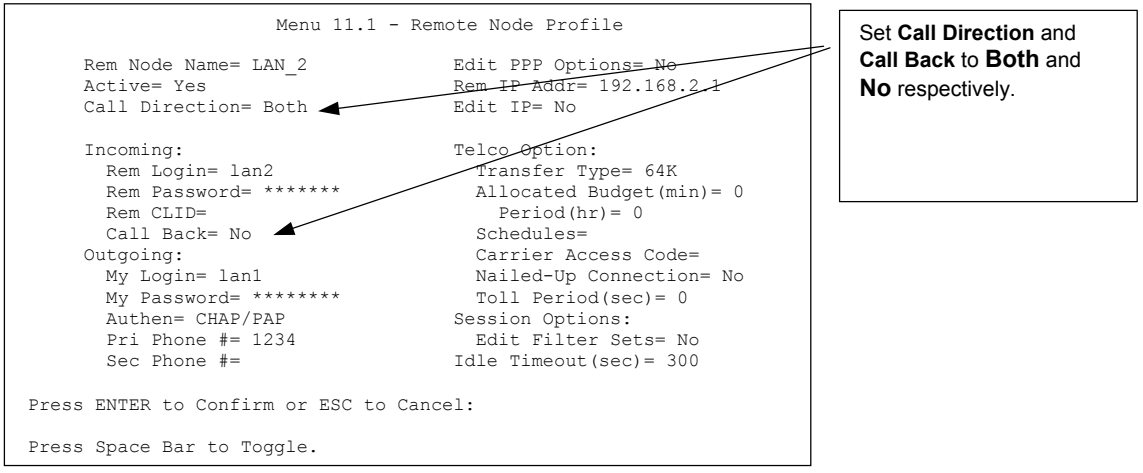


Figure 10-9 LAN 1 LAN-to-LAN Application

LAN 2

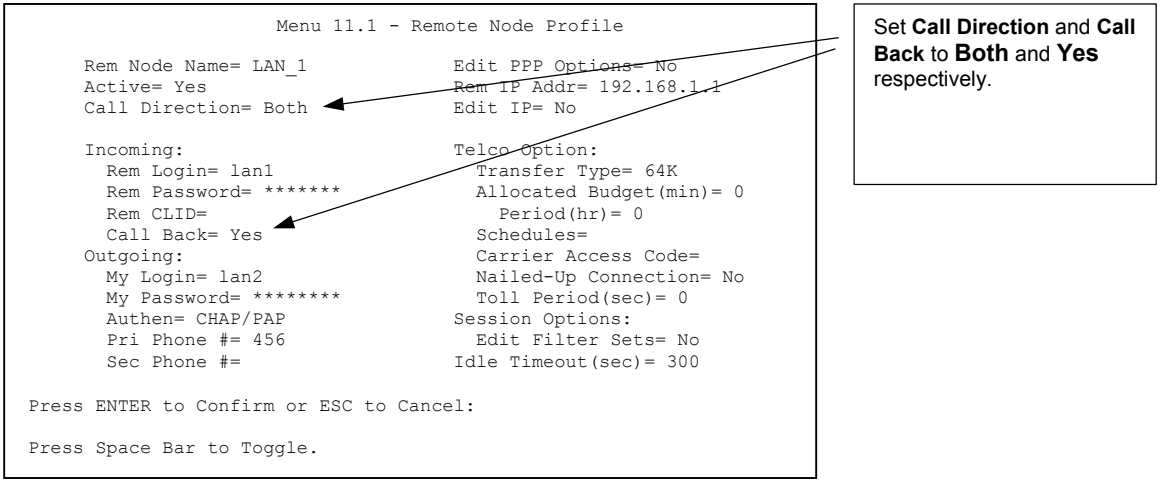


Figure 10-10 LAN 2 LAN-to-LAN Application

Go to menu 24.4.5 of the Prestige on LAN 1 and enter the numbers that correspond to the menu in LAN 1 above to test callback with your connection.

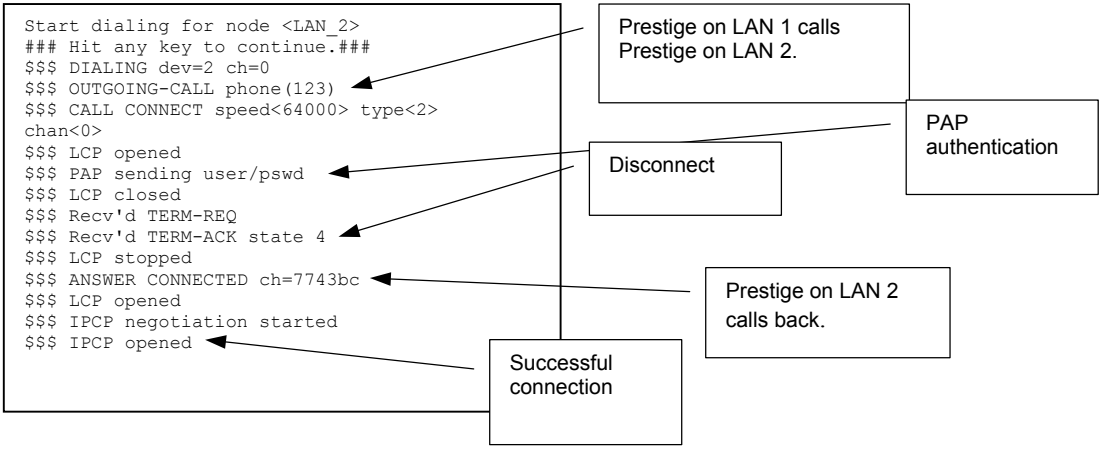


Figure 10-11 Testing Callback With Your Connection

10.7.2 Configuring With CLID in LAN-to-LAN Application

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

Prestige on LAN 2

```
                    Menu 11.1 - Remote Node Profile

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

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

                 Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

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

Figure 10-12 Callback With CLID Configuration

Menu 13

```
                      Menu 13 - Default Dial-in Setup

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

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

                  Press ENTER to Confirm or ESC to Cancel:

 Press Space Bar to Toggle.
```

Set this field to **Required**.

Figure 10-13 Configuring CLID With Callback

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

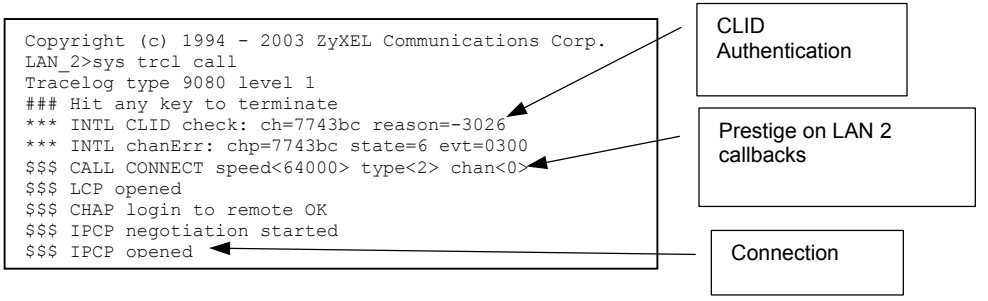


Figure 10-14 Callback and CLID Connection Test

Chapter 11
Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

11.1 NAT Overview

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

11.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the Prestige, for example, the computers 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 a router, for example, 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 traveling 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.

Table 11-1 NAT Definitions

ITEM	DESCRIPTION
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.

NAT never changes the IP address (either local or global) of an outside **host.**

11.1.2 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 to 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, for example, 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 *Table 11-2*), NAT offers the additional benefit of firewall protection. With no servers defined, your Prestige filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

11.1.3 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 figure illustrates this.

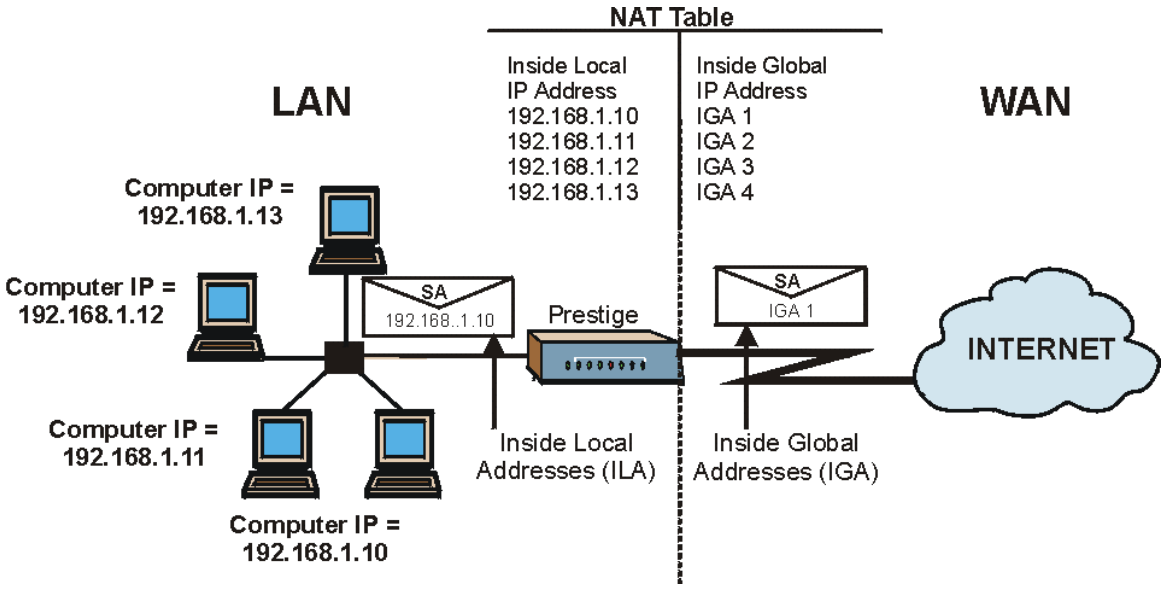


Figure 11-1 How NAT Works

11.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the Prestige can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

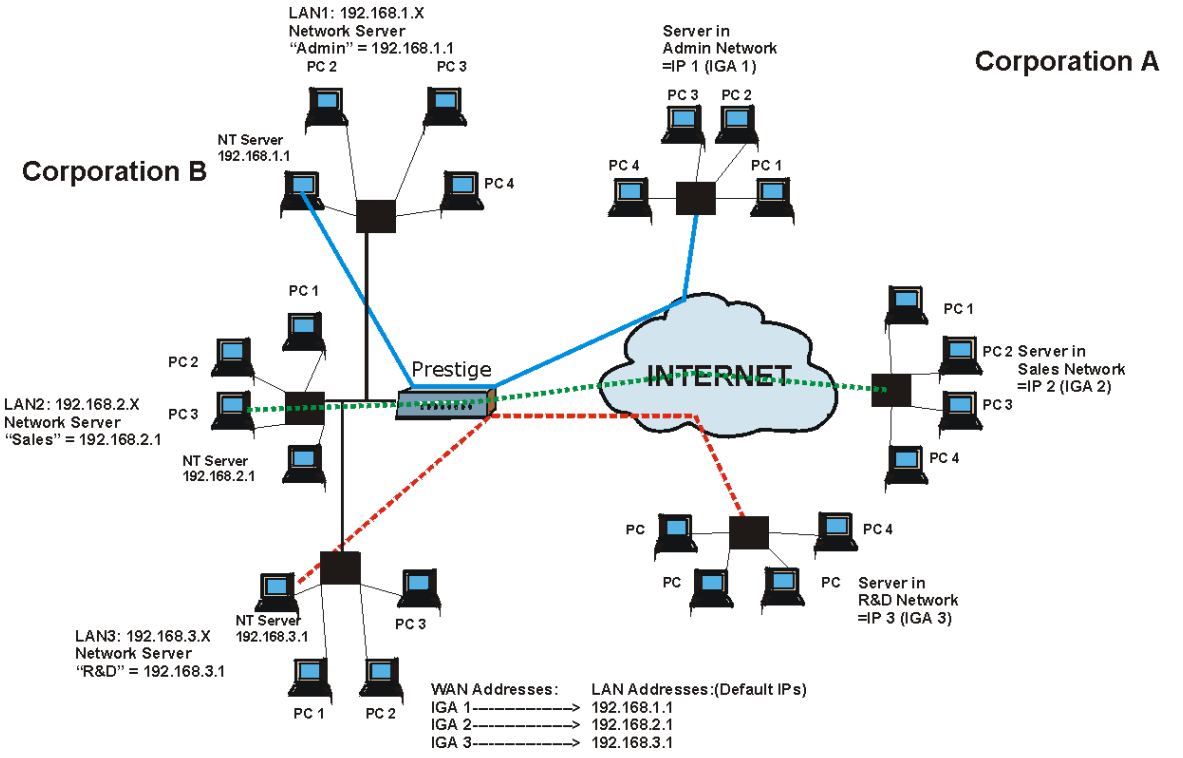


Figure 11-2 NAT Application With IP Alias

11.1.5 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 (for instance, PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the **SUA Only** option in today's routers).
3. **Many to Many Overload**: In Many-to-Many Overload mode, the Prestige maps the multiple local IP addresses to shared global IP addresses.
4. **Many-to-Many No Overload**: In Many-to-Many No Overload mode, the Prestige maps each local IP 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.

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

The following table summarizes these types.

Table 11-2 NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION
One-to-One	ILA1←→ IGA1	1:1
Many-to-One (SUA/PAT)	ILA1←→ IGA1 ILA2←→ IGA1 …	M:1
Many-to-Many Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA1 ILA4←→ IGA2 …	M:M Ov
Many-to-Many No Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA3 …	M:M No OV
Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1	Server

11.1.6 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See section *11.3.1* for a detailed description of the NAT set for SUA. The Prestige also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in *Table 11-2*.

1. **Choose** SUA Only **if you have just one public WAN IP address for your Prestige.**

2. **Choose** Full Feature **if you have multiple public WAN IP addresses for your Prestige.**

11.2 Applying NAT

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

```
                Menu 4 - Internet Access Setup

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


                  NAT= SUA Only
                    Address Mapping Set= N/A

                  Telco Options:
                  Transfer Type= 64K

                  Multilink= Off
                  Idle Timeout= 100

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

Figure 11-3 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 and select a remote node.

Step 2. Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options.**

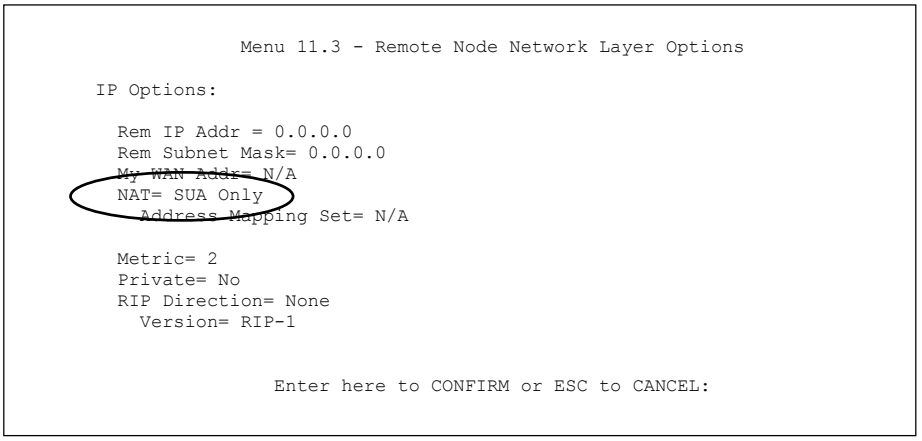


Figure 11-4 Applying NAT to the Remote Node

Table 11-3 Applying NAT to the Remote Node

FIELD	DESCRIPTION	EXAMPLE
NAT	Press [SPACE BAR] and then [ENTER] to select **Full Feature** if you have multiple public WAN IP addresses for your Prestige. The SMT uses the address mapping set that you configure and enter in the **Address Mapping Set** field (menu 15.1 - see section *11.3.1*). When you select **Full Feature** you must configure at least one address mapping set!	**Full Feature**
	Select **None** to disable NAT.	
	When you select **SUA Only**, the SMT uses Address Mapping Set 255 (menu 15.1 - see section *11.3.1*). Choose **SUA Only** if you have just one public WAN IP address for your Prestige.	

11.3 NAT Setup

Use the Address Mapping Sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN. You can see two NAT Address Mapping sets in menu 15.1. You can only configure **Set 1**. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**, which supports all mapping types as outlined in Table 11-2. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The Server Set is a list of LAN side servers mapped to external ports. To use this set (one set for the Prestige 10), a server rule must be set up inside the NAT Address Mapping set. Please see *section 11.4* for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

```
                        Menu 15 — NAT Setup

          1.    Address Mapping Sets
          2.    NAT Server Sets


                     Enter Menu Selection Number:
```

Figure 11-5 Menu 15 NAT Setup

11.3.1 Address Mapping Sets

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

```
                          Menu 15.1 - Address Mapping Sets

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


                             Enter Menu Selection Number:

Enter Menu Selection Number:
```

Figure 11-6 Menu 15.1 Address Mapping Sets

SUA Address Mapping Set

Enter 255 to display the next screen (see also *section 11.1.6)*. The fields in this menu cannot be changed.

```
                        Menu 15.1.255 - Address Mapping Rules

 Set Name=

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

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

Figure 11-7 Menu 15.1.255 SUA Address Mapping Rules

Table 11-4 Menu 15.1.255 SUA Address Mapping Rules

FIELD	DESCRIPTION	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 11-1)*. **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).	
Type	These are the mapping types discussed above (see *Table 11-2*). **Server** allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.	Server
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

11.3.2 User-Defined Address Mapping Sets

Now let's look at option 1 in menu 15.1. Enter 1 to bring up this menu. We'll just look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this

screen. 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.

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

```
                        Menu 15.1.1 - Address Mapping Rules

 Set Name= ?

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

                  Action= Edit          Select Rule=

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

Figure 11-8 Menu 15.1.1 Address Mapping Rules First Set

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

11.3.3 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 rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

Table 11-5 Fields in Menu 15.1.1

FIELD	DESRIPTION	EXAMPLE
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.	NAT_SET

Table 11-5 Fields in Menu 15.1.1

FIELD	DESRIPTION	EXAMPLE
Action	The default is **Edit**. **Edit** means you want to edit a selected rule (see following field). **Insert Before** means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. **Delete** means to delete the selected rule and then all the rules after the selected one will be advanced one rule. **None** disables the **Select Rule** item.	**Edit**
Select Rule	When you choose **Edit**, **Insert Before** or **Delete** in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.	1

You must press [ENTER] **at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.**

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

An End IP address must be numerically greater than its corresponding IP Start address.

```
                Menu 15.1.1.1 Address Mapping Rule

        Type= One-to-One

        Local IP:
          Start=
          End  = N/A

        Global IP:
          Start=
          End  = N/A

        Server Mapping Set= N/A

             Press ENTER to Confirm or ESC to Cancel:

    Press Space Bar to Toggle.
```

Figure 11-9 Menu 15.1.1.1 Address Mapping Rule

Table 11-6 Menu 15.1.1.1 Address Mapping Rule

FIELD	DESCRIPTION	EXAMPLE
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in Table 11-2. **Server** allows you to specify multiple servers of different types behind NAT to this computer. See *section 11.5.3* for an example.	**One-to-One**
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.	N/A
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**.	N/A
Server Mapping Set	Only available when **Type** is set to **Server**. Type a number from 1 to 10 to choose a server set from menu 15.2.	
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

11.4 NAT Server Sets – Port Forwarding

A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

Use **Menu 15 - NAT Setup** to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

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.

Table 11-7 Services & Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

11.4.1 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

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

Step 2. Enter 2 to display **Menu 15.2 - NAT Server Sets** as shown next.

```
                Menu 15.2 - NAT Server Sets

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


                Enter Set Number to Edit:
```

Figure 11-10 Menu 15.2 NAT Server Sets

Step 3. Enter 1 to go to **Menu 15.2 NAT Server Setup** as follows.

```
                Menu 15.2 - NAT Server Setup

 Rule   Start Port No.   End Port No.   IP Address
-------------------------------------------------
   1.     Default          Default        0.0.0.0
   2.       21               25           192.168.1.33
   3.       0                0            0.0.0.0
   4.       0                0            0.0.0.0
   5.       0                0            0.0.0.0
   6.       0                0            0.0.0.0
   7.       0                0            0.0.0.0
   8.       0                0            0.0.0.0
   9.       0                0            0.0.0.0
  10.       0                0            0.0.0.0
  11.       0                0            0.0.0.0
  12.       0                0            0.0.0.0

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

Figure 11-11 Menu 15.2 NAT Server Setup

Step 4. Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.

Step 5. Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.

Step 6. 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.

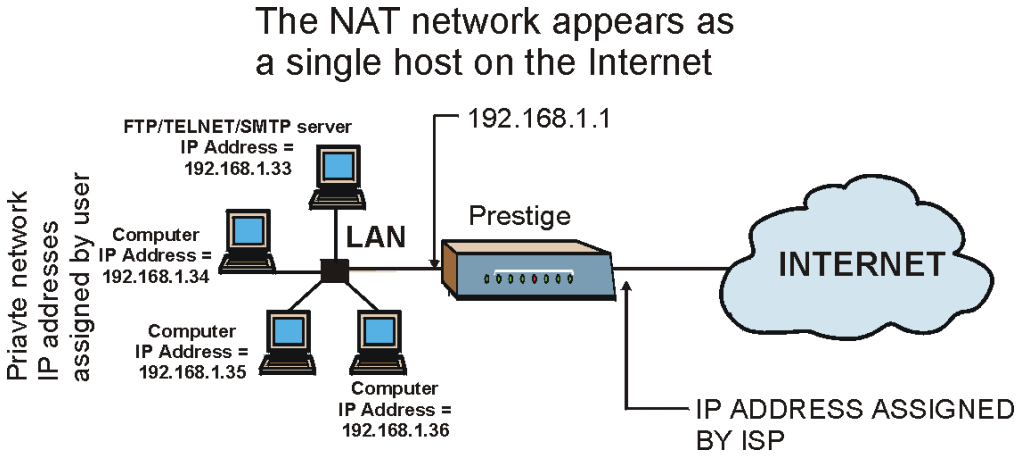


Figure 11-12 Multiple Servers Behind NAT Example

11.5 General NAT Examples

This section provides some examples with Network Address Translation.

11.5.1 Example 1: Internet Access Only

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

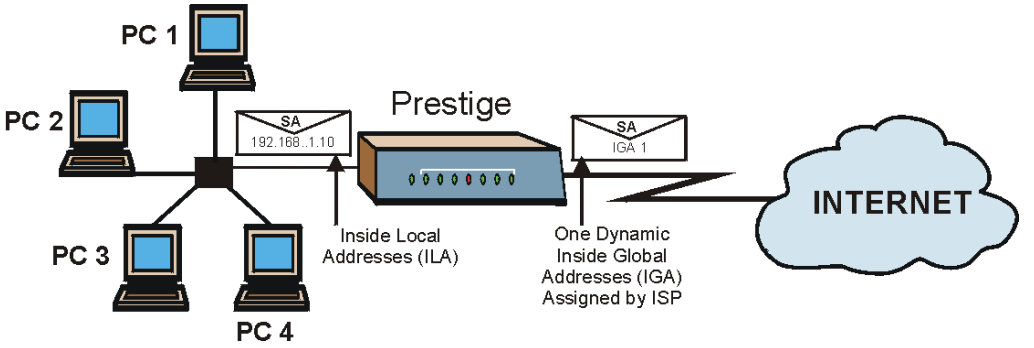


Figure 11-13 NAT Example 1

```
                    Menu 4 - Internet Access Setup

Menu 4 - Internet Access Setup

              ISP's Name= test
              Encapsulation= RFC 1483
              Multiplexing= LLC-based
              VPI #= 1
              VCI #= 1
              Service Name= N/A
              My Login= N/A
              My Password= N/A
              NAT= SUA Only
                Address Mapping Set= N/A
              IP Address Assignment= Static
                IP Address= 0.0.0.0
              ENET ENCAP Gateway= N/A


              Press ENTER to Confirm or ESC to
```

Figure 11-14 Menu 4 Internet Access & NAT Example

From menu 4, choose the **SUA Only** option from the **NAT** field. This is the Many-to-One mapping discussed in *section 11.5*. The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

11.5.2 Example 2: Internet Access with an Inside Server

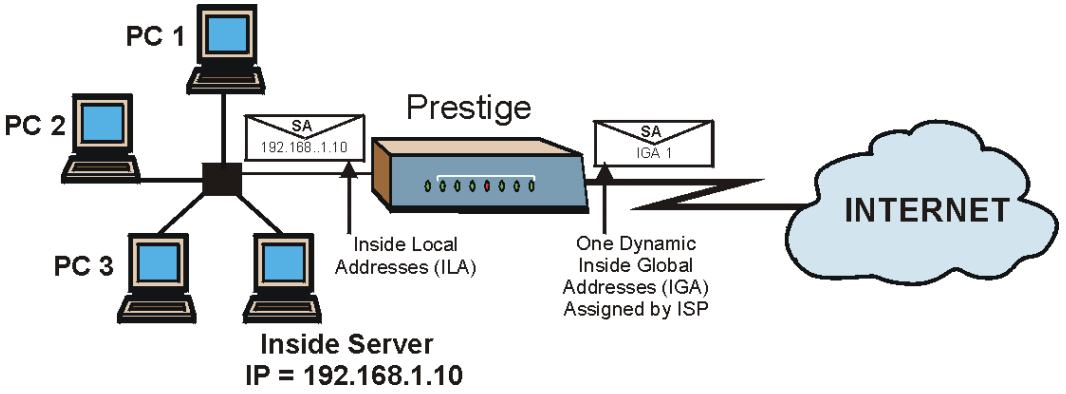


Figure 11-15 NAT Example 2

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.

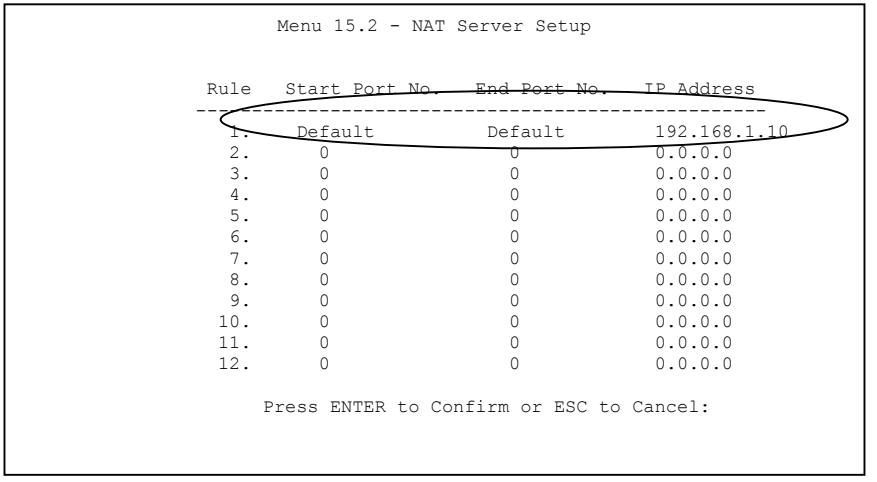


Figure 11-16 Menu 15.2 Specifying an Inside Server

11.5.3 Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two uni-directional as follows.

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

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

Rule 3. Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).

Rule 4. You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

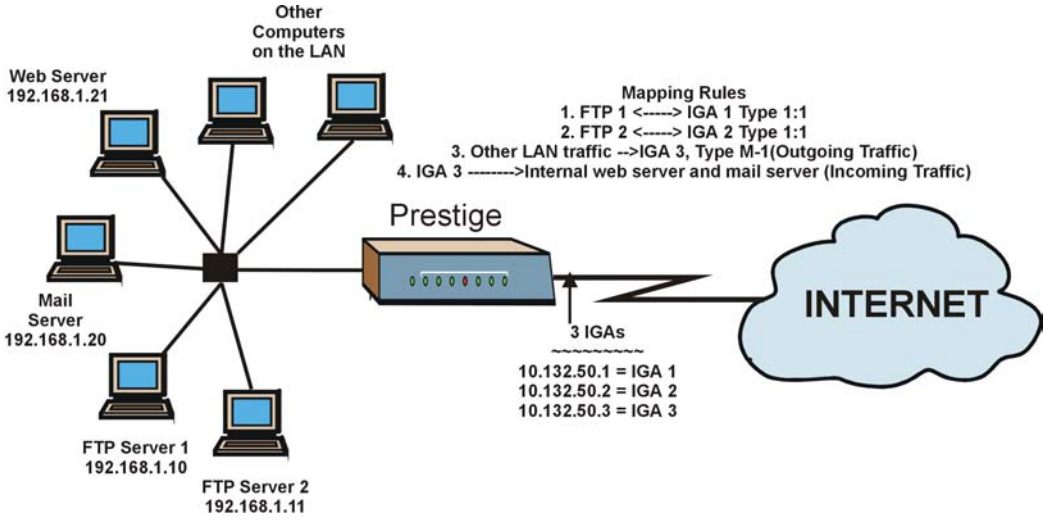


Figure 11-17 NAT Example 3

Step 1. In this case 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) in *Figure 11-18*.

Step 2. Then enter 15 from the main menu.

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

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

Step 5. Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See *Figure 11-19).*

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

```
            Menu 11.3 - Remote Node Network Layer Options

IP Options:                          Bridge Options:
  IP Address Assignment= Static        Ethernet Addr Timeout (min)= 0
  Rem IP Addr: 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= Full Feature
    Address Mapping Set= 2
  Metric= 2
  Private= No
  RIP Direction= Both
    Version= RIP-2B
  Multicast= IGMP-v2
  IP Policies=

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

Figure 11-18 Example 3: Menu 11.3

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

        Server Mapping Set= N/A


                        Press ENTER to Confirm or ESC to Cancel:

    Press Space Bar to Toggle.
```

Figure 11-19 Example 3: Menu 15.1.1.1

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

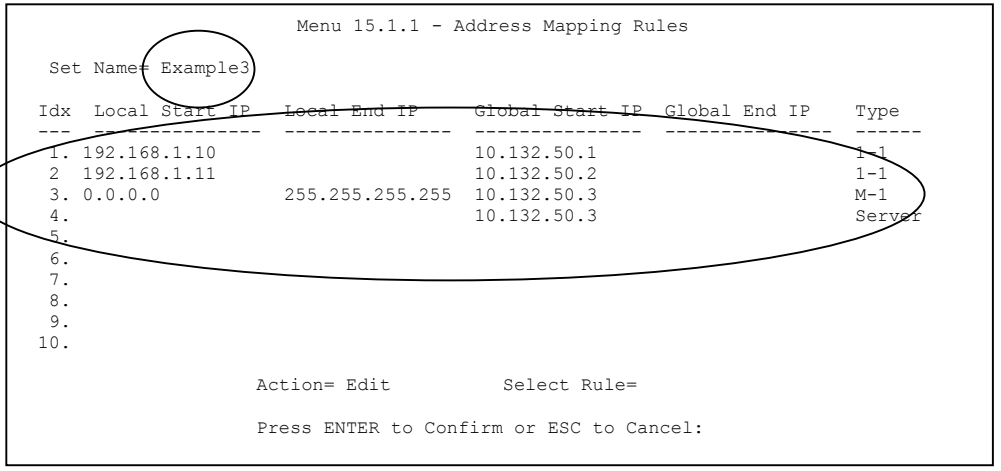


Figure 11-20 Example 3: Final Menu 15.1.1

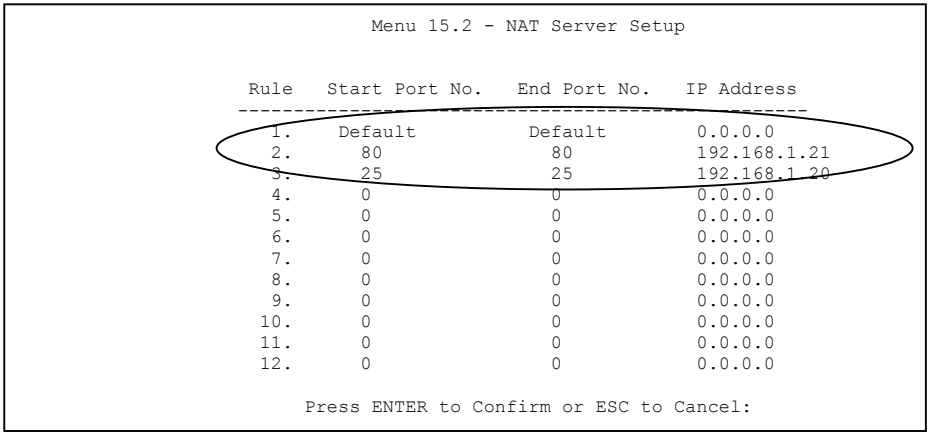
Step 7. Menu 15.1.1 should look as above.

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

Step 8. Enter 15 from the main menu.

Step 9. Enter 2 in **Menu 15 - NAT Setup**.

Step 10. Enter 1 in **Menu 15.2 - NAT Server Sets** to see the following menu. Configure it as shown.



Example 3: Menu 15.2.1

11.5.4 Example 4: NAT Unfriendly Application Programs

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

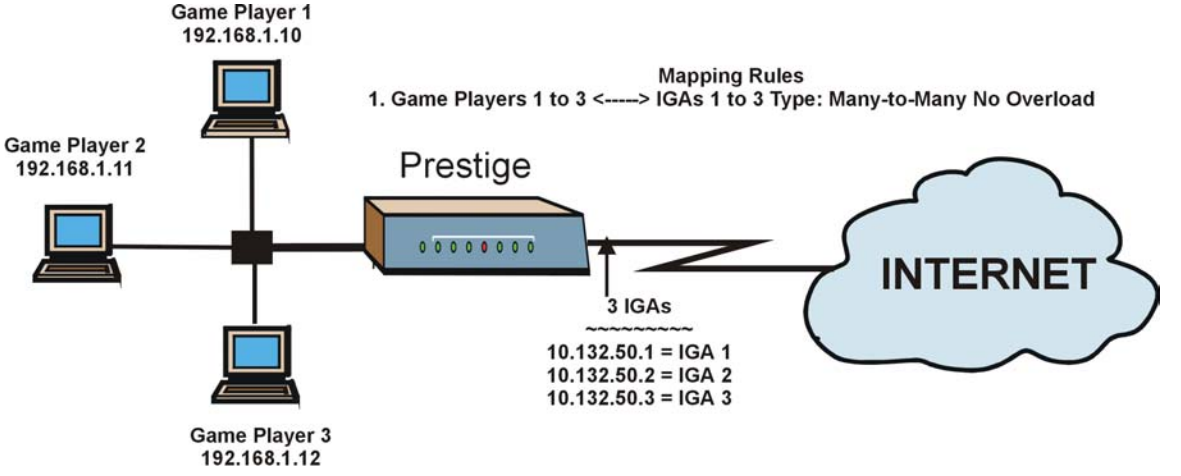


Figure 11-21 NAT Example 4

Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won't work through NAT even when using One-to-One **and** Many-to-Many No Overload **mapping types.**

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

```
                    Menu 15.1.1.1 Address Mapping Rule

        Type= Many-to-Many No Overload

        Local IP:
          Start= 192.168.1.10
          End  = 192.168.1.12

        Global IP:
          Start= 10.132.50.1
          End  = 10.132.50.3

        Server Mapping Set= N/A

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

Figure 11-22 Example 4: Menu 15.1.1.1 Address Mapping Rule

After you've configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

```
                    Menu 15.1.1 - Address Mapping Rules

 Set Name= Example4

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

                  Action= Edit          Select Rule=

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

Figure 11-23 Example 4: Menu 15.1.1 Address Mapping Rules

Part III:

Firewall

This part introduces firewalls in general and the Prestige firewall. It also explains customized services and logs and gives example firewall rules.

Chapter 12
Firewalls

This chapter gives some background information on firewalls and explains how to get started with the Prestige firewall.

12.1 Firewall Overview

Originally, the term *firewall* referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem. A firewall is *one* of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the *only* mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

12.2 Types of Firewalls

There are three main types of firewalls:

1. Packet Filtering Firewalls
2. Application-level Firewalls
3. Stateful Inspection Firewalls

12.2.1 Packet Filtering Firewalls

Packet filtering firewalls restrict access based on the source/destination computer network address of a packet and the type of application.

12.2.2 Application-level Firewalls

Application-level firewalls restrict access by serving as proxies for external servers. Since they use programs written for specific Internet services, such as HTTP, FTP and telnet, they can evaluate network packets for valid application-specific data. Application-level gateways have a number of general advantages over the default mode of permitting application traffic directly to internal hosts:

i. Information hiding prevents the names of internal systems from being made known via DNS to outside systems, since the application gateway is the only host whose name must be made known to outside systems.

ii. Robust authentication and logging pre-authenticates application traffic before it reaches internal hosts and causes it to be logged more effectively than if it were logged with standard host logging. Filtering rules at the packet filtering router can be less complex than they would be if the router needed to filter application traffic and direct it to a number of specific systems. The router need only allow application traffic destined for the application gateway and reject the rest.

12.2.3 Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. See *section 12.5* for more information on Stateful Inspection.

Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

12.3 Introduction to ZyXEL's Firewall

The Prestige firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (in SMT menu 21.2 or in the web configurator). The Prestige's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The Prestige can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network. The Prestige also has packet-filtering capabilities.

The Prestige is installed between the LAN and the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The Prestige has one ISDN port and one Ethernet LAN port, which physically separate the network into two areas.

- The ISDN port connects to the Internet.
- The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP, and the World Wide Web. However, "inbound access" will not be allowed unless you configure remote management or create a firewall rule to allow a remote host to use a specific service.

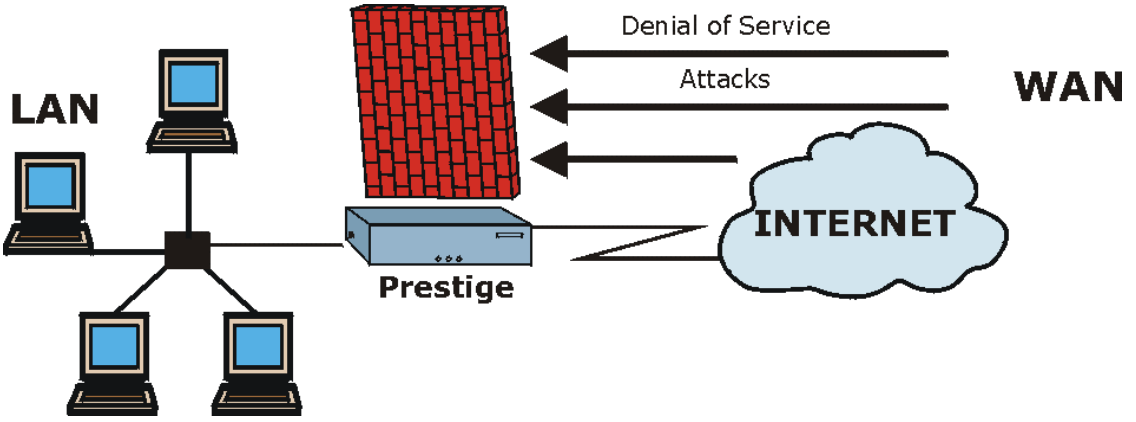


Figure 12-1 Prestige Firewall Application

12.4 Denial of Service

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The Prestige is pre-configured to automatically detect and thwart all known DoS attacks.

12.4.1 Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An "extension number", called the "TCP port" or "UDP port" identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc. For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server "listens" on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

Table 12-1 Common IP Ports

21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

12.4.2 Types of DoS Attacks

There are four types of DoS attacks:

1. Those that exploit bugs in a TCP/IP implementation.
2. Those that exploit weaknesses in the TCP/IP specification.
3. Brute-force attacks that flood a network with useless data.
4. IP Spoofing.

1. "**Ping of Death**" and "**Teardrop**" attacks exploit bugs in the TCP/IP implementations of various computer and host systems.

   1-a Ping of Death uses a "ping" utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot.

   1-b Teardrop attack exploits weaknesses in the re-assembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

2. Weaknesses in the TCP/IP specification leave it open to "**SYN Flood**" and "**LAND**" attacks. These attacks are executed during the handshake that initiates a communication session between two applications.

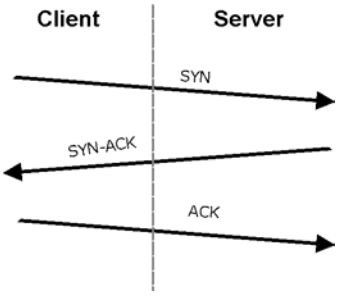


Figure 12-2 Three-Way Handshake

Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

2-a **SYN Attack** floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

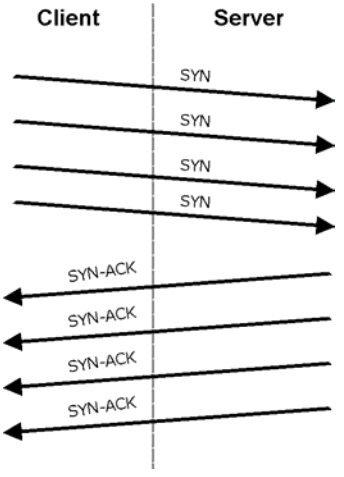


Figure 12-3 SYN Flood

2-b In a **LAND Attack**, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

3. A **brute-force** attack, such as a "Smurf" attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the network, the router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic. If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only clog up the "intermediary" network, but will also congest the network of the spoofed source IP address, known as the "victim" network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

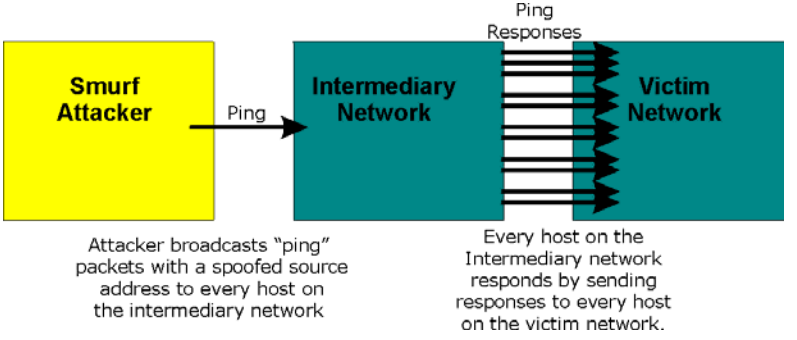


Figure 12-4 Smurf Attack

- ICMP Vulnerability

ICMP is an error-reporting protocol that works in concert with IP. The following ICMP types trigger an alert:

Table 12-2 ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

- Illegal Commands (NetBIOS and SMTP)

The only legal NetBIOS commands are the following - all others are illegal.

Table 12-3 Legal NetBIOS Commands

MESSAGE:
REQUEST:
POSITIVE:
NEGATIVE:
RETARGET:
KEEPALIVE:

All SMTP commands are illegal except for those displayed in the following tables.

Table 12-4 Legal SMTP Commands

AUTH	DATA	EHLO	ETRN	EXPN	HELO	HELP	MAIL	NOOP
QUIT	RCPT	RSET	SAML	SEND	SOML	TURN	VRFY	

- Traceroute

Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes when a packet filter firewall is configured incorrectly an attacker can traceroute the firewall gaining knowledge of the network topology inside the firewall.

4. Often, many DoS attacks also employ a technique known as "**IP Spoofing**" as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall. The Prestige blocks all IP Spoofing attempts.

12.5 Stateful Inspection

With stateful inspection, fields of the packets are compared to packets that are already known to be trusted. For example, if you access some outside service, the proxy server remembers things about your original request, like the port number and source and destination addresses. This "remembering" is called *saving the state.* When the outside system responds to your request, the firewall compares the received packets with the saved state to determine if they are allowed in. The Prestige uses stateful packet inspection to protect the private LAN from hackers and vandals on the Internet. By default, the Prestige's stateful inspection allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet. In summary, stateful inspection:

- Allows all sessions originating from the LAN (local network) to the WAN (Internet).

- Denies all sessions originating from the WAN to the LAN.

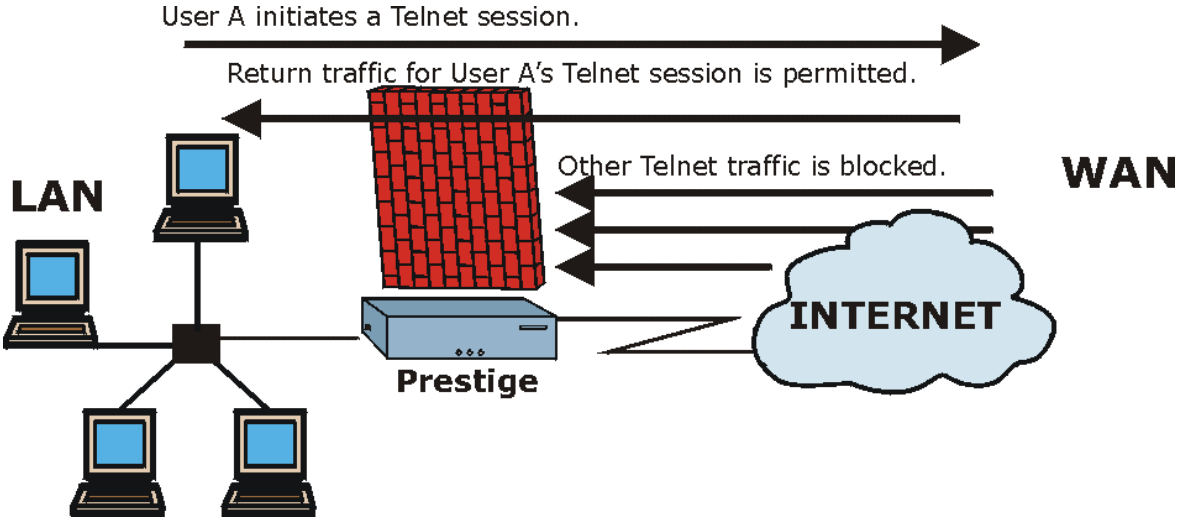


Figure 12-5 Stateful Inspection

The previous figure shows the Prestige's default firewall rules in action as well as demonstrates how stateful inspection works. User A can initiate a Telnet session from within the LAN and responses to this request are allowed. However other Telnet traffic initiated from the WAN is blocked.

12.5.1 Stateful Inspection Process

In this example, the following sequence of events occurs when a TCP packet leaves the LAN network through the firewall's WAN interface. The TCP packet is the first in a session, and the packet's application layer protocol is configured for a firewall rule inspection:

1. The packet travels from the firewall's LAN to the WAN.
2. The packet is evaluated against the interface's existing outbound access list, and the packet is permitted (a denied packet would simply be dropped at this point).
3. The packet is inspected by a firewall rule to determine and record information about the state of the packet's connection. This information is recorded in a new state table entry created for the new connection. If there is not a firewall rule for this packet and it is not an attack, then **the default action for packets not matching following rules** field determines the action for this packet.
4. Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary

access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.

5. The outbound packet is forwarded out through the interface.
6. Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.
7. The packet is inspected by a firewall rule, and the connection's state table entry is updated as necessary. Based on the updated state information, the inbound extended access list temporary entries might be modified, in order to permit only packets that are valid for the current state of the connection.
8. Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.
9. When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

12.5.2 Stateful Inspection and the Prestige

Additional rules may be defined to extend or override the default rules. For example, a rule may be created which will:

i. Block all traffic of a certain type, such as IRC (Internet Relay Chat), from the LAN to the Internet.

ii. Allow certain types of traffic from the Internet to specific hosts on the LAN.

iii. Allow access to a Web server to everyone but competitors.

iv. Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by evaluating the network traffic's Source IP address, Destination IP address, IP protocol type, and comparing these to rules set by the administrator.

The ability to define firewall rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting firewall rules. Test changes after creating them to make sure they work correctly.

Below is a brief technical description of how these connections are tracked. Connections may either be defined by the upper protocols (for instance, TCP), or by the Prestige itself (as with the "virtual connections" created for UDP and ICMP).

12.5.3 TCP Security

The Prestige uses state information embedded in TCP packets. The first packet of any new connection has its SYN flag set and its ACK flag cleared; these are "initiation" packets. All packets that do not have this flag structure are called "subsequent" packets, since they represent data that occurs later in the TCP stream.

If an initiation packet originates on the WAN, this means that someone is trying to make a connection from the Internet into the LAN. Except in a few special cases (see "Upper Layer Protocols" shown next), these packets are dropped and logged.

If an initiation packet originates on the LAN, this means that someone is trying to make a connection from the LAN to the Internet. Assuming that this is an acceptable part of the security policy (as is the case with the default policy), the connection will be allowed. A cache entry is added which includes connection information such as IP addresses, TCP ports, sequence numbers, etc.

When the Prestige receives any subsequent packet (from the Internet or from the LAN), its connection information is extracted and checked against the cache. A packet is only allowed to pass through if it corresponds to a valid connection (that is, if it is a response to a connection which originated on the LAN).

12.5.4 UDP/ICMP Security

UDP and ICMP do not themselves contain any connection information (such as sequence numbers). However, at the very minimum, they contain an IP address pair (source and destination). UDP also contains port pairs, and ICMP has type and code information. All of this data can be analyzed in order to build "virtual connections" in the cache.

For instance, any UDP packet that originates on the LAN will create a cache entry. Its IP address and port pairs will be stored. For a short period of time, UDP packets from the WAN that have matching IP and UDP information will be allowed back in through the firewall.

A similar situation exists for ICMP, except that the Prestige is even more restrictive. Specifically, only outgoing echoes will allow incoming echo replies, outgoing address mask requests will allow incoming address mask replies, and outgoing timestamp requests will allow incoming timestamp replies. No other ICMP packets are allowed in through the firewall, simply because they are too dangerous and contain too little tracking information. For instance, ICMP redirect packets are never allowed in, since they could be used to reroute traffic through attacking machines.

12.5.5 Upper Layer Protocols

Some higher layer protocols (such as FTP and RealAudio) utilize multiple network connections simultaneously. In general terms, they usually have a "control connection" which is used for sending commands between endpoints, and then "data connections" which are used for transmitting bulk information.

Consider the FTP protocol. A user on the LAN opens a control connection to a server on the Internet and requests a file. At this point, the remote server will open a data connection from the Internet. For FTP to

work properly, this connection must be allowed to pass through even though a connection from the Internet would normally be rejected.

In order to achieve this, the Prestige inspects the application-level FTP data. Specifically, it searches for outgoing "PORT" commands, and when it sees these, it adds a cache entry for the anticipated data connection. This can be done safely, since the PORT command contains address and port information, which can be used to uniquely identify the connection.

Any protocol that operates in this way must be supported on a case-by-case basis. You can use the web configurator's Custom Ports feature to do this.

12.6 Guidelines For Enhancing Security With Your Firewall

1. Change the default password via SMT or web configurator.
2. Think about access control *before* you connect a console port to the network in any way, including attaching a modem to the port. Be aware that a break on the console port might give unauthorized individuals total control of the firewall, even with access control configured.
3. Limit who can telnet into your router.
4. Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Protect against IP spoofing by making sure the firewall is active.
7. Keep the firewall in a secured (locked) room.

12.6.1 Security In General

You can never be too careful! Factors outside your firewall, filtering or NAT can cause security breaches. Below are some generalizations about what you can do to minimize them.

1. Encourage your company or organization to develop a comprehensive security plan. Good network administration takes into account what hackers can do and prepares against attacks. The best defense against hackers and crackers is information. Educate all employees about the importance of security and how to minimize risk. Produce lists like this one!
2. DSL or cable modem connections are "always-on" connections and are particularly vulnerable because they provide more opportunities for hackers to crack your system. Turn your computer off when not in use.

3. Never give out a password or any sensitive information to an unsolicited telephone call or e-mail.
4. Never e-mail sensitive information such as passwords, credit card information, etc., without encrypting the information first.
5. Never submit sensitive information via a web page unless the web site uses secure connections. You can identify a secure connection by looking for a small "key" icon on the bottom of your browser (Internet Explorer 3.02 or better or Netscape 3.0 or better). If a web site uses a secure connection, it is safe to submit information. Secure web transactions are quite difficult to crack.
6. Never reveal your IP address or other system networking information to people outside your company. Be careful of files e-mailed to you from strangers. One common way of getting BackOrifice on a system is to include it as a Trojan horse with other files.
7. Change your passwords regularly. Also, use passwords that are not easy to figure out. The most difficult passwords to crack are those with upper and lower case letters, numbers and a symbol such as % or #.
8. Upgrade your software regularly. Many older versions of software, especially web browsers, have well known security deficiencies. When you upgrade to the latest versions, you get the latest patches and fixes.
9. If you use "chat rooms" or IRC sessions, be careful with any information you reveal to strangers.
10. If your system starts exhibiting odd behavior, contact your ISP. Some hackers will set off hacks that cause your system to slowly become unstable or unusable.
11. Always shred confidential information, particularly about your computer, before throwing it away. Some hackers dig through the trash of companies or individuals for information that might help them in an attack.

12.7 Packet Filtering Vs Firewall

Below are some comparisons between the Prestige's filtering and firewall functions.

12.7.1 Packet Filtering:

- The router filters packets as they pass through the router's interface according to the filter rules you designed.
- Packet filtering is a powerful tool, yet can be complex to configure and maintain, especially if you need a chain of rules to filter a service.
- Packet filtering only checks the header portion of an IP packet.

When To Use Filtering

1. To block/allow LAN packets by their MAC addresses.
2. To block/allow special IP packets which are neither TCP nor UDP, nor ICMP packets.

3. To block/allow both inbound (WAN to LAN) and outbound (LAN to WAN) traffic between the specific inside host/network "A" and outside host/network "B". If the filter blocks the traffic from A to B, it also blocks the traffic from B to A. Filters can not distinguish traffic originating from an inside host or an outside host by IP address.
4. To block/allow IP trace route.

12.7.2 Firewall

- The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet is intended for other layers, from the network layer (IP headers) up to the application layer.
- The firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
- The firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
- The firewall provides e-mail service to notify you of routine reports and when alerts occur.

When To Use The Firewall

1. To prevent DoS attacks and prevent hackers cracking your network.
2. A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule making the firewall a better choice when complex rules are required.
3. To selectively block/allow inbound or outbound traffic between inside host/networks and outside host/networks. Remember that filters can not distinguish traffic originating from an inside host or an outside host by IP address.
4. The firewall performs better than filtering if you need to check many rules.
5. Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.
6. The firewall can block specific URL traffic that might occur in the future. The URL can be saved in an Access Control List (ACL) database.

Chapter 13
Introducing the Prestige Firewall

This chapter shows you how to get started with the Prestige firewall.

13.1 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your Prestige has to offer. For this reason, it is recommended that you configure your firewall using the web configurator; see the following chapters for instructions. SMT screens allow you to activate the firewall and view firewall logs.

13.2 Using Prestige SMT Menus

From the main menu enter 21 to go to **Menu 21 - Filter Set and Firewall Configuration** to display the screen shown next**.**

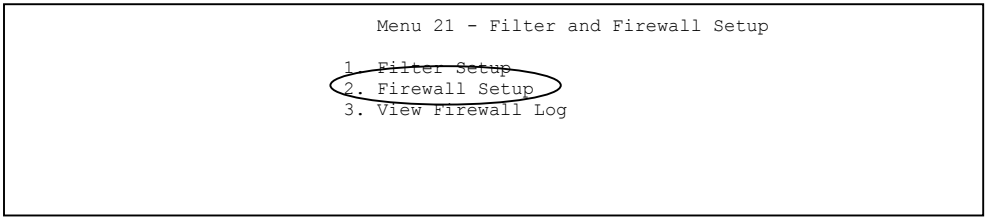


Figure 13-1 Menu 21 Filter and Firewall Setup

13.2.1 Activating the Firewall

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Additional rules may be configured using the web configurator.

```
                          Menu 21.2 - Firewall Setup

The firewall protects against Denial of Service (DOS) attacks when
it is active. The default Policy sets

    1. allow all sessions originating from the LAN to the WAN and
    2. deny all sessions originating from the WAN to the LAN

You may define additional Policy rules or modify existing ones but
please exercise extreme caution in doing so

      Active: Yes

    LAN-to-WAN Set Name: ACL Default Set
    WAN-to-LAN Set Name: ACL Default Set

Please configure the Firewall function through web configurator

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

Figure 13-2 Menu 21.2 Firewall Setup

Configure the firewall rules using the web configurator or Command Interpreter.

13.2.2 Viewing the Firewall Log

In menu 21, enter 3 to view the firewall log. An example of a firewall log is shown next.

```
# Time      Packet Information                  Reason            Action
0|Jan 1 00 |From:192.168.17.1 To:192.168.17.255 |default policy |block
 | 15:43:19|UDP src port:00520 dest port:00520  |<2,00>         |
1|Jan 1 00 |From:172.20.1.179 To:172.21.1.66    |default policy |block
 | 15:43:20|UDP src port:03571 dest port:00161  |<2,00>         |
2|Jan 1 00 |From:172.21.1.148 To:172.21.255.255 |default policy |block
 | 15:43:20|UDP src port:00137 dest port:00137  |<2,00>         |
Clear Firewall Log (y/n):
```

Figure 13-3 Example Firewall Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

Table 13-1 View Firewall Log

FIELD	DESCRIPTION	EXAMPLES
#	This is the index number of the firewall log. 128 entries are available numbered from 0 to 127. Once they are all used, the log wraps around and the old logs are lost.	23
Time	This is the time the log was recorded in this format. You must configure menu 24.10 for real time; otherwise the clock will start at 2000/01/01 00:00:00 the last time the Prestige was reset.	mm:dd:yy e.g., Jan 1 00 hh:mm:ss e.g., 00:00:00
Packet Information	This field lists packet information such as protocol and src/dest port numbers (TCP, UDP), or protocol, type and code (ICMP).	From and To IP addresses Protocol and port numbers
Reason	This field states the reason for the log; i.e., was the rule matched, did not match or was there an attack. The set and rule coordinates (<X, Y> where X=1,2; Y=00~10) follow with a simple explanation. There are two policy sets; set 1 (X = 1) is for LAN to WAN rules and set 2 (X = 2) for WAN to LAN rules. Y represents the rule in the set. You can configure up to 10 rules in any set (Y = 01 to 10). Rule number 00 is the default rule. This is a log for a DoS attack.	not match <1,01> dest IP This means this packet does not match the destination IP address in set 1, rule 1. Other reasons (instead of dest IP) are src IP, dest port, src port and protocol. attack land, ip spoofing, icmp echo, icmp vulnerability, NetBIOS, smtp illegal command, traceroute, teardrop or syn flood
Action	This field displays whether the packet was blocked or forwarded. None means that no action is dictated by this rule.	block, forward or none
After viewing the firewall log, ENTER "y" to clear the log or "n" to retain it. With either option you will be returned to **Menu 21- Filter and Firewall Setup**.		

Chapter 14
Configuring Firewall with the Web Configurator

This chapter shows you how to configure your firewall with the web configurator.

14.1 Web Configurator Login and Main Menu Screens

Use the Prestige web configurator, to configure your firewall. To get started, follow the steps shown next.

Step 1. Launch your web browser and enter 192.168.1.1 as the URL.

Step 2. Enter "admin" as the user name and "1234" (default) as the password and click **Login**.

Step 3. The **Site Map** screen displays as shown next.

Figure 14-1 Site Map Screen

Use the help icon (located in the upper right portion of most screens) for explanations of fields and choices.

If you forget your password, refer to the *Resetting the Prestige* section to see how to reset the default configuration file.

Step 4. Click **Advanced Setup** in the navigation panel, then click **Firewall**. The Firewall Functions screen displays as shown next.

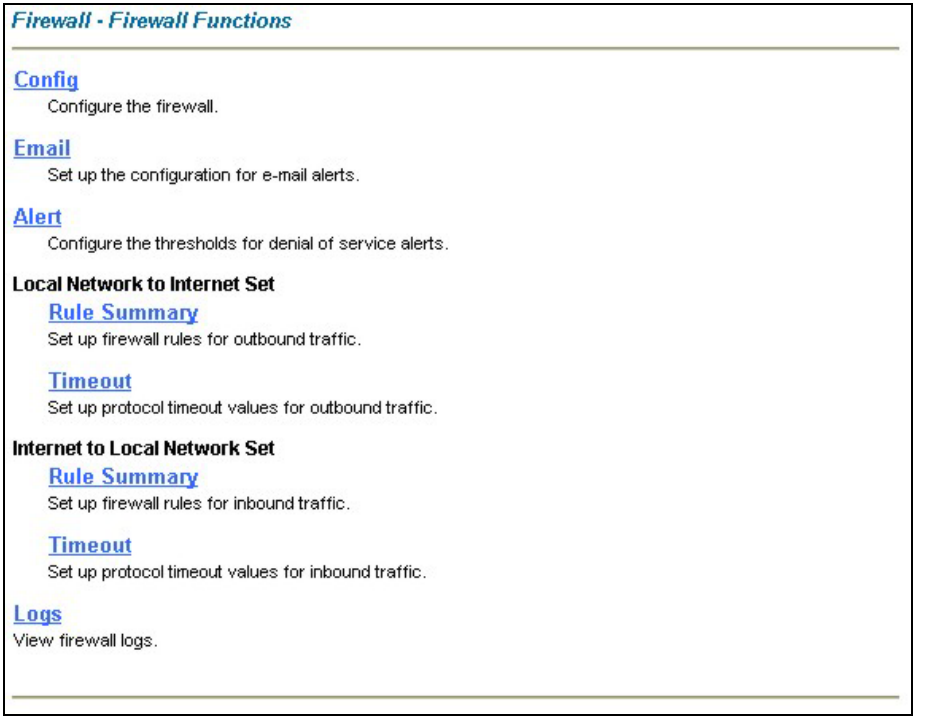


Figure 14-2 Firewall Functions

The following table describes the fields in this screen.

Table 14-1 Predefined Services

LINK	DESCRIPTION
Config	Click this link to enable the firewall.
Email	Click this link to configure an alert report to be sent to a specific e-mail address.
Alert	Click this link to configure alerts to be sent in the event of attacks.
Local Network to Internet Set	
Rule Summary	Click this link to set up firewall rules for LAN to WAN traffic.
Timeout	Click this link to set up protocol timeout values for LAN to WAN traffic.
Internet to Local Network Set	

Table 14-1 Predefined Services

Rule Summary	Click this link to set up firewall rules for WAN to LAN traffic.
Timeout	Click this link to set up protocol timeout values for WAN to LAN traffic.
Logs	Click this link to view the firewall's logs.

14.2 Enabling the Firewall

Click **Advanced Setup**, **Firewall**, and then **Config** to display the following screen. Click the **Firewall Enabled** check box and then click **Apply** to enable (or activate) the firewall.

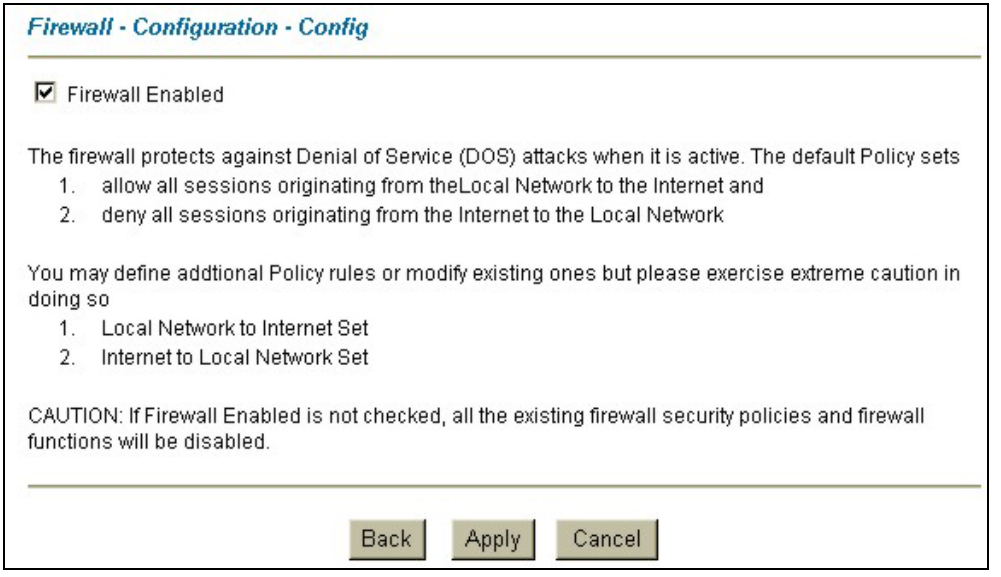


Figure 14-3 Enabling the Firewall

14.3 E-mail

The E-mail screen allows you to specify your mail server, where e-mail alerts should be sent as well as when and how often they should be sent.

14.3.1 Alerts

Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when an attack is detected in the **Attack Alert** screen *(Figure 14-6* - check the **Generate alert when attack detected** checkbox) or when a rule is matched in the **Rule Config** screen (see *Figure 15-4)*. When an event generates an alert, a message is immediately sent to an e-mail account specified by you. Enter the complete e-mail address to which alert messages will be sent in the **E-mail Alerts To** field and schedule times for sending alerts in the **Log Timer** fields in the **E-mail** screen (following screen).

Click **Advanced Setup**, **Firewall**, and then **E-mail** to bring up the following screen.

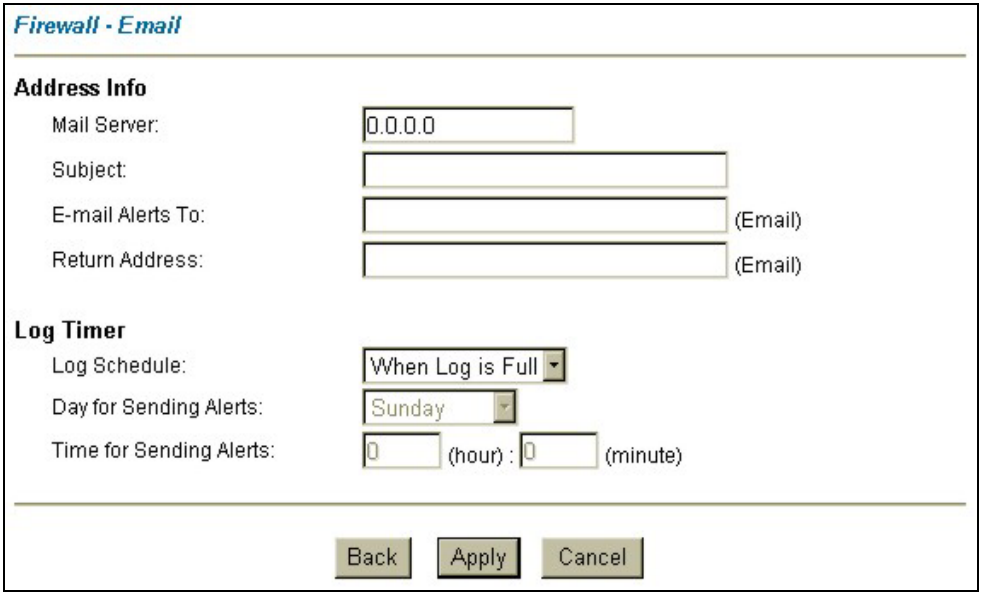


Figure 14-4 E-mail

The following table describes the fields in this screen.

Table 14-2 E-mail

FIELD	DESCRIPTION	EXAMPLE
Address Info		
Mail Server	Enter the IP address of your mail server in dotted decimal notation. Your Internet Service Provider (ISP) should be able to provide this information. If this field is left blank, log and alert messages will not be sent via e-mail.	
Subject	Enter a subject that you want to appear in the subject field of your e-mail here (see *Figure 14-5)*. If you leave this field blank then the default "Firewall Alert From Prestige" displays as your e-mail subject.	
E-mail Alerts To	Enter the e-mail address of whoever is responsible for maintaining the firewall, e.g., your system administrator. If this field is left blank, alert messages will not be sent via e-mail.	username@mydomain.com
Return Address	Enter an e-mail address to identify the Prestige as the sender of the e-mail messages i.e., a "return-to-sender" address for backup purposes.	returnaddress@prestige.com
Log Timer Log Schedule	This pop-up menu is used to configure the frequency of log messages being sent as e-mail: daily, weekly, hourly, only when the log is full or none. If the **Weekly** or the **Daily** option is selected, specify a time of day when the e-mail should be sent. If the **Weekly** option is selected, then also specify which day of the week the e-mail should be sent. If the **When Log is Full** option is selected, an alert is sent when the log fills up. If you select **None**, no log messages are e-mailed.	**Hourly**
Day for Sending Alerts	Click which day of the week you want to send the alert from the drop down list box.	**Sunday**
Time for Sending Alerts	Click the up or down arrows to the right of the list box to choose a time to send the alerts.	
Click **Back** to return to the previous screen. Click **Apply** to save your customized settings and exit this screen. Click **Cancel** to return to the previous configuration. Use the **Help** icon to find field descriptions.		

14.3.2 SMTP Error Messages

If there are difficulties in sending e-mail the following error messages appear. Please see the *Support Notes* on the included disk for information on other types of error messages.

E-mail error messages appear in SMT menu 24.3.1 as "SMTP action request failed. ret= ??". The "??"are described in the following table.

Table 14-3 SMTP Error Messages

-1 means Prestige out of socket
-2 means tcp SYN fail
-3 means smtp server OK fail
-4 means HELO fail
-5 means MAIL FROM fail
-6 means RCPT TO fail
-7 means DATA fail
-8 means mail data send fail

14.3.3 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

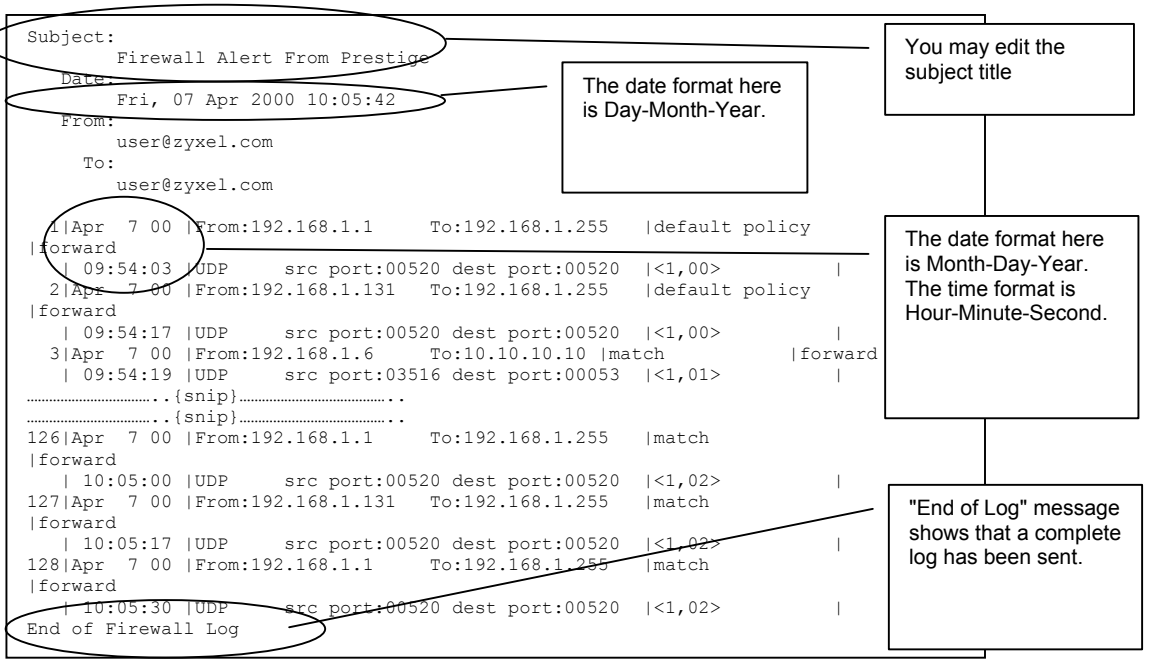


Figure 14-5 E-mail Log

14.4 Attack Alert

Attack alerts are real-time reports of DoS attacks. In the **Attack Alert** screen, shown later, you may choose to generate an alert whenever an attack is detected. For DoS attacks, the Prestige uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions.

You can use the default threshold values, or you can change them to values more suitable to your security requirements.

14.4.1 Threshold Values

Tune these parameters when something is not working and after you have checked the firewall counters. These default values should work fine for most small offices. Factors influencing choices for threshold values are:

1. The maximum number of opened sessions.

2. The minimum capacity of server backlog in your LAN network.
3. The CPU power of servers in your LAN network.
4. Network bandwidth.
5. Type of traffic for certain servers.

If your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy), then the default values should be reduced.
You should make any changes to the threshold values before you continue configuring firewall rules.

14.4.2 Half-Open Sessions

An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) could indicate that a Denial of Service attack is occurring. For TCP, "half-open" means that the session has not reached the established state-the TCP three-way handshake has not yet been completed (see *Figure 12-2*). For UDP, "half-open" means that the firewall has detected no return traffic.

The Prestige measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (**max-incomplete high**), the Prestige starts deleting half-open sessions as required to accommodate new connection requests. The Prestige continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (**max-incomplete low**).

When the rate of new connection attempts rises above a threshold (**one-minute high**), the Prestige starts deleting half-open sessions as required to accommodate new connection requests. The Prestige continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (**one-minute low**). The rate is the number of new attempts detected in the last one-minute sample period.

TCP Maximum Incomplete and Blocking Time

An unusually high number of half-open sessions with the same destination host address could indicate that a Denial of Service attack is being launched against the host.

Whenever the number of half-open sessions with the same destination host address rises above a threshold (**TCP Maximum Incomplete**), the Prestige starts deleting half-open sessions according to one of the following methods:

1. If the **Blocking Time** timeout is 0 (the default), then the Prestige deletes the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.

2. If the **Blocking Time** timeout is greater than 0, then the Prestige blocks all new connection requests to the host giving the server time to handle the present connections. The Prestige continues to block all new connection requests until the **Blocking Time** expires.

The Prestige also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections. Click **Advanced Setup**, **Firewall**, and **Alert** to bring up the next screen.

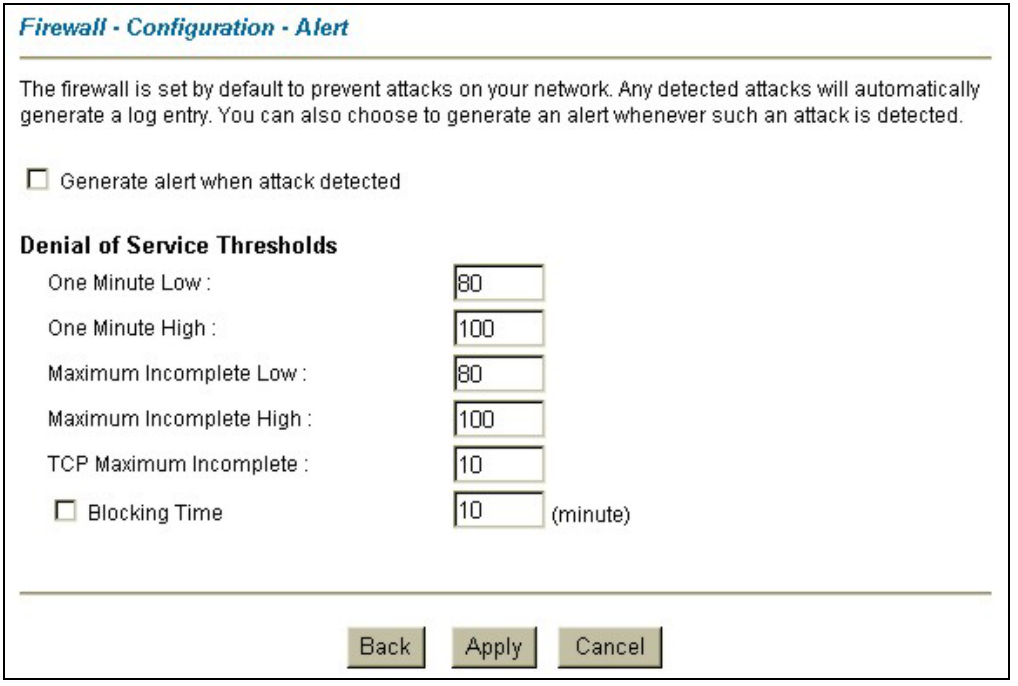


Figure 14-6 Attack Alert

The following table describes the fields in this screen.

Table 14-4 Attack Alert

FIELD	DESCRIPTION	DEFAULT VALUES
Generate alert when attack detected	A detected attack automatically generates a log entry. Check this box to generate an alert (as well as a log) whenever an attack is detected. See the *Logs Chapter* for more information on logs and alerts.	

Table 14-4 Attack Alert

Denial of Service Thresholds		
One Minute Low	This is the rate of new half-open sessions that causes the firewall to stop deleting half-open sessions. The Prestige continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.	80 existing half-open sessions.
One Minute High	This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the Prestige deletes half-open sessions as required to accommodate new connection attempts.	100 half-open sessions per minute. The above numbers cause the Prestige to start deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 80 session establishment attempts have been detected in the last minute.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The Prestige continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.	80 existing half-open sessions.
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the Prestige deletes half-open sessions as required to accommodate new connection requests. Do not set **Maximum Incomplete High** to lower than the current **Maximum Incomplete Low** number.	100 half-open sessions per minute. The above values causes the Prestige to start deleting half-open sessions when the number of existing half-open sessions rises above 100, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 80.

Table 14-4 Attack Alert

TCP Maximum Incomplete	This is the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 250. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth.	10 existing half-open TCP sessions.
Blocking Time	When **TCP Maximum Incomplete** is reached you can choose if the next session should be allowed or blocked. If you select the **Blocking Time** checkbox, any new sessions will be blocked for the length of time you specify in the next field (min) and all old incomplete sessions will be cleared during this period. If you want strong security, it is better to block the traffic for a short time, as it will give the server some time to digest the loading.	10 minutes (default)
(minute)	Enter the length of **Blocking Time** in minutes.	0
Click **Back** to return to the previous screen. Click **Apply** to save your customized settings and exit this screen. Click **Cancel** to return to the previous configuration. Use the **Help** icon to view field descriptions.		

Chapter 15
Creating Custom Rules

This chapter contains instructions for defining both Local Network and Internet rules.

15.1 Rules Overview

Firewall rules are subdivided into "Local Network" and "Internet". By default, the Prestige's stateful packet inspection allows all communications to the Internet that originate from the local network, and blocks all traffic to the LAN that originates from the Internet. You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

You might inadvertently introduce security risks to the firewall and to the protected network, if you try to configure rules without a good understanding of how rules work. Make sure you test your rules after you configure them.

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a Web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing network traffic's Source IP address, Destination IP address, IP protocol type to rules set by the administrator. Your customized rules take precedence, and may override the Prestige's default rules.

15.2 Rule Logic Overview

Study these points carefully before configuring rules.

15.2.1 Rule Checklist

1. State the intent of the rule. For example, "This restricts all IRC access from the LAN to the Internet." Or, "This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server."

2. Is the intent of the rule to forward or block traffic?
3. What is the direction connection: from the LAN to the Internet, or from the Internet to the LAN?
4. What IP services will be affected?
5. What computers on the LAN are to be affected (if any)?
6. What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

15.2.2 Security Ramifications

Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:

1. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
2. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
3. Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
4. Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the **Rules** screen in the web configurator.

15.2.3 Key Fields For Configuring Rules

Action

Should the action be to **Block** or **Forward**?

"Block" means the firewall silently discards the packet.

Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See *section 15.5* for more information on predefined services.

Source Address

What is the connection's source address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

Destination Address

What is the connection's destination address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

15.3 Connection Direction

This section talks about configuring firewall rules for connections going from LAN to WAN and WAN to LAN in your firewall.

15.3.1 LAN to WAN Rules

The default rule for LAN to WAN traffic is that all users on the LAN are allowed non-restricted access to the WAN. When you configure Policy -> LAN to WAN -> Rules, you in essence want to limit some or all users from accessing certain services on the WAN. See the following figure.

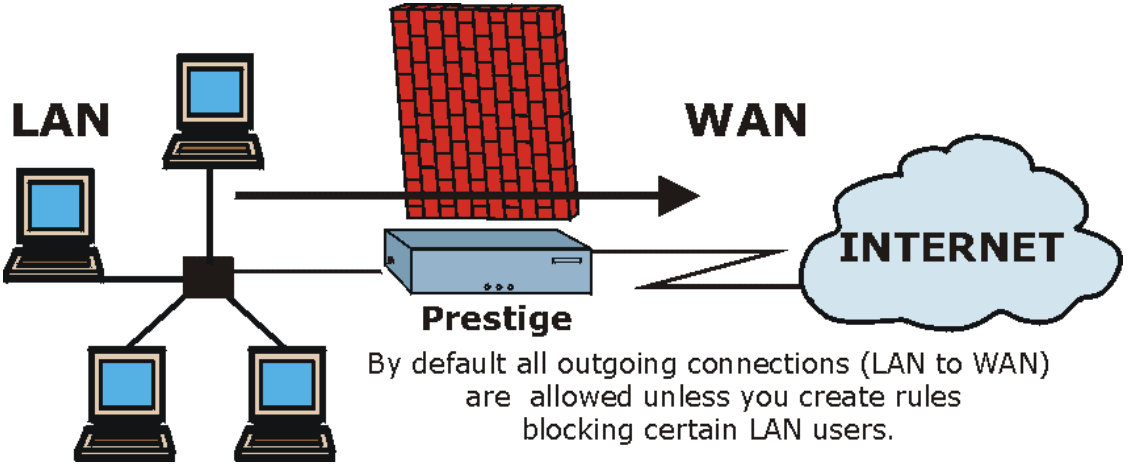


Figure 15-1 LAN to WAN Traffic

15.3.2 WAN to LAN Rules

The default rule for WAN to LAN traffic blocks all incoming connections (WAN to LAN). If you wish to allow certain WAN users to have access to your LAN, you will need to create custom rules to allow it.

See the following figure.

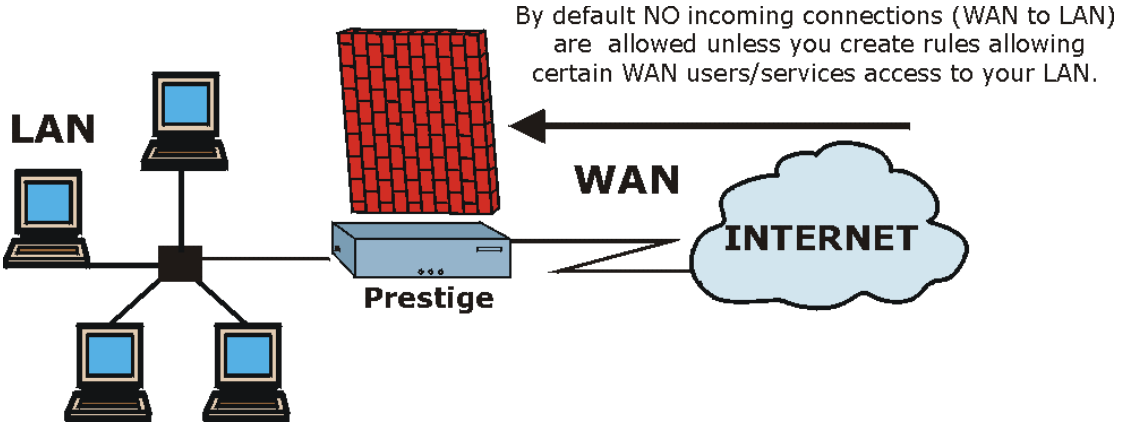


Figure 15-2 WAN to LAN Traffic

15.4 Rule Summary

The fields in the Rule Summary **screens are the same for** Local Network **and** Internet**, so the discussion below refers to both.**

Click on **Firewall**, then **Rules Summary** for **Local Network to Internet Set** or **Internet to Local Network Set** to bring up the following screen. This screen is a summary of the existing rules. Note the order in which the rules are listed.

The ordering of your rules is very important as rules are applied in turn.

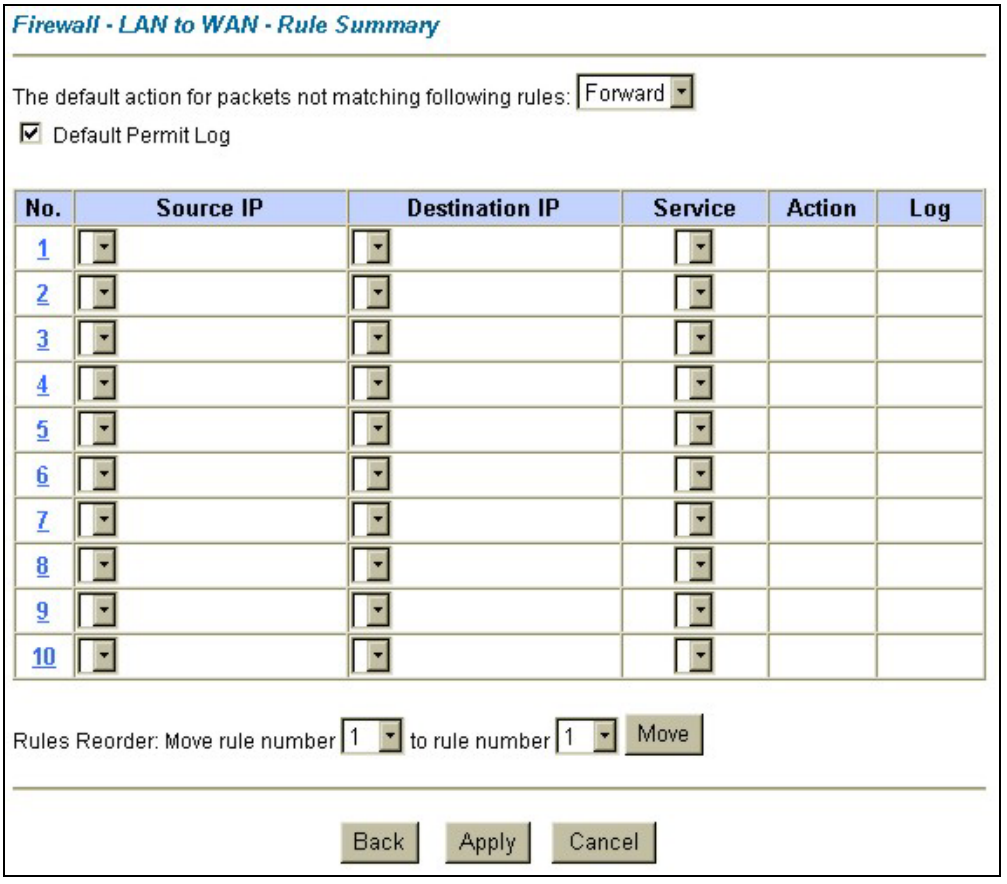


Figure 15-3 Firewall Rules Summary: First Screen

Table 15-1 Firewall Rules Summary: First Screen

FIELD	DESCRIPTION	EXAMPLE
The default action for packets not matching following rules:	Should packets that do not match the following rules be blocked or forwarded? Make your choice from the drop down list box. Note that "block" means the firewall silently discards the packet.	**Forward**
Default Permit Log	Select this check box to log all matched rules in the ACL default set.	

Table 15-1 Firewall Rules Summary: First Screen

FIELD	DESCRIPTION	EXAMPLE
The following fields summarize the rules you have created. Note that these fields are read only. Click the tab at the top of the box to order the rules according to that tab.		
No.	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. The **Move** field below allows you to reorder your rules. Click a rule's number to edit the rule.	
Source IP	This is the source address of the packet.	
Destination IP	This is the destination address of the packet.	
Service	This is the service to which the rule applies. See *Table 15-2* for more information.	
Action	This is the specified action for that rule. Note that **Block** means the firewall silently discards the packet.	**Block**
Log	This field shows you if a log is created for packets that match the rule (**Match**), don't match the rule (**Not Match**), both (**Both**) or no log is created (**None**).	**None**
Rules Reorder: Move rule number	You may reorder your rules using this function. Select by clicking on the rule you want to move. The ordering of your rules is important as rules are applied in turn.	
to rule number	Select the number you want to move the rule to.	
Move	Click **Move** to move the rule.	
Click **Back** to return to the previous screen. Click **Apply** to save your customized settings and exit this screen. Click **Cancel** to return to the previous configuration. Click the **Help** icon for field descriptions.		

15.5 Predefined Services

The **Available Services** list box in the **Edit Rule** screen (see *Figure 15-4*) displays all predefined services that the Prestige already supports. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the default configuration labeled "(**DNS**)". **(UDP/TCP:53)** means UDP port 53 and TCP port 53. Up to 128 entries are supported. Custom services may also be configured using the **Custom Ports** function discussed later.

Table 15-2 Predefined Services

SERVICE	DESCRIPTION
AIM(TCP:5190)	AOL's Internet Messenger service, used as a listening port by ICQ.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323(TCP:1720)	Net Meeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IKE(UDP:500)	The Internet Key Exchange algorithm is used for key distribution and management.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file-sharing for network environments.

Table 15-2 Predefined Services

NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS(TCP/UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRM WORKS(UDP:1558)	Stream Works Protocol.

Table 15-2 Predefined Services

TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.

15.5.1 Creating/Editing Firewall Rules

To create a new rule, click a number (**No.**) in the last screen shown to display the following screen.

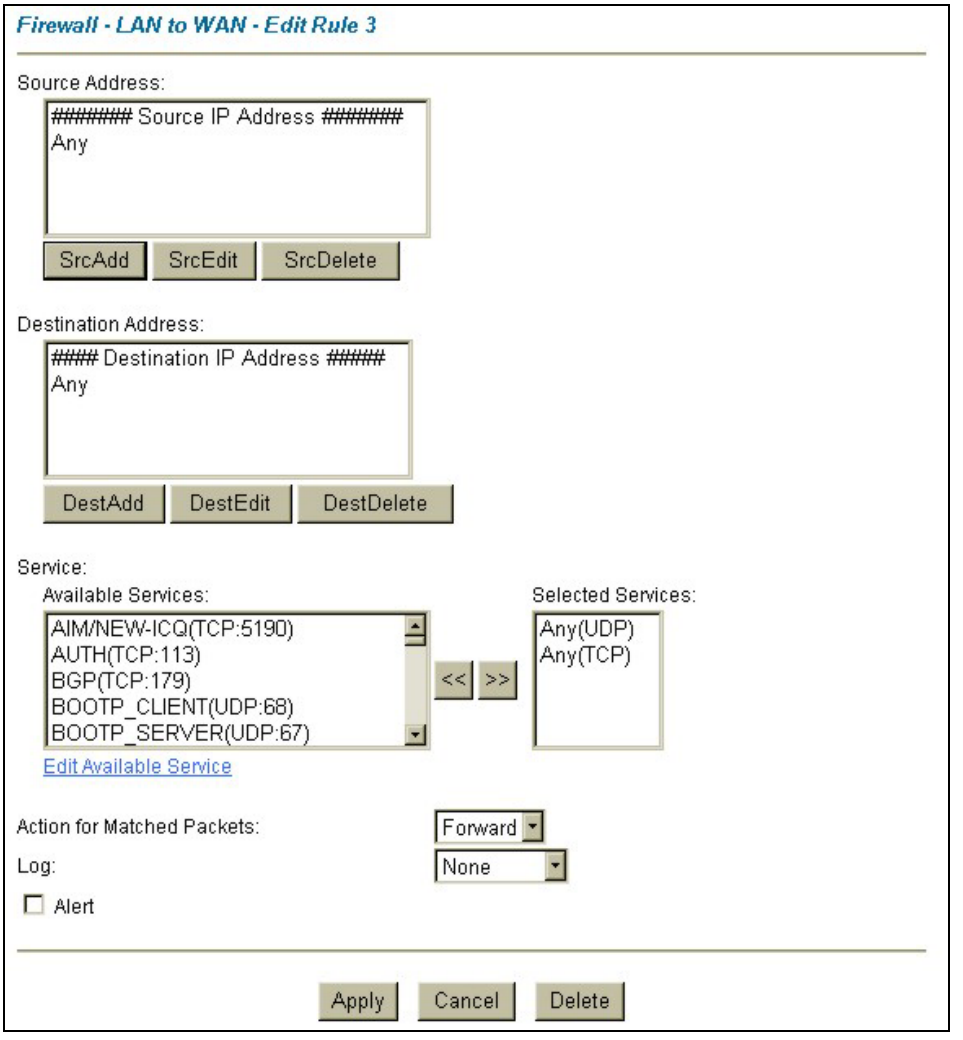


Figure 15-4 Creating/Editing A Firewall Rule

The following table describes the fields in this screen.

Table 15-3 Creating/Editing A Firewall Rule

FIELD	DESCRIPTION	EXAMPLE
Source Address:	Click **SrcAdd** to add a new address, **SrcEdit** to edit an existing one or **SrcDelete** to delete one. Please see the next section for more information on adding and editing source addresses.	**SrcAdd**
Destination Address:	Click **DestAdd** to add a new address, **DestEdit** to edit an existing one or **DestDelete** to delete one. Please see the following section on adding and editing destination addresses.	**DestAdd**
Service: Available/Selected Services:	Please see *Table 15-2* for more information on services available. Highlight a service from the **Available Services** box on the left, then click **>>** to add it to the **Selected Services** box on the right. To remove a service, highlight it in the **Selected Services** box on the right, then click **<<**.	
Edit Available Service	Click this button to go to the list of available custom services.	
Action for Matched Packets:	Should packets that match this rule be blocked or forwarded? Make your choice from the drop down list box. Note that **Block** means the firewall silently discards the packet.	**Block**
Log:	This field determines if a log is created for packets that match the rule, don't match the rule, both or no log is created.	**Match**
Alert	Check the **Alert** check box to determine that this rule generates an alert when the rule is matched.	
Click **Back** to return to the previous screen. Click **Apply** to save your customized settings and exit this screen. Click **Cancel** to exit this screen without saving. Use the **Help** icon to view field descriptions.		

15.5.2 Source and Destination Addresses

To add a new source or destination address, click **SrcAdd** or **DestAdd** from the previous screen. To edit an existing source or destination address, select it from the box and click **SrcEdit** or **DestEdit** from the previous screen**.** Either action displays the following screen.

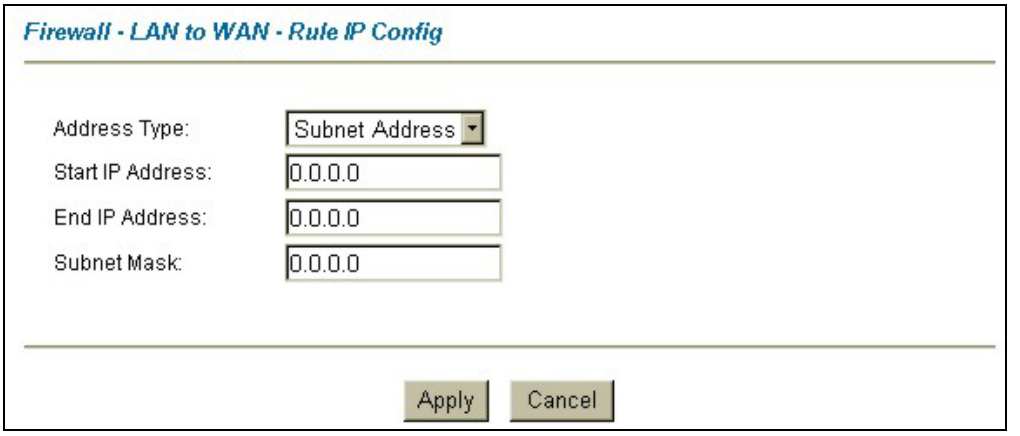


Figure 15-5 Adding/Editing Source and Destination Addresses

The following table describes the fields in this screen.

Table 15-4 Adding/Editing Source and Destination Addresses

FIELD	DESCRIPTION	EXAMPLE
Address Type	Do you want your rule to apply to packets with a particular (single) IP address, a range of IP addresses (e.g., 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop down list box	**Subnet Address**
Start IP Address	Enter the single IP address or the starting IP address in a range here.	
End IP Address	Enter the ending IP address in a range here.	
Subnet Mask	Enter the subnet mask here, if applicable.	
Click **Apply** to save your customized settings and exit this screen. Click **Cancel** to return to the previous configuration. Use the **Help** icon to view field descriptions.		

15.6 Timeout

The fields in the Timeout **screens are the same for** Local **and** Internet networks**, so the discussion below refers to both.**

15.6.1 Configuring Timeout Values

The factors influencing choices for timeout values are the same as the factors influencing choices for threshold values – see *section 14.4.1*. Click **Timeout** for either **Local Network to Internet Set** or **Internet to Local Network Set**.

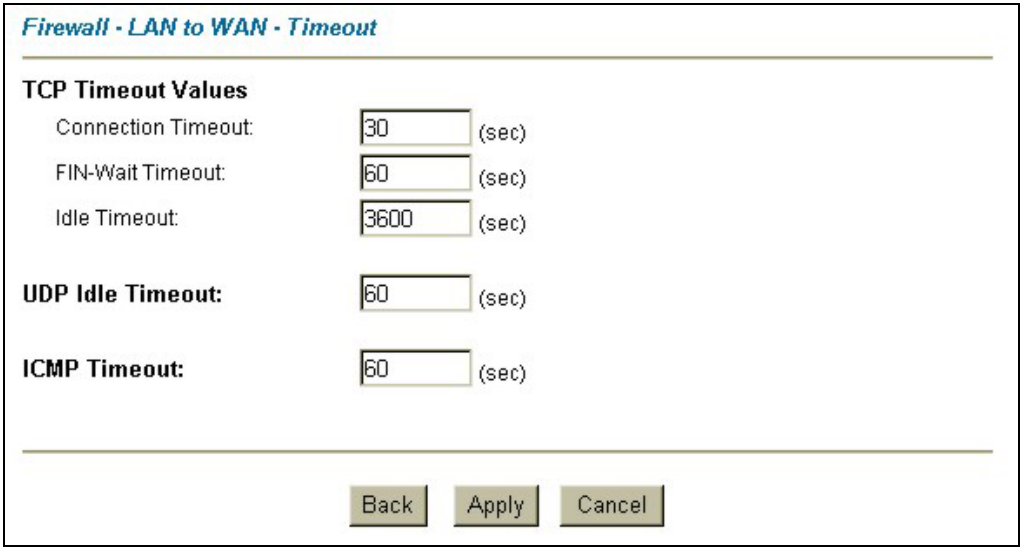


Figure 15-6 Timeout Screen

The following table describes the fields in this screen.

Table 15-5 Timeout Menu

FIELD	DESCRIPTION	DEFAULT VALUE
TCP Timeout Values		
Connection Timeout	This is the length of time the Prestige waits for a TCP session to reach the established state before dropping the session.	30 seconds
FIN-Wait Timeout	This is the length of time a TCP session remains open after the firewall detects a FIN-exchange (indicating the end of the TCP session).	60 seconds

Idle Timeout	This is the length of time of inactivity a TCP connection remains open before the Prestige considers the connection closed.	3600 seconds (1 hour)
UDP Idle Timeout	This is the length of time of inactivity a UDP connection remains open before the Prestige considers the connection closed.	60 seconds
ICMP Timeout	This is the length of time an ICMP session waits for the ICMP response.	60 seconds
Click **Back** to return to the previous screen. Click **Apply** to save your customized settings and exit this screen. Click **Cancel** to return to the previous configuration. Use the **Help** icon to view field descriptions.		

Chapter 16
Customized Services

This chapter covers creating, viewing and editing custom services.

16.1 Customized Services Overview

Configure customized services and port numbers not predefined by the Prestige (see *Figure 15-4)*. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. For further information on these services, please read *section 15.5*. To configure a custom service, click **Edit Available Service** in an edit rule screen to bring up the following screen.

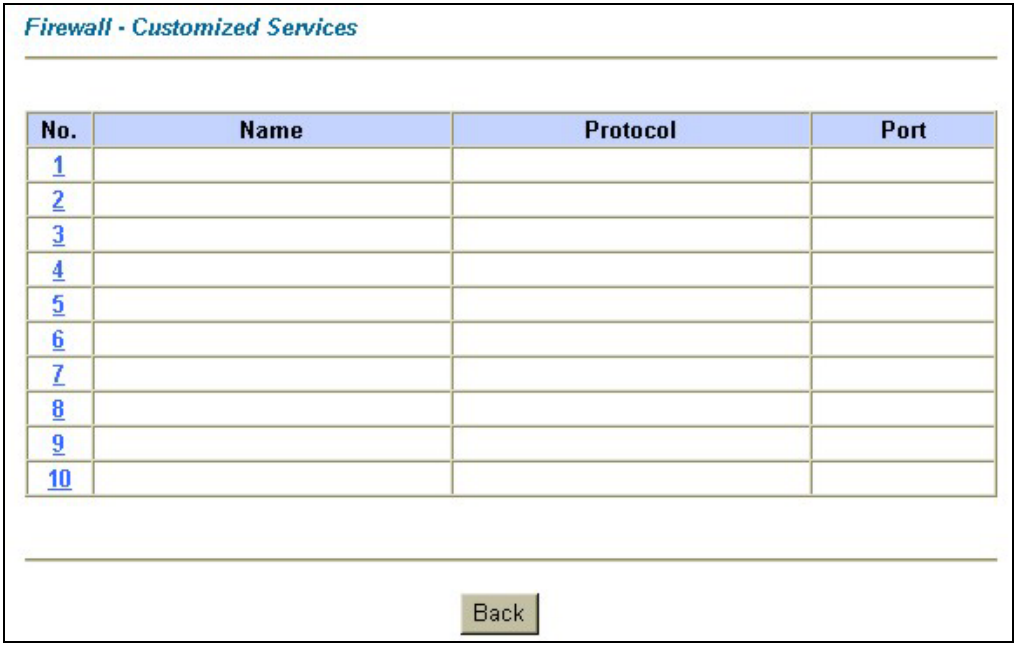


Figure 16-1 Customized Services

The following table describes the fields in this screen.

Table 16-1 Customized Services

FIELD	DESCRIPTION
No.	This is the number of your customized port. Click a rule's number to edit the rule.
Name	This is the name of your customized port.
Protocol	This shows the IP protocol (TCP, UDP or Both) that defines your customized port.
Port	This is the port number or range that defines your customized port.
Use the **Help** icon for field descriptions. When you have finished viewing this screen, click another link to exit. Click **Back** to return to the previous screen.	

16.2 Creating/Editing A Customized Service

Click a rule number in the previous screen to create a new custom port or edit an existing one. This action displays the following screen.

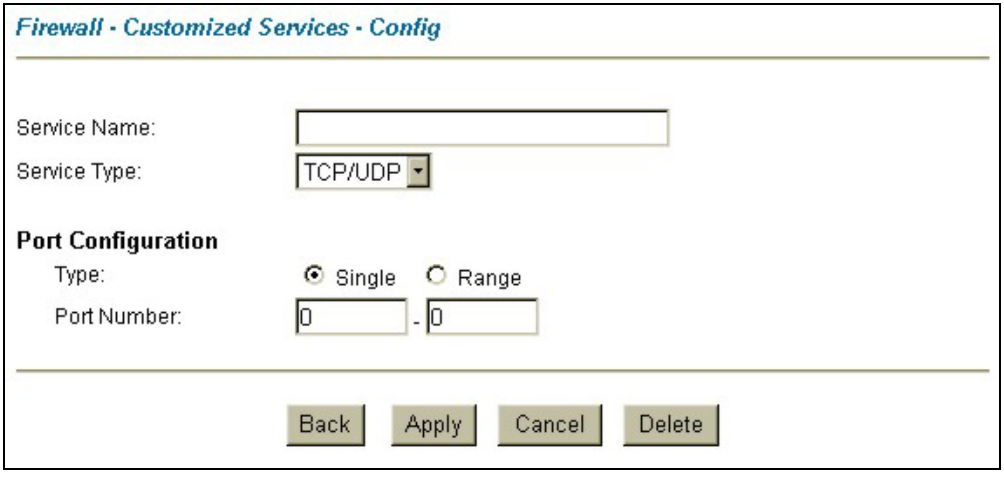


Figure 16-2 Creating/Editing A Customized Service

The next table describes the fields in this screen.

Table 16-2 Creating/Editing A Custom Port

FIELD	DESCRIPTION	EXAMPLE
Service Name	Enter a unique name for your custom port.	
Service Type	Choose the IP port (**TCP**, **UDP** or **TCP/UDP**) that defines your customized port from the drop down list box.	**TCP/UDP**
Port Configuration		
Type	Click **Single** to specify one port only or **Range** to specify a span of ports that define your customized service.	**Single** **Range**
Port Number	Enter a single port number or the range of port numbers that define your customized service.	
Click **Back** to return to the previous screen. When you have finished, click **Apply** to save your customized settings and exit this screen, **Cancel** to return to the previously saved settings, **Delete** to remove this customized service. Click the **Help** icon for field descriptions.		

16.3 Example Firewall Rule

The following are some Internet firewall rule examples that allow DHCP negotiation between the ISP and the Prestige and allow a syslog connection from the Internet. Follow the procedure shown next to first configure a custom port.

Step 1. Click **Rule Summary** under **Internet to Local Network Set**.

Step 2. Click a rule number to open the edit rule screen.

Step 3. Click **Any** in the Source Address box and then click **ScrDelete**.

Step 4. Click **ScrAdd** to open the Rule IP Config screen. Configure it as follows and click **Apply**.

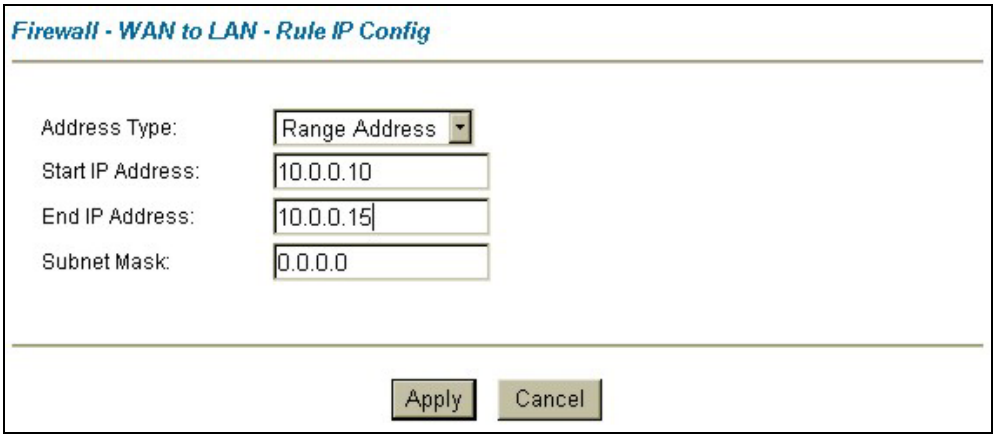


Figure 16-3 Configure Source IP

Step 5. Click **Edit Available Service** in the edit rule screen and then click a rule number to bring up the **Firewall Customized Services Config** screen. Configure as follows.

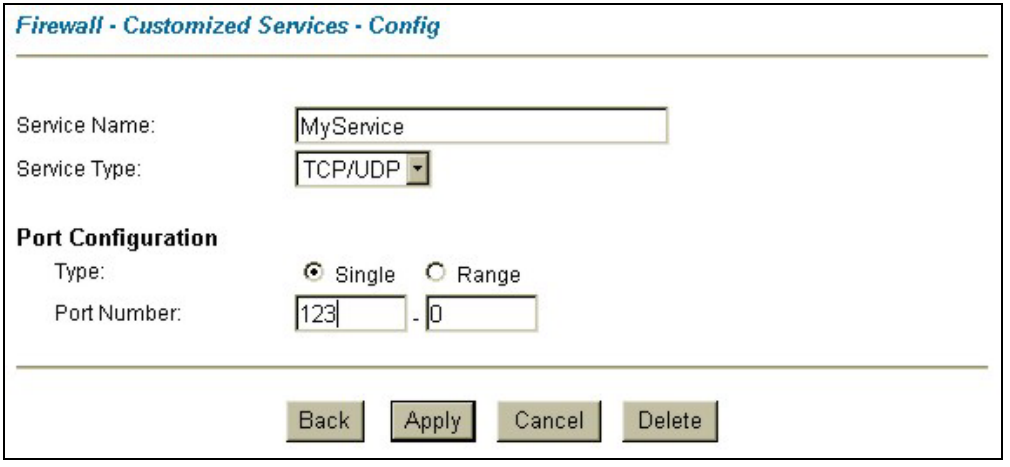


Figure 16-4 Customized Service for MyService

Customized services show up with an "*" before their names in the Services **list box and the Rule Summary list box. Click** Apply **after you've created your customized service.**

Step 5. Follow the procedures outlined earlier in this chapter to configure all your rules. Configure the rule configuration screen like the one below and apply it.

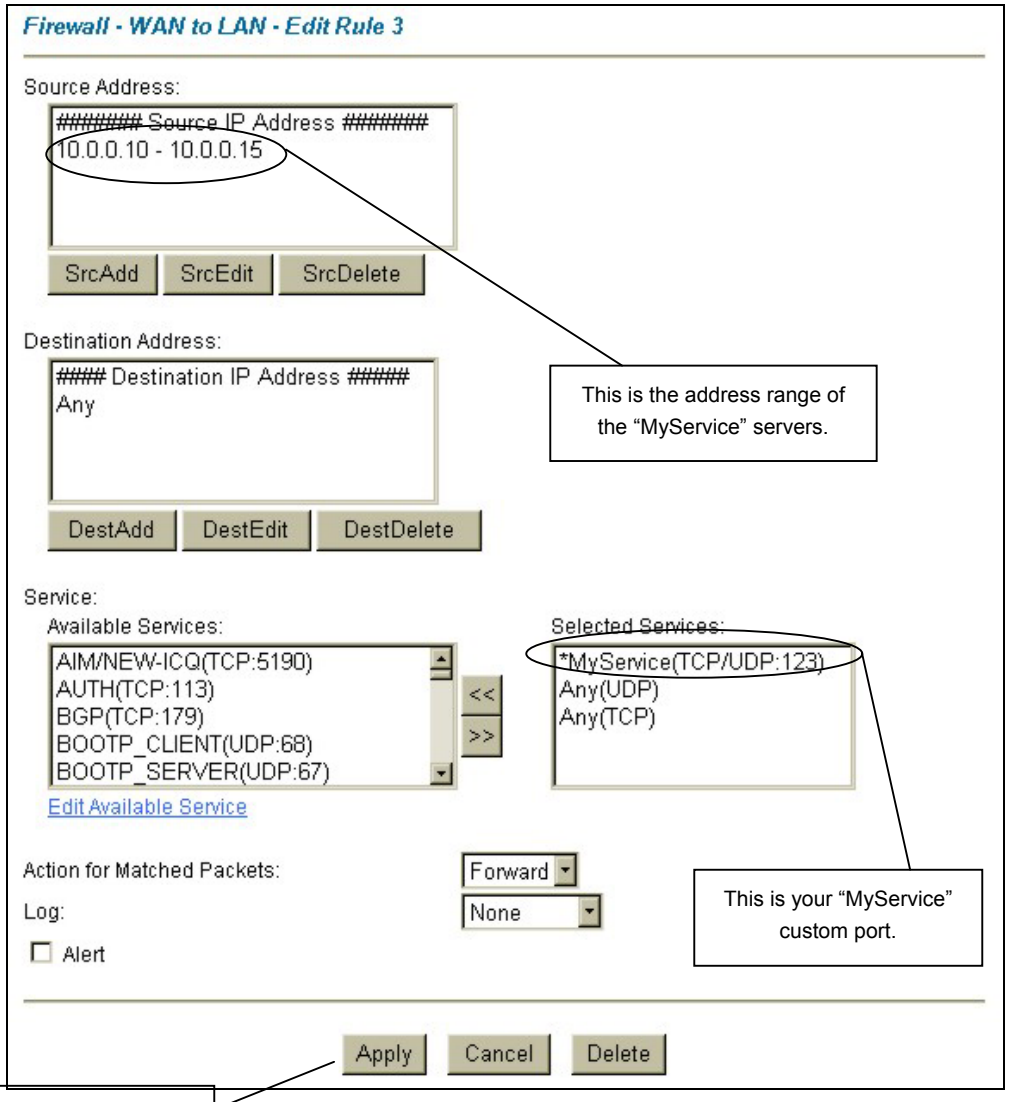


Figure 16-5 MyService Rule Configuration

Step 6. On completing the configuration procedure for these Internet firewall rules, the **Rule Summary** screen should look like the following. Don't forget to click **Apply** when you have finished configuring your rule(s) to save your settings back to the Prestige.

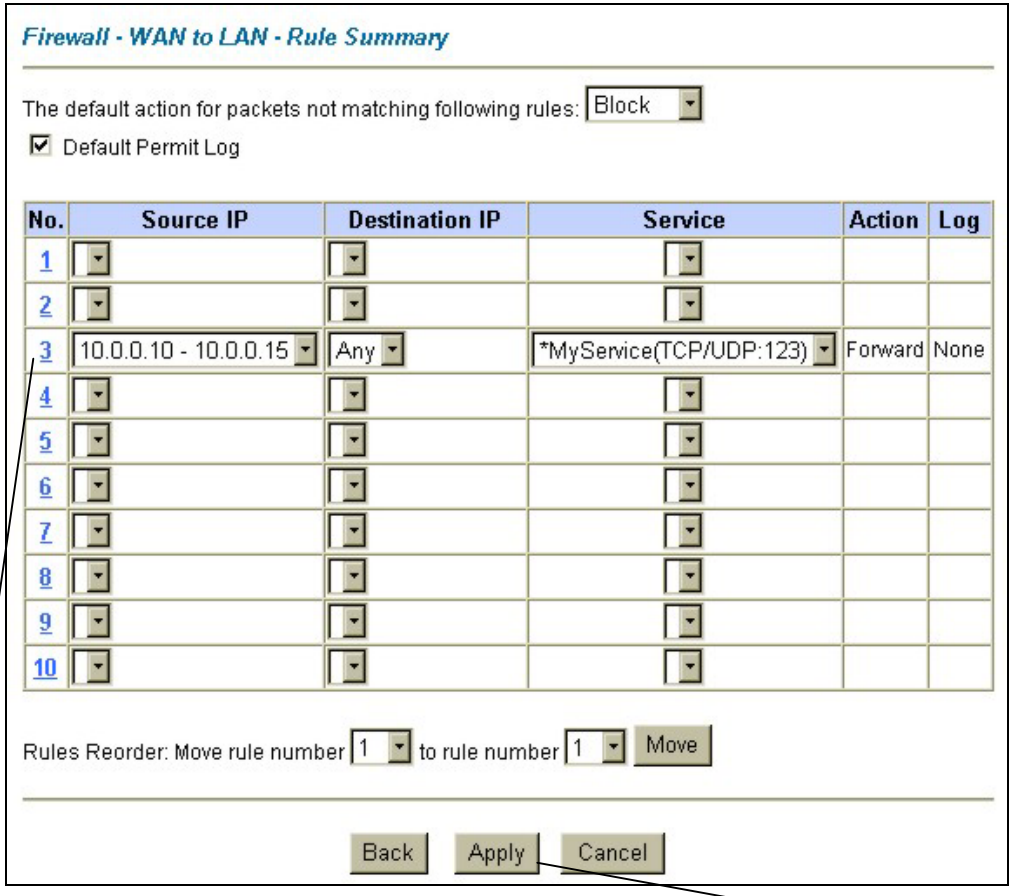


Figure 16-6 Example Rule Summary

Rule 3: Allows a "MyService" connection from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 on the LAN.

Click **Apply** to save your settings back to the Prestige.

Chapter 17
Firewall Logs

This chapter contains information about using the log screen to view the results of the rules you have configured.

17.1 Log Screen

When you configure a new rule you also have the option to log events that match, don't match (or both) this rule (see *Figure 15-4*). Click **Logs** to bring up the next screen. Firewall logs may also be viewed in SMT Menu 21.3 (see *section 13.2)* or via syslog (SMT **Menu 24.3.2 - System Maintenance - UNIX Syslog**). Syslog is an industry standard protocol used for capturing log information for devices on a network. 128 entries are available numbered from 0 to 127. Once they are all used, the log wraps around and the old logs are lost.

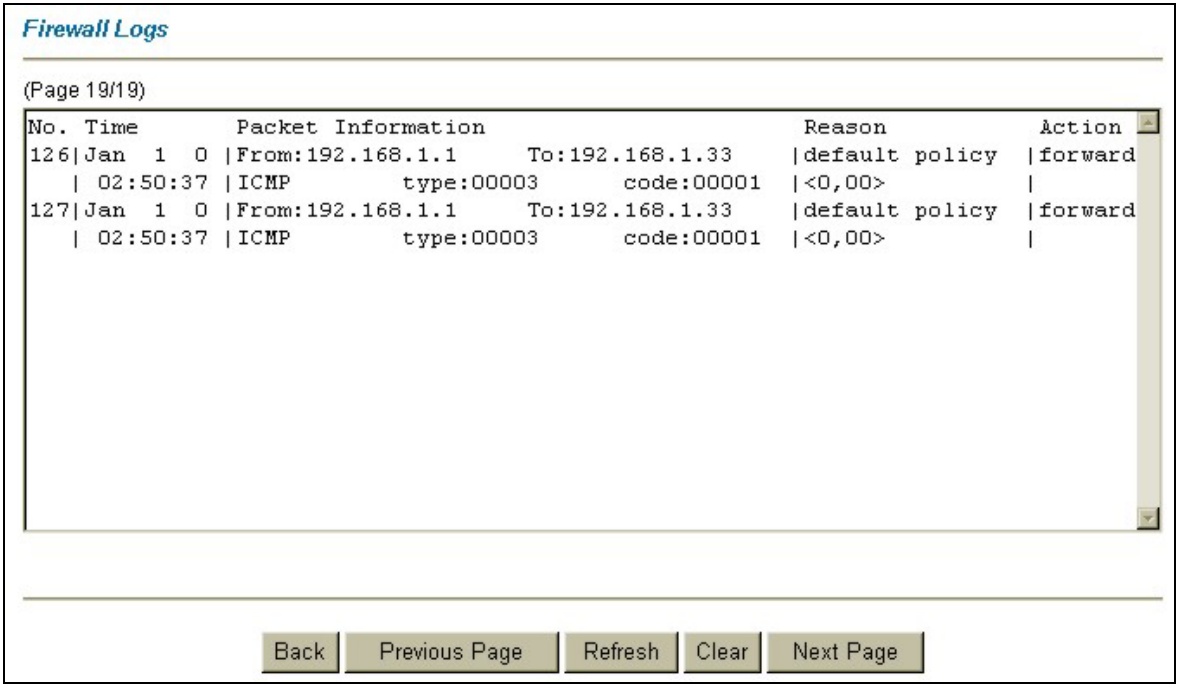


Figure 17-1 Log Screen

The following table describes the fields in this screen.

Table 17-1 Log Screen

FIELD	DESCRIPTION	EXAMPLE
No.	This is the index number of the firewall log. 128 entries are available numbered from 0 to 127. Once they are all used, the log will wrap around and the old logs will be lost.	
Time	This is the time the log was recorded in this format. You must configure menu 24.10 for real-time; otherwise the time shown in these examples is displayed.	dd:mm:yy e.g., Jan 1 0 hh:mm:ss e.g., 00:00:00
Packet Information	This field lists packet information such as:	From and To IP addresses protocol and port numbers.
Reason	This field states the reason for the log; i.e., was the rule matched, not matched, or was there an attack. The set and rule coordinates (<X, Y> where X=1,2; Y=00~10) follow with a simple explanation. There are two policy sets; set 1 (X = 1) is for LAN to WAN rules and set 2 (X = 2) for WAN to LAN rules. Y represents the rule in the set. You can configure up to 10 rules in any set (Y = 01 to 10). Rule number 00 is the default rule.	not match <1,01> dest IP This means this packet does not match the destination IP address in set 1, rule 1. Other reasons (instead of dest IP) are src IP, dest port, src port and protocol.
	This is a log for a DoS attack	attack land, ip spoofing, icmp echo, icmp vulnerability, NetBIOS, smtp illegal command, traceroute, teardrop, or syn flood.
Action	This field displays whether the packet was blocked (i.e., silently discarded), forwarded or neither (Block, Forward or None). "None" means that no action is dictated by this rule.	**Block**, **Forward** or **None**
Click **Back** to return to the previous screen. Click **Previous Page** or **Next Page** to view other pages in your log. Click **Refresh** to renew the log screen or **Clear** to clear all the logs. Click the **Help** icon for field descriptions.		

Part IV:

Advanced Management

This part discusses Filtering, SNMP, System Information and Diagnosis, Firmware and Configuration File Maintenance, System Maintenance and Information, Call Scheduling, Remote Management and Virtual Private Networking (VPN/IPSec).

Chapter 18
Filter Configuration

This chapter shows you how to create and apply filters.

18.1 Filtering Overview

Your Prestige uses filters to decide whether or not to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

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

Outgoing packets must undergo data filtering before they encounter call filtering. Call filters are divided into two groups, the built-in call filters and user-defined call filters. Your Prestige has built-in call filters that prevent administrative, for example, RIP packets from triggering calls. These filters are always enabled and not accessible to you. Your Prestige applies the built-in filters first and then the user-defined call filters, if applicable, as shown next.

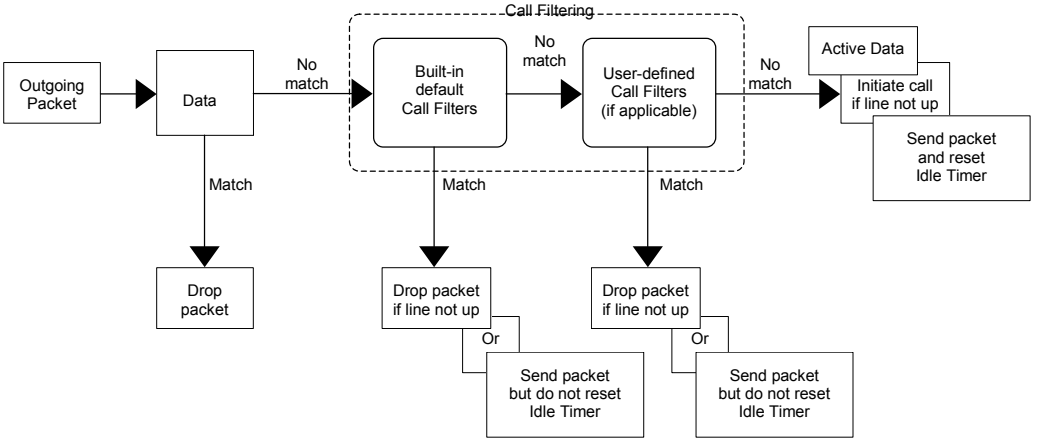


Figure 18-1 Outgoing Packet Filtering Process

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

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

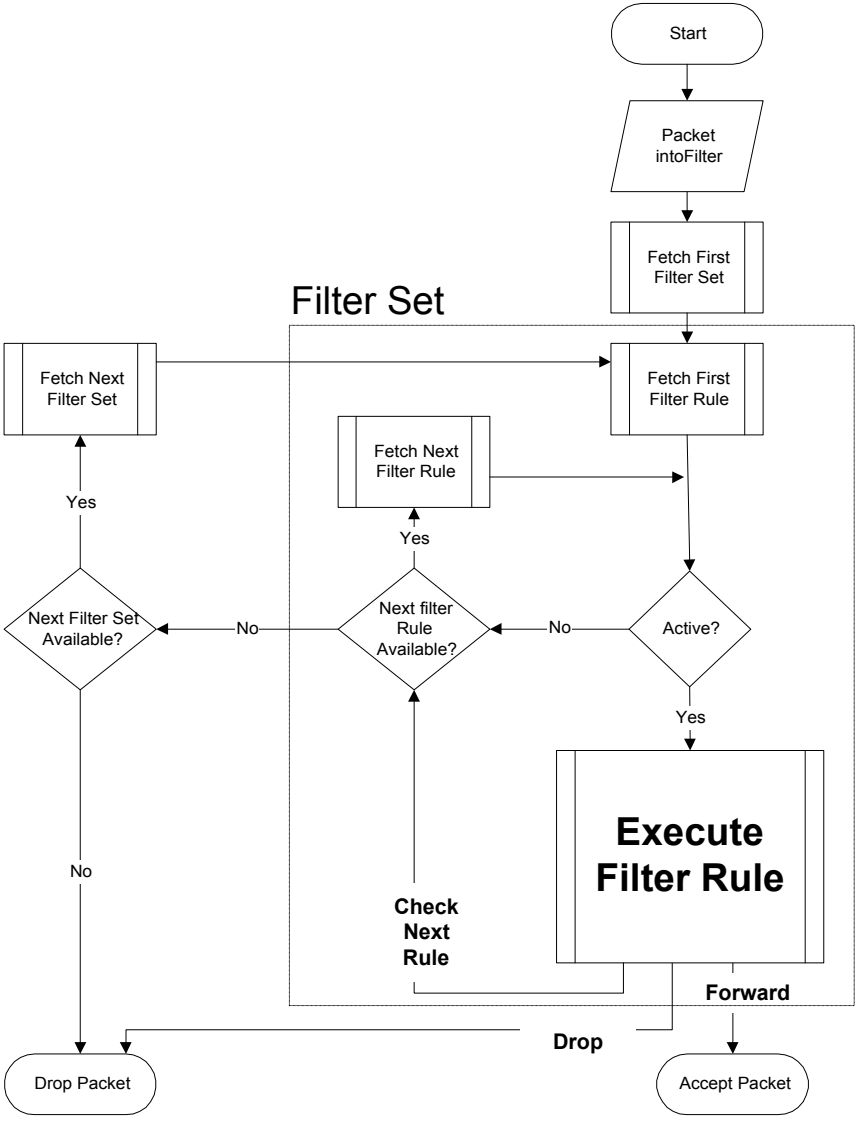


Figure 18-2 Filter Rule Process

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

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

The Filter Structure of the Prestige

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

18.2 Configuring a Filter Set

To configure a filter set, follow the steps shown next.

Step 1. Enter 21 in the main menu to open menu 21.

```
          Menu 21 - Filter and Firewall Setup

        1. Filter Setup
        2. Firewall Setup
        3. View Firewall Log

              Enter Menu Selection Number:
```

Figure 18-3 Menu 21 Filter and Firewall Setup

Step 2. Enter 1 to bring up the following menu.

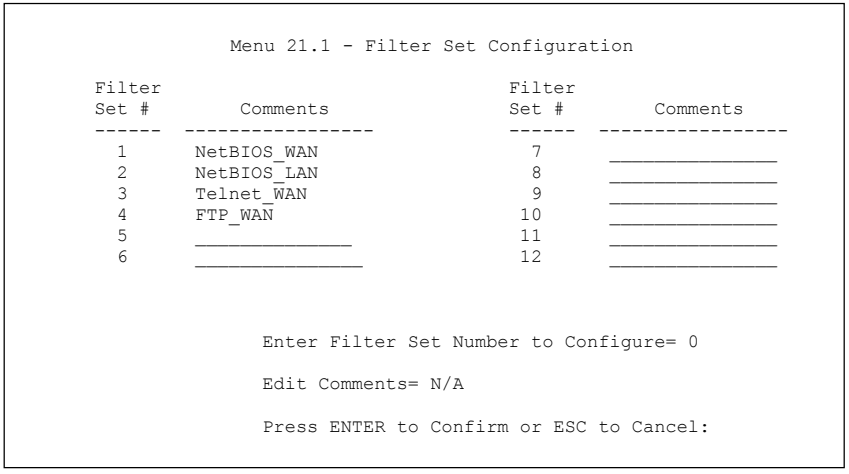


Figure 18-4 Menu 21.1 Filter Set Configuration

Step 3. Select the filter set you wish to configure (1-12) and press [ENTER].

Step 4. Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

Step 5. Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.x- Filter Rules Summary**. The following shows filter rules summary screens for filter sets 1 through 4.

```
                    Menu 21.1.1 - Filter Rules Summary

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


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

Figure 18-5 NetBIOS_WAN Filter Rules Summary

```
                    Menu 21.1.2 - Filter Rules Summary

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




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

Figure 18-6 NetBIOS _LAN Filter Rules Summary

```
                    Menu 21.1.3 - Filter Rules Summary

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




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

Figure 18-7 Telnet WAN Filter Rules Summary

```
                    Menu 21.1.4 - Filter Rules Summary
# A Type                       Filter Rules                              M m n
- - ---- ------------------------------------------------------------- - - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=21                           N D F
2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=20                           N D F
3 N
4 N
5 N
6 N




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

Figure 18-8 FTP_WAN Filter Rules Summary

18.2.1 Filter Rules Summary Menus

The following tables briefly describe the abbreviations used in the previous menus.

TABLE 18-1 FILTER RULES SUMMARY MENU ABBREVIATIONS

FIELD	DESCRIPTION
#	The filter rule number: 1 to 6.
A	Active: "Y" means the rule is active. "N" means the rule is inactive.
Type	The type of filter rule: "GEN" for Generic, "IP" for TCP/IP.
Filter Rules	These parameters are displayed here.
M	More. "Y" means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. "N" means there are no more rules to check. You can specify an action to be taken for instance, forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
m	Action Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.
n	Action Not Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

Table 18-2 Rule Abbreviations Used

FILTER TYPE	DESCRIPTION
IP	
Pr	Protocol
SA	Source Address
SP	Source Port Number
DA	Destination Address
DP	Destination Port Number
GEN	
Off	Offset
Len	Length

18.3 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.x – Filter Rules Summary** and press [ENTER] to open menu 21.1.x.x for the rule.

There are two types of filter rules: **TCP/IP** and **Generic**. Depending on the type of rule, the parameters for each type will be different. Use [SPACE BAR] to select the type of rule that you want to create in the **Filter Type** field and press [ENTER] to open the respective menu.

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

18.3.1 TCP/IP Filter Rule

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

To configure TCP/IP rules, select **TCP/IP Filter Rule** in the **Filter Type** field and press [ENTER] to open **Menu 21.1.x.x – TCP/IP Filter Rule**. The following example screen shows menu 21.1.7.1.

```
                    Menu 21.1.7.1 - TCP/IP Filter Rule
                Filter #: 4,1
                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 18-9 Menu 21.1.7.1 TCP/IP Filter Rule

Table 18-3 Menu 21.1.7.1 TCP/IP Filter Rule

FIELD	DESCRIPTION	EXAMPLE
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third filter rule of that set.	7,1
Filter Type	Use [SPACE BAR] and then [ENTER] to choose a rule. Parameters displayed for each type will be different. Choices are **TCP/IP Filter Rule** or **Generic Filter Rule**.	**TCP/IP Filter Rule**
Active	Use [SPACE BAR] and then [ENTER] to select **Yes** to activate or **No** to deactivate the filter rule.	**No** (default)
IP Protocol	This is the upper layer protocol, for example, TCP is 6, UDP is 17 and ICMP is 1. The value must be between 0 and 255. A value of O matches ANY protocol.	0 to 255
IP Source Route	IP Source Route is an optional header that dictates the route an IP packet takes from its source to its destination. If **Yes**, the rule applies to any packet with an IP source route. The majority of IP packets do not have source route.	**No** (default)
Destination: IP Addr	Type the destination IP address of the packet you want to filter. This field is ignored if it is 0.0.0.0.	IP address
IP Mask	Type the IP mask to apply to the **Destination: IP Addr** field.	IP mask

Table 18-3 Menu 21.1.7.1 TCP/IP Filter Rule

FIELD	DESCRIPTION	EXAMPLE
Port #	Type the destination port of the packets you want to filter. The field range is 0 to 65535. A 0 field is ignored.	0 to 65535
Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in **Destination: Port #.** Choices are **None**, **Less**, **Greater**, **Equal** or **Not Equal**.	**None**
Source: IP Addr	Type the source IP Address of the packet you want to filter. A 0.0.0.0 field is ignored.	IP address
IP Mask	Type the IP mask to apply to the **Source: IP Addr** field.	IP mask
Port #	Type the source port of the packets you want to filter. The range of this field is 0 to 65535. A 0 field is ignored.	0 to 65535
Port # Comp	Select the comparison to apply to the source port in the packet against the value given in **Source: Port #** field. Choices are **None**, **Less**, **Greater**, **Equal** or **Not Equal**.	**None**
TCP Estab	This applies only when the IP Protocol field is 6, TCP. If **Yes**, the rule matches packets that want to establish TCP connection(s) (SYN=1 and ACK=0); else it is ignored.	**No** (default)
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be N/A.	**No** (default)
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	Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule** (default)

Table 18-3 Menu 21.1.7.1 TCP/IP Filter Rule

FIELD	DESCRIPTION	EXAMPLE
Action Not Matched	Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule** (default)
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

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

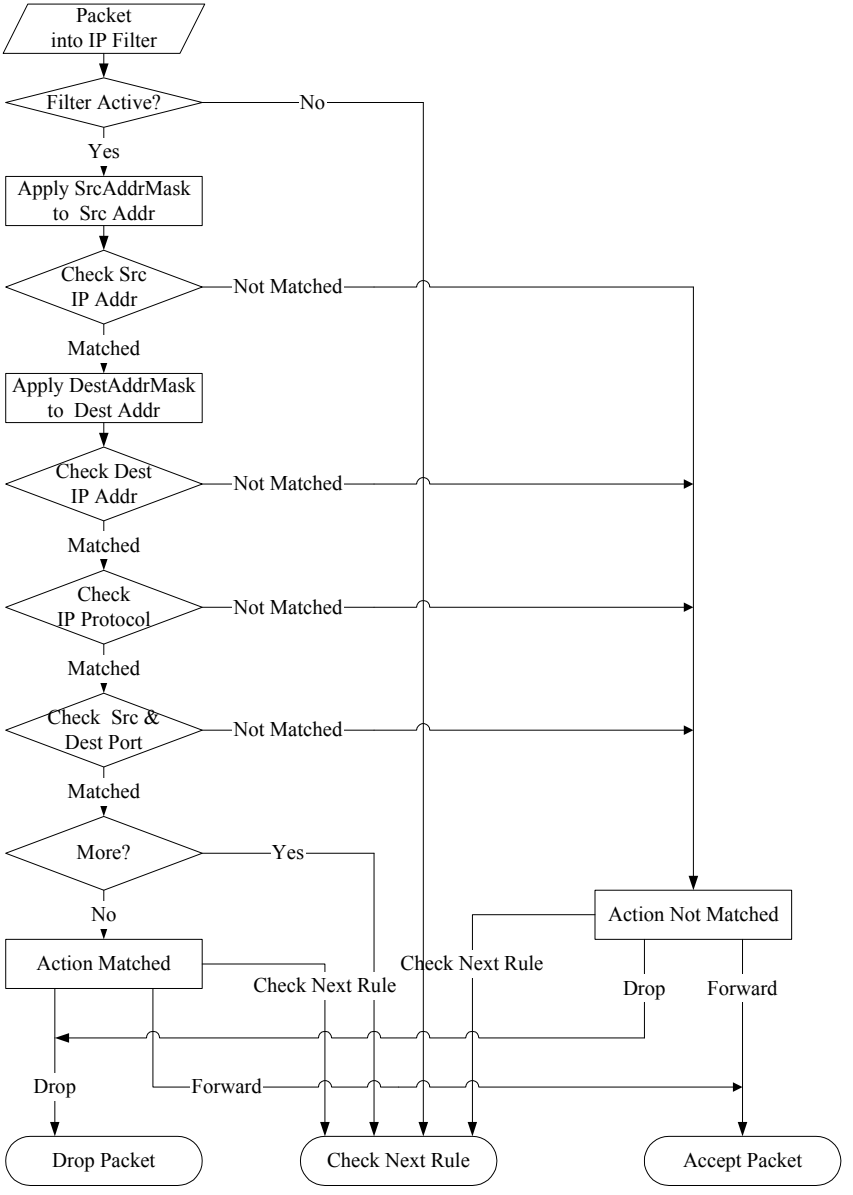


Figure 18-10 Executing an IP Filter

18.3.2 Generic Filter Rule

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

For generic rules, the Prestige treats a packet as a byte stream as opposed to an IP 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** fields are specified in hexadecimal digits. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, FFFFFFFF.

To configure a generic rule select an empty filter set in menu 21.1, for example 8. Select **Generic Filter Rule** in the **Filter Type** field and press [ENTER] to open **Menu 21.1.x.x – Generic Filter Rule**. The following example screen shows menu 21.1.8.1.

```
                    Menu 21.1.8.1 - Generic Filter Rule

                  Filter #: 5,1
                  Filter Type= Generic Filter Rule
                  Active= No
                  Offset= 0
                  Length= 0
                  Mask= N/A
                  Value= N/A
                  More= No            Log= None
                  Action Matched= Check Next Rule
                  Action Not Matched= Check Next Rule

                  Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 18-11 Menu 21.1.5.1 Generic Filter Rule

Table 18-4 Menu 21.1.5.1 Generic Filter Rule

FIELD	DESCRIPTION	EXAMPLE
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third rule of that set.	5,1

Table 18-4 Menu 21.1.5.1 Generic Filter Rule

FIELD	DESCRIPTION	EXAMPLE
Filter Type	Press [SPACE BAR] and then [ENTER] to select a type of rule. Parameters displayed below each type will be different. Choices are **Generic Filter Rule** or **TCP/IP Filter Rule**.	**Generic Filter Rule**
Active	Select **Yes** to turn on or **No** to turn off the filter rule.	**No** (default)
Offset	Type the starting byte of the data portion in the packet that you want to compare. The range for this field is from 0 to 255.	0 (default)
Length	Type the byte count of the data portion in the packet that you want to compare. The range for this field is 0 to 8.	0 (default)
Mask	Type the mask (in hexadecimal) to apply to the data portion before comparison.	
Value	Type the value (in hexadecimal) to compare with the data portion.	
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**.	**No** (default)
Log	Select the logging option from the following: **None** – No packets will be logged. **Action Matched** – Only matching packets and rules 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	Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule** (default)
Action Not Matched	Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule** (default)
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

18.4 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 IP packets.

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 where the Prestige is receiving and sending the packets; for instance, the interface. The interface can be an Ethernet, or any other hardware port. The following figure illustrates this.

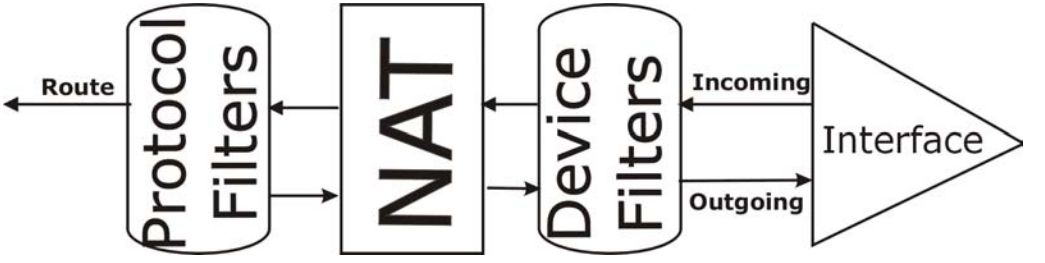


Figure 18-12 Protocol and Device Filter Sets

18.5 Example Filter

Let's look at an example to block outside users from telnetting into the Prestige.

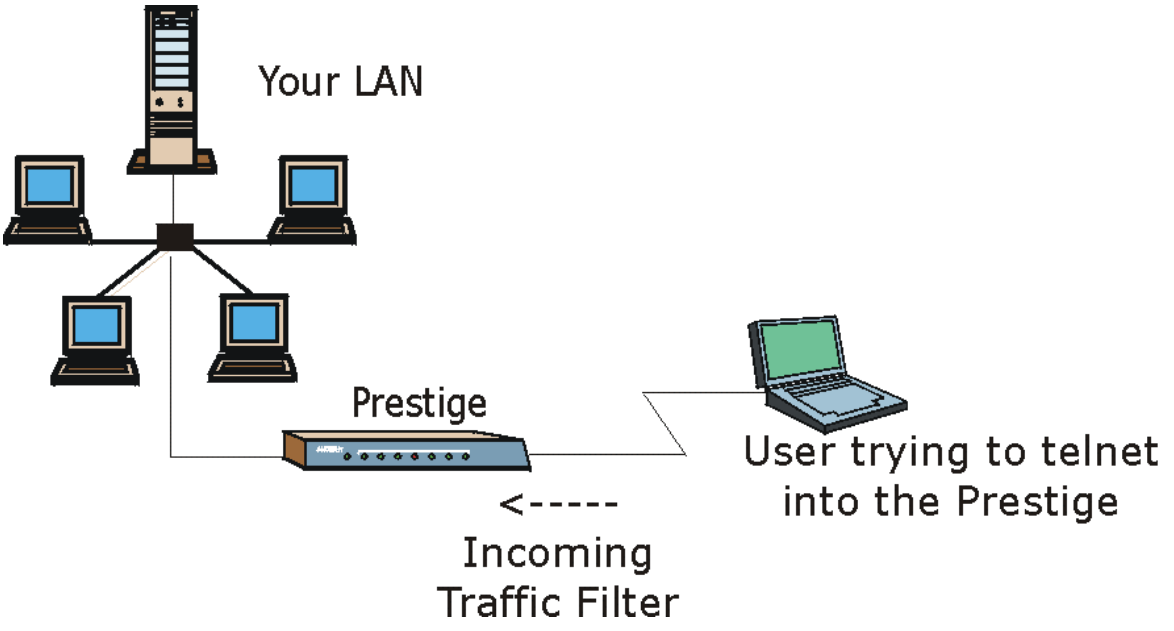


Figure 18-13 Sample Telnet Filter

Step 1. Enter 21 from the main menu to open **Menu 21 - Filter and Firewall Setup**.

Step 2. Enter 1 to open **Menu 21.1 - Filter Set Configuration**.

Step 3. Enter the index of the filter set you wish to configure (such as 4) and press [ENTER].

Step 4. Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

Step 5. Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.9 - Filter Rules Summary**.

Step 6. Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

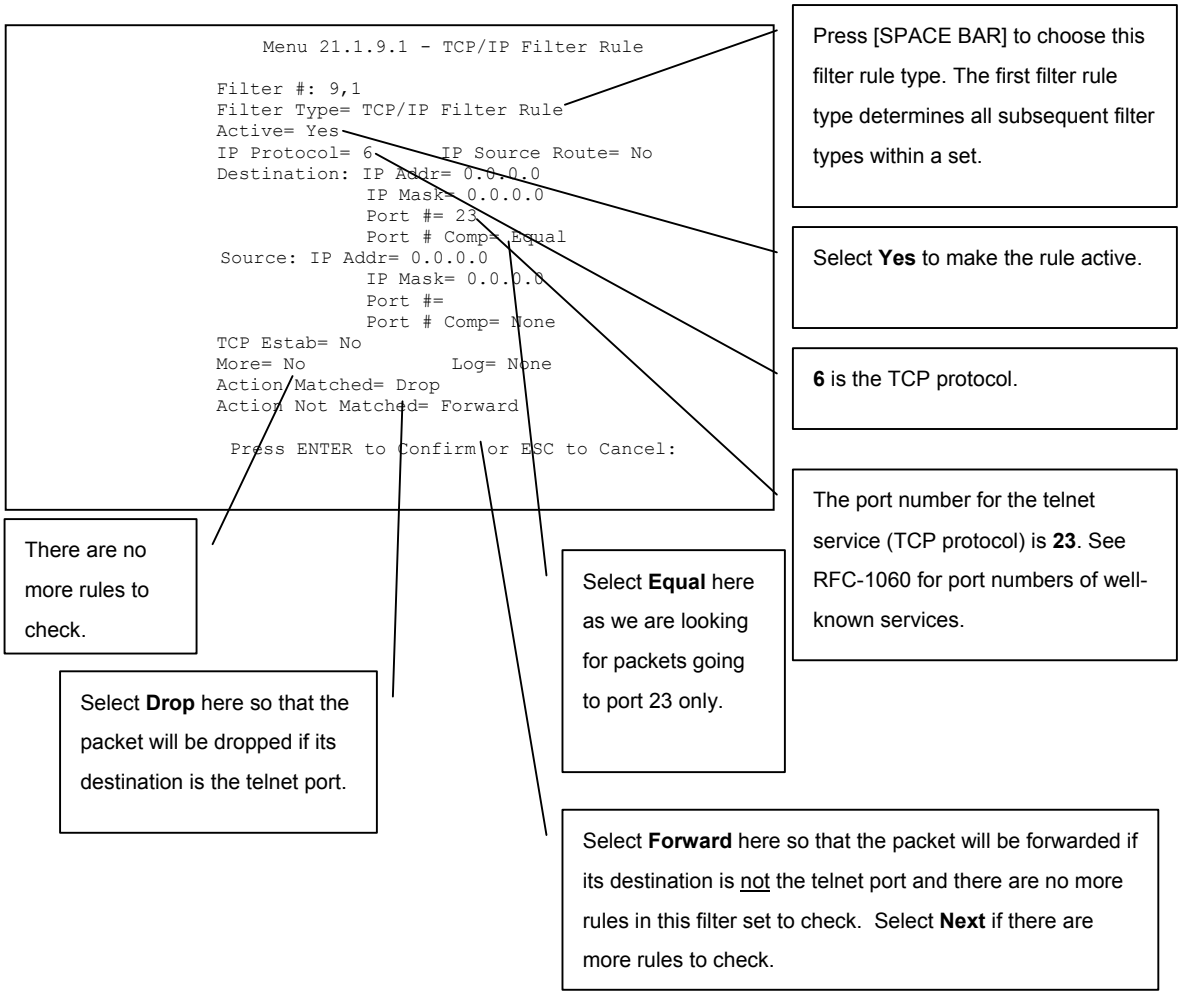


Figure 18-14 Sample Filter Menu 21.1.9.1

Step 7. Type 1 to configure the first filter rule. Make the entries in this menu as shown next.

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

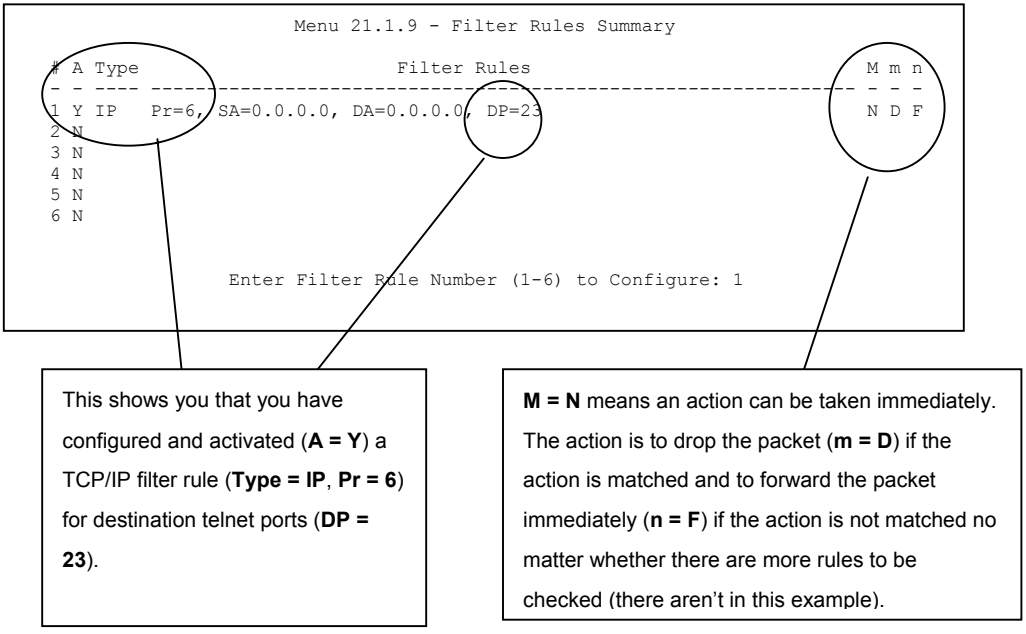


Figure 18-15 Sample Filter Rules Summary Menu 21.1.9

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

Step 8. Type 11 in the main menu to go to menu 11 and type the remote node number to edit.

Step 9. Go to the **Edit Filter Sets** field, press [SPACE BAR] to choose **Yes** and press [ENTER].

Step 10. This brings you to menu 11.5. Apply the example filter set (for example, filter set 3) in this menu as shown in the next section.

18.6 Applying Filters and Factory Defaults

Table 18-5 Filter Sets Table

FILTER SETS	DESCRIPTION
Input Filter Sets:	Apply filters for incoming traffic. You may apply protocol or device filter rules.
Output Filter Sets:	Apply filters for traffic leaving the Prestige. You may apply filter rules for protocol or device filters.
Call Filter Sets:	Apply filters to decide if a packet should be allowed to trigger a call.

18.6.1 Ethernet Traffic

You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and type 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 typing their numbers separated by commas, for example, 3, 4, 6, 11. The factory default filter set, NetBIOS_LAN, is inserted in the **protocol filters** field under **Input Filter Sets** in menu 3.1 in order to prevent local NetBIOS messages from triggering calls to the DNS server.

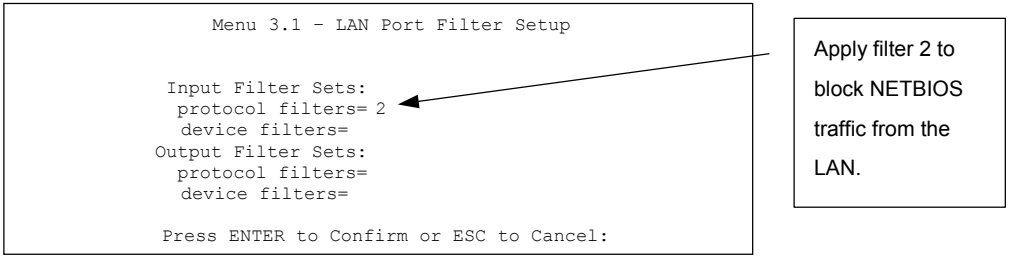


Figure 18-16 Filtering Ethernet Traffic

18.6.2 Remote Node Filters

Go to menu 11.5 (shown next) and type the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by typing their numbers separated by commas.

For PPPoE encapsulation, you have the option of specifying remote node call filter sets. Insert the factory default filter set, NetBIOS_WAN, in the **protocol filters** field under **Call Filter Sets** in menu 11.5 to block local NetBIOS traffic from triggering calls to the ISP.

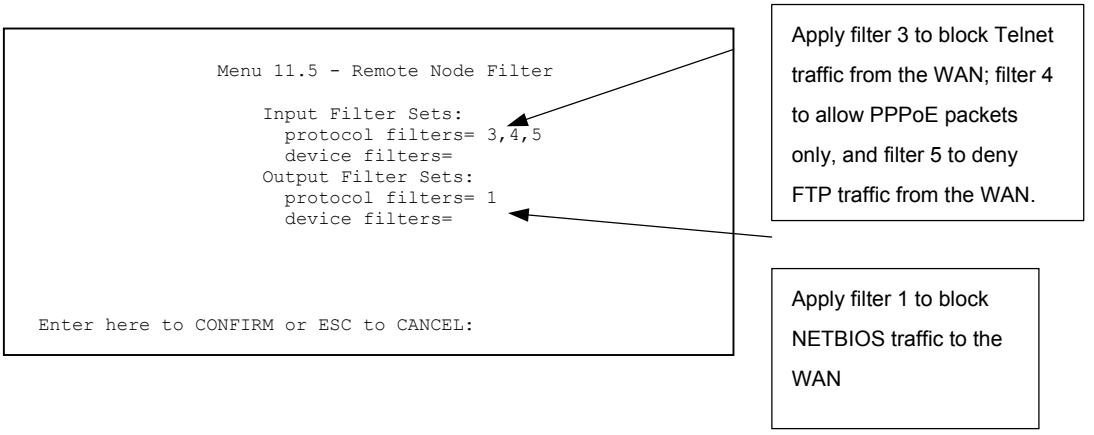


Figure 18-17 Filtering Remote Node Traffic

Chapter 19
SNMP Configuration

This chapter explains SNMP Configuration menu 22.

19.1 SNMP Overview

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your Prestige supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige through the network. The Prestige supports SNMP version one (SNMPv1) and version two c (SNMPv2c). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

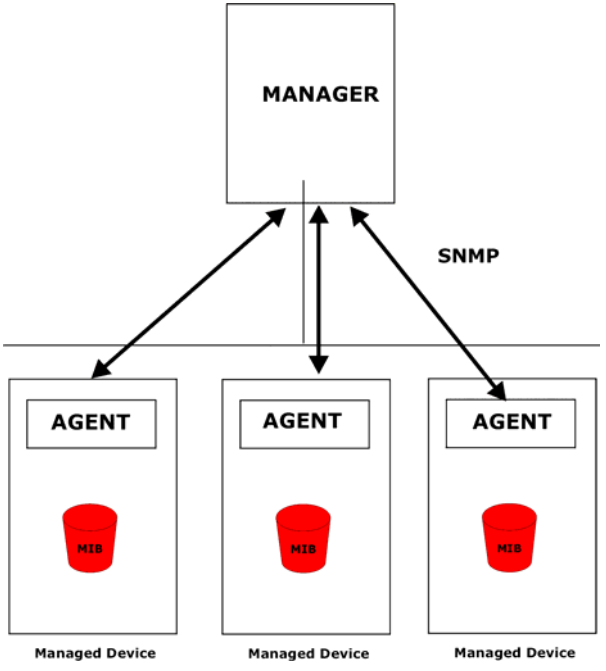


Figure 19-1 SNMP Management Model

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 (the Prestige). 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 number of packets received, node port status, etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a 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.

19.2 Supported MIBs

The Prestige supports RFC-1215 and MIB II as defined in RFC-1213. The focus of the MIBs is to let administrators collect statistic data and monitor status and performance.

19.3 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 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 19-2 Menu 22 SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 19-1 Menu 22 SNMP Configuration

FIELD	DESCRIPTION	EXAMPLE
SNMP: Get Community	Type the **Get Community**, which is the password for the incoming Get- and GetNext requests from the management station.	**public**
Set Community	Type 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 will only respond to SNMP messages from this address. A blank (default) field means your Prestige will respond to all SNMP messages it receives, regardless of source.	**0.0.0.0**
Trap: Community	Type the trap community, which is the password sent with each trap to the SNMP manager.	**public**
Destination	Type the IP address of the station to send your SNMP traps to.	**0.0.0.0**
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

19.4 SNMP Traps

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

Table 19-2 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
1	coldStart (*defined in RFC-1215*)	A trap is sent after booting (power on).
2	warmStart (*defined in RFC-1215*)	A trap is sent after booting (software reboot).
3	linkUp (*defined in RFC-1215*)	A trap is sent with the port number.
4	authenticationFailure (*defined in RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set requirements with wrong community (password).
6	linkDown (*defined in RFC-1215*)	A trap is sent with the port number when any of the links are down. See the following table.

The port number is its interface index under the interface group.

Table 19-3 Ports and Permanent Virtual Circuits

PORT	PVC (PERMANENT VIRTUAL CIRCUIT)
1	Ethernet LAN
2	1
3	2
…	…
13	12
14	DSL

Chapter 20
System Information and Diagnosis

This chapter covers the information and diagnostic tools in SMT menus 24.1 to 24.4.

20.1 System Status Overview

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

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

```
Menu 24 - System Maintenance

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

Enter Menu Selection Number:
```

Figure 20-1 Menu 24 System Maintenance

20.2 System Status

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

To get to System Status, type 24 to go to **Menu 24 – System Maintenance.** From this menu, type 1**. System Status**. There are two commands in **Menu 24.1 – System Maintenance – Status**. Typing 1 resets the counters, [ESC] takes you back to the previous screen.

The following table describes the fields present in **Menu 24.1 – System Maintenance – Status** which are READ-ONLY and meant for diagnostic purposes.

```
                  Menu 24.1 - System Maintenance - Status          01:36:21
                                                              Sat. Jan. 01, 2000
Chan    Link     Type        TxPkts      RxPkts     Errors  CLU  ALU     Up Time
--      Down     0Kbps            0           0          0   0%   0%     0:00:00
--      Down     0Kbps            0           0          0   0%   0%     0:00:00

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

Ethernet   Status                TxPkts         RxPkts          Collision
          100M/Full Duplex       2479           2363                  0

    Total Outcall Time:     0:00:00      CPU Load =    4.95%

    LAN Packet Which Triggered Last Call: (Type: IP)
    45 00 00 28 FE EB 00 00 FE 06 50 01 C0 A8 01 21 AC 16 00 03 04 61 02 0C
    99 90 38 9D 00 00 00 00 50 04 FA F0 6E 72 00 00

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

Figure 20-2 Menu 24.1 System Maintenance Status

Table 20-1 Menu 24.1 System Maintenance Status

FIELD	DESCRIPTION
Chan	This shows statistics for **B1** and **B2** channels respectively. This is the information displayed for each channel.
Link	This shows the name of the remote node or the user the channel is currently connected to or the status of the channel (e.g., **Down**, **Idle**, **Calling, Answering, NetCAPI,** etc.).
Type	This is the current connecting speed.
TxPkts	This is the number of transmitted packets on this channel.
RxPkts	This is the number of received packets on this channel.
Errors	This is the number of error packets on this channel.
CLU	The CLU (Current Line Utilization) is the percentage of current bandwidth used on this channel.
ALU	The ALU (Average Line Utilization) is a 5-second moving average of usage for this channel.
Up Time	Time this channel has been connected to the current remote node.
Chan	This shows statistics for **B1** and **B2** channels respectively. This is the information displayed for each channel.
Own IP Address	This refers to the IP address of the Prestige.

Table 20-1 Menu 24.1 System Maintenance Status

FIELD	DESCRIPTION
Own CLID	Shows your Caller ID.
Peer IP Address	This refers to the IP address of the peer.
Peer CLID	This shows the Caller ID of the peer.
Ethernet	This shows statistics for the LAN.
Status	This displays the port speed and duplex setting.
TxPkts	This is the number of transmitted packets to the LAN.
RxPkts	This is the number of received packets from the LAN.
Collision	This is the number of collisions.
Total Outcall Time	This shows the total outgoing call time for both **B1** and **B2** channels since the system has been powered up.
CPU Load	This specifies the percentage of CPU utilization.
LAN Packet Which Triggered Last Call	This shows the first 48 octets of the LAN packet that triggered the last outgoing call.
Commands	
Drop B1	This command drops the B1 channel.
Drop B2	This command drops the B2 channel.
Reset Counters	This command resets all counters.
Drop All	This command drops all channels.

20.3 System Information and Console Port Speed

This section describes your system and allows you to choose different console port speeds. To get to the System Information and Console Port Speed:

Step 1. Enter 24 to go to **Menu 24 – System Maintenance**.

Step 2. Enter 2 to open **Menu 24.2 – System Information and Console Port Speed**.

Step 3. From this menu you have two choices as shown in the next figure:

```
                Menu 24.2 - System Information and Console Port Speed
                      1. System Information
                      2. Console Port Speed

                            Please enter selection:
```

Figure 20-3 Menu 24.2 System Information and Console Port Speed

20.3.1 System Information

Enter 1 in menu 24.2 to display the screen shown next.

```
                    Menu 24.2.1 - System Maintenance - Information

                    Name: name
                    Routing: IP
                    ZyNOS F/W Version: V3.40(NV.0)b4 | 6/12/2003
                    Country Code: 255


                    LAN
                      Ethernet Address: 00:a0:c5:01:23:45
                      IP Address: 192.168.1.1
                      IP Mask: 255.255.255.0
                      DHCP: Server

                           Press ESC or RETURN to Exit:
```

Figure 20-4 Menu 24.2.1 System Maintenance Information

Table 20-2 Menu 24.2.1 System Maintenance Information

FIELD	DESCRIPTION
Name	Displays the system name of your Prestige. This information can be changed in **Menu 1 – General Setup**.
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
Country Code	This is the country code value (in decimal notation).
LAN	
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) of your Prestige.

Table 20-2 Menu 24.2.1 System Maintenance Information

FIELD	DESCRIPTION
IP Address	This is the IP address of the Prestige in dotted decimal notation.
IP Mask	This shows the subnet mask of the Prestige.
DHCP	This field shows the DHCP setting (None, Relay or Server) of the Prestige.

20.3.2 Console Port Speed

You can set up different port speeds for the console port through **Menu 24.2.2 – System Maintenance – Console Port Speed**. Your Prestige supports 9600 (default), 19200, 38400 and 57600bps. Use [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown in the following figure.

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

                          Console Port Speed: 9600

                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 20-5 Menu 24.2.2 System Maintenance Change Console Port Speed

20.4 Log and Trace

Type 3 in menu 24 to open **Menu 24.3-Log and Trace**. This menu allows you to view the error log and the Unix Syslog, configure an accounting server, and see call-triggering packet information.

20.4.1 Viewing Error Log

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

Step 1. Type 24 in the main menu to display **Menu 24** – **System Maintenance**.

Step 2. From menu 24, type 3 to display **Menu 24.3** – **System Maintenance** – **Log and Trace**.

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


                1. View Error Log
                2. UNIX Syslog
                3. Accounting Server
                4. Call-Triggering Packet
```

Figure 20-6 Menu 24.3 System Maintenance Log and Trace

Step 3. Enter 1 from **Menu 24.3** – **System Maintenance** – **Log and Trace** to display the error log in the system.

After the Prestige finishes displaying the error log, you will have the option to clear it. Samples of typical error and information messages are presented in the next figure.

```
  59 Thu Jan 01 00:00:03 1970 PP0f  INFO  LAN promiscuous mode <0>
  60 Thu Jan 01 00:00:03 1970 PP00 -WARN  SNMP TRAP 0: cold start
  61 Thu Jan 01 00:00:03 1970 PP00  INFO  main: init completed
  62 Thu Jan 01 00:00:19 1970 PP00  INFO  SMT Session Begin
  63 Thu Jan 01 00:00:24 1970 PP0a  WARN  MPOA Link Down
Clear Error Log (y/n):
```

Figure 20-7 Sample Error and Information Messages

20.4.2 Unix Syslog

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

```
Menu 24.3.2 - System Maintenance - UNIX Syslog

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

        Types:
        CDR= No
        Packet triggered= No
        Filter log= No
        PPP log= No
        POTS log=No
        Firewall log=No


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

Figure 20-8 Menu 24.3.2 System Maintenance Unix Syslog

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

Table 20-3 Menu 24.3.2 System Maintenance Unix Syslog

FIELD	DESCRIPTION
Syslog:	
Active	Press [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog IP Address	Enter the IP Address of the server that will log the CDR (Call Detail Record) and system messages i.e., the syslog server.
Log Facility	Press [SPACE BAR] and then [ENTER] to select a Local option. The log facility allows you to log the message to different files in the server. Please refer to your UNIX manual for more details.
Types: CDR	 Call Detail Record (CDR) logs all data phone line activity if set to **Yes**.
Packet Triggered	The first 48 bytes or octets and protocol type of the triggering packet is sent to the UNIX syslog server when this field is set to **Yes**.
Filter log	No filters are logged when this field is set to **No**. Filters with the individual filter Log Filter field set to **Yes** are logged when this field is set to **Yes**.
PPP log	PPP events are logged when this field is set to **Yes**.
POTS log	Voice calls are logged when this field is set to **Yes.**

Table 20-3 Menu 24.3.2 System Maintenance Unix Syslog

FIELD	DESCRIPTION
Firewall log	Firewall events are logged when this field is set to **Yes.**
When finished configuring this screen, press [ENTER] to confirm or [ESC] to cancel.	

The following are examples of syslog messages sent by the Prestige:

1. CDR

CDR Message Format

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

        L02 Call Terminated
        C02 Call Terminated
Jul 19 11:19:27 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2 ch=0 40002
Jul 19 11:19:32 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 OutCall Connected 64000 40002
Jul 19 11:20:06 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 Call Terminated
```

2. Packet triggered

Packet triggered Message Format

```
SdcmdSyslogSend( SYSLOG_PKTTRI, SYSLOG_NOTICE, String );
        String = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x
        Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)
        Data: We will send forty-eight Hex characters to the server
Jul 19 11:28:39 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f707172
7374
Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4
Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000
```

3. Filter log

Filter log Message Format

```
        SdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String );
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD

IP[…] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m) drop
(D).
        Src: Source Address
        Dst: Destination Address
        prot: Protocol ("TCP","UDP","ICMP")
spo: Source port
dpo: Destination port
Mar 03 10:39:43 202.132.155.97 ZyXEL:
GEN[ffffffffffnordff0080] }S05>R01mF
Mar 03 10:41:29 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 10:41:34 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP]}S04>R01mF
Mar 03 11:59:20 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 12:00:52 202.132.155.97 ZyXEL:
GEN[ffffffffffff0080] }S05>R01mF
Mar 03 12:00:57 202.132.155.97 ZyXEL:
GEN[00a0c5f502010080] }S05>R01mF
Mar 03 12:01:06 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170  dpo=00021]}S04>R01mF
```

4. PPP log

PPP Log Message Format

```
SdcmdSyslogSend( SYSLOG_PPPLOG, SYSLOG_NOTICE, String );
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP /
IPXCP
Jul 19 11:42:44 192.168.102.2 ZyXEL: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 ZyXEL: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 ZyXEL: ppp:CCP Closing
```

5. POTS log

POTS Log Message Format

SdcmdSyslogSend (SYSLOG_POTSLOG, SYSLOG_NOTICE, String);
String = Call Connect / Disconnect: Dir = xx Remote Call= xxxxx Local Call= xxxxx

Dir = Call Direction 1: Incoming call 2: Outgoing call
Remote Call = a string type which represents as the remote call number

20.5 Accounting Server

Type 3 in menu 24.3 to open **Menu 24.3.3-Accounting Server**. This menu allows you to activate and configure an accounting server.

```
            Menu 24.3.3 - System Maintenance - Accounting Server

                 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 20-9 Menu 24.3.3 System Maintenance Accounting Server

FIELD	DESCRIPTION	EXAMPLE
Accounting Server		
Active	Press the [SPACE BAR] to select Yes and press [ENTER] to enable wireless client authentication through an external accounting server.	**Yes**
Type	This non-editable field shows the type of accounting server being used.	**RADIUS**
Server Address	Enter the IP address of the external accounting server in dotted decimal notation.	**10.11.12.133**
Port #	The default port for the Radius server for accounting is 1646. You do not need to change this value unless your network administrator instructs you to do so.	**1646**
Key	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the Prestige.	
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

20.6 Call Triggering Packet

Type 3 in menu 24.3 to open **Menu 24.3.4-Call Triggering Packet**. This menu allows you to view the packets that triggered dial-out calls in a human-readable format. An example is shown next.

```
IP Frame: ENET0-RECV Size:  44/  44   Time: 17:02:44.262
 Frame Type:

   IP Header:
     IP Version               = 4
     Header Length            = 20
     Type of Service          = 0x00 (0)
     Total Length             = 0x002C (44)
     Identification            = 0x0002 (2)
     Flags                    = 0x00
     Fragment Offset          = 0x00
     Time to Live             = 0xFE (254)
     Protocol                 = 0x06 (TCP)
     Header Checksum          = 0xFB20 (64288)
     Source IP                = 0xC0A80101 (192.168.1.1)
     Destination IP           = 0x00000000 (0.0.0.0)

   TCP Header:
     Source Port              = 0x0401 (1025)
     Destination Port         = 0x000D (13)
     Sequence Number          = 0x05B8D000 (95997952)
     Ack Number               = 0x00000000 (0)
     Header Length            = 24
     Flags                    = 0x02 (....S.)
     Window Size              = 0x2000 (8192)
     Checksum                 = 0xE06A (57450)
     Urgent Ptr               = 0x0000 (0)
     Options                  =
         0000: 02 04 02 00

   RAW DATA:
     0000: 45 00 00 2C 00 02 00 00-FE 06 FB 20 C0 A8 01 01  E......... ....
     0010: 00 00 00 00 04 01 00 0D-05 B8 D0 00 00 00 00 00  ................
     0020: 60 02 20 00 E0 6A 00 00-02 04 02 00
Press any key to continue...
```

Figure 20-10 Menu 24.3.4 Call Triggering Packet.

20.7 Diagnostic

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

```
                Menu 24.4 - System Maintenance - Diagnostic

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

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

                      Enter Menu Selection Number:

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

Figure 20-11 Menu 24.4 System Maintenance Diagnostic

Follow the procedure next to get to Diagnostic:

Step 1. From the main menu, type 24 to open **Menu 24 – System Maintenance**.

Step 2. From this menu, type 4. Diagnostic to open **Menu 24.4 – System Maintenance – Diagnostic**.

Table 20-4 System Maintenance Menu Diagnostic

FIELD	DESCRIPTION
Hang Up B1 Call	This tool hangs up the B1 channel. It is only applicable if the B1 channel is currently in use.
Hang Up B2 Call	This tool hangs up the B2 channel. It is only applicable if the B2 channel is currently in use.
Reset ISDN	This command re-initializes the ISDN link to the telephone company.
ISDN Connection Test	You can test to see if your ISDN line is working properly by using this option. This command triggers the Prestige to perform a loop-back test to check the functionality of the ISDN line. If the test is not successful, note the error message that you receive and consult your network administrator.
Manual Call	This provides a way for you to place a call to a remote node manually. This tests the connectivity to that remote node. When you use this command, the screen displays what is happening during the call setup and protocol negotiation. The following is an example of a successful connection.

Table 20-4 System Maintenance Menu Diagnostic

FIELD	DESCRIPTION
Internet Setup Test	This test checks to see if your Internet access configuration has been done correctly. When this option is chosen, the Prestige places a manual call to the ISP remote node. If everything is working properly, you will receive an appropriate response. Otherwise, note the error message and consult your network administrator.
Ping Host	This diagnostic test pings the host, which determines the functionality of the TCP/IP protocol on both systems and the links in between.
Reboot System	This option reboots the Prestige.
Command Mode	This option allows you to enter the command mode. It allows you to diagnose and test your Prestige using a specified set of commands.
Manual Call Remote Node	If you entered **5** above, then enter the remote node number (with reference to the remote node listing on Menu 11 – Remote Node Setup) you wish to call.
Host IP Address	If you entered **12** above, then enter the IP address of the machine you want to ping in this field.

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

```
Start dialing for node <1>
### Hit any key to continue. ###
Dialing chan<2> phone<last 9-digit>:12345
Call CONNECT speed<64000> chan<2> prot<1>
LCP up
CHAP send response
CHAP login to remote OK!
IPCP negotiation started
IPCP up
```

Figure 20-12 Display for a Successful Manual Call

Chapter 21
Firmware and Configuration File Maintenance

This chapter tells you how to back up and restore your configuration file as well as upload new firmware and a new configuration file.

21.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a "rom" filename extension. Once you have customized the Prestige's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```
This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the Prestige.

```
ftp> get rom-0 config.cfg
```
This is a sample FTP session saving the current configuration to the computer file "config.cfg".

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the Prestige only recognizes "rom-0" and "ras". Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the Prestige and the external filename refers to the filename not on the Prestige, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **ZyNOS F/W Version** field in **Menu 24.2.1 - System Maintenance - Information** to confirm that you have uploaded the correct firmware version. The AT command is the command you enter after you press "y" when prompted in the SMT menu to go into debug mode.

Table 21-1 Filename Conventions

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

21.2 Backup Configuration

The Prestige displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24. 7.1 and 24.7.2; depending on whether you use the console port or Telnet.

Option 5 from **Menu 24 - System Maintenance** allows you to backup the current Prestige configuration to your computer. Backup is highly recommended once your Prestige is functioning properly. FTP is the preferred method for backing up your current configuration to your computer since it is faster. You can also perform backup and restore using menu 24 through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don't have to rename the files.

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

21.2.1 Backup Configuration

Follow the instructions as shown in the next screen.

```
                Menu 24.5 - System Maintenance - Backup Configuration

To transfer the configuration file to your computer, follow the procedure
below:

1. Launch the FTP client on your computer.
2. Type "open" and the IP address of your system. Then type "root" and
   SMT password as requested.
3. Locate the 'rom-0' file.
4. Type 'get rom-0' to back up the current router configuration to
   your computer.

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 this menu to back up using TFTP), please see your user manual.


                                Press ENTER to Exit:
```

Figure 21-1 Menu 24.5 System Maintenance – Backup Configuration

21.2.2 Using the FTP Command from the Command Line

Step 1. Launch the FTP client on your computer.

Step 2. Enter "open", followed by a space and the IP address of your Prestige.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is "1234").

Step 5. Enter "bin" to set transfer mode to binary.

Step 6. Use "get" to transfer files from the Prestige to the computer, for example, "get rom-0 config.rom" transfers the configuration file on the Prestige to your computer and renames it "config.rom". See earlier in this chapter for more information on filename conventions.

Step 7. Enter "quit" to exit the ftp prompt.

21.2.3 Example of FTP Commands from the Command Line

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 21-2 FTP Session Example

21.2.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 21-2 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
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).

21.2.5 Remote Management Limitations

TFTP, FTP and Telnet from the LAN or WAN will not work when:

1. A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. There is an SMT console session running.

3. There is already another remote management session of the same type (web, FTP or Telnet) running. You may only have one remote management session of the same type running at one time.
4. There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there is already a web session.

21.2.6 Backup Configuration Using TFTP

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

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

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

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

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

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

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

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "get" to transfer from the Prestige to the computer and "binary" to set binary transfer mode.

21.2.7 TFTP Command Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the Prestige IP address, "get" transfers the file source on the Prestige (rom-0, name of the configuration file on the Prestige) to the file destination on the computer and renames it config.rom.

21.2.8 GUI-based TFTP Clients

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

Table 21-3 General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the Prestige. 192.168.1.1 is the Prestige's default IP address when shipped.
Send/Fetch	Use "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.

Refer to *section 21.2.5* to read about configurations that disallow TFTP and FTP from the WAN.

21.2.9 Backup Via Console Port

Back up configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

Step 1. Display menu 24.5 and enter "y" at the following screen.

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

Figure 21-3 System Maintenance Backup Configuration

Step 2. The following screen indicates that the Xmodem download has started.

```
You can enter ctrl-x to terminate operation any time.
Starting XMODEM download...
```

Figure 21-4 System Maintenance: Starting Xmodem Download Screen

Step 3. Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

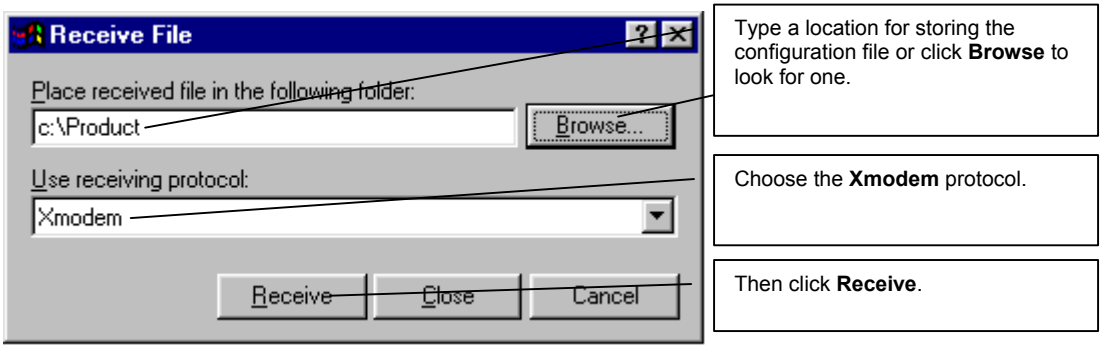


Figure 21-5 Backup Configuration Example

Step 4. After a successful backup you will see the following screen. Press any key to return to the SMT menu.

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

Figure 21-6 Successful Backup Confirmation Screen

21.3 Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring a previously saved configuration to your Prestige since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

WARNING!
DO NOT INTERRUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR PRESTIGE, WHEN THE UPLOAD CONFIGURATION/FIRMWARE PROCESS IS COMPLETE, THE PRESTIGE WILL AUTOMATICALLY RESET.

21.3.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

```
                Menu 24.6 -- System Maintenance - Restore Configuration

To transfer the firmware and configuration file to your workstation, follow the procedure
below:

1. Launch the FTP client on your computer.
2. Type "open" and the IP address of your router. Then type "root" and
   SMT password as requested.
3. Type "put backupfilename rom-0" where backupfilename is the name of
   your backup configuration file on your computer and rom-0 is the
   remote file name on the system. This restores the configuration to
   your system.
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 backup using TFTP (note that you must remain
in this menu to back up using TFTP), please see your user manual.


                                Press ENTER to Exit:
```

Figure 21-7 Telnet into Menu 24.6

Step 1. Launch the FTP client on your computer.

Step 2. Enter "open", followed by a space and the IP address of your Prestige.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is "1234").

Step 5. Enter "bin" to set transfer mode to binary.

Step 6. Find the "rom" file (on your computer) that you want to restore to your Prestige.

Step 7. Use "put" to transfer files from the Prestige to the computer, for example, "put config.rom rom-0" transfers the configuration file "config.rom" on your computer to the Prestige. See earlier in this chapter for more information on filename conventions.

Step 8. Enter "quit" to exit the ftp prompt. The Prestige will automatically restart after a successful restore process.

21.3.2 Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Figure 21-8 Restore Using FTP Session Example

Refer to *section 21.2.5* to read about configurations that disallow TFTP and FTP from the WAN.

21.3.3 Restore Via Console Port

Restore configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

Step 1. Display menu 24.6 and enter "y" at the following screen.

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

Figure 21-9 System Maintenance: Restore Configuration

Step 2. The following screen indicates that the Xmodem download has started.

```
Starting XMODEM download (CRC mode) ...
CCCCCCCCC
```

Figure 21-10 System Maintenance: Starting Xmodem Download Screen

Step 3. Run the HyperTerminal program by clicking **Transfer**, then **Send File** as shown in the following screen.

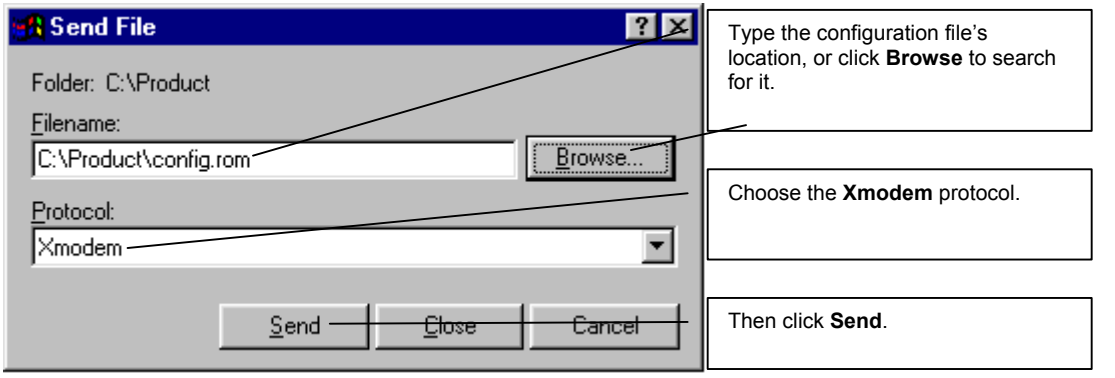


Figure 21-11 Restore Configuration Example

Step 4. After a successful restoration you will see the following screen. Press any key to restart the Prestige and return to the SMT menu.

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

Figure 21-12 Successful Restoration Confirmation Screen

21.4 Uploading Firmware and Configuration Files

This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in the previous *Restore Configuration* section or by following the instructions in **Menu 24.7.2 - System Maintenance - Upload System Configuration File** (for console port).

WARNING!
DO NOT INTERRUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR PRESTIGE, WHEN THE UPLOAD CONFIGURATION/FIRMWARE PROCESS IS COMPLETE, THE PRESTIGE WILL AUTOMATICALLY RESET.

21.4.1 Firmware File Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you telnet into the Prestige, type 7 in menu 24. You will see **Menu 24.7 – System Maintenance – Upload Firmware** as shown.

```
                Menu 24.7 - System Maintenance - Upload Firmware

                     1. Upload Router Firmware
                     2. Upload Router Configuration File


                          Enter Menu Selection Number:
```

Figure 21-13 - System Maintenance Upload Firmware

Enter 1 in menu 24.7 to display the following screen an upload firmware using FTP.

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

To upload the system firmware, follow the procedure below:

  1. Launch the FTP client on your computer.
  2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
  3. Type "put firmwarefilename ras" where "firmwarefilename" is the name
     of your firmware upgrade file on your computer and "ras" is the
     remote file name on the system.
  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 system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.


Press ENTER to Exit:
```

Figure 21-14 Menu 24.7.1 Upload System Firmware

21.4.2 Configuration File Upload

You can see the following screen when you enter 2 in menu 24.7.

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

To upload the system configuration file, follow the procedure below:


  1. Launch the FTP client on your computer.
  2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
  3. Type "put configurationfilename rom-0" where "configurationfilename"
     is the name of your system configuration file on your computer, which
     will be transferred to the "rom-0" file on the system.
  4. The system reboots automatically after the upload system configuration
     file process is complete.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.

Press ENTER to Exit:
```

Figure 21-15 Menu 24.7.2 - System Maintenance – Upload Configuration File

To upload the firmware and the configuration file, follow these examples

21.4.3 FTP File Upload Command from the DOS Prompt Example

Step 1. Launch the FTP client on your computer.

Step 2. Enter "open", followed by a space and the IP address of your Prestige.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is "1234").

Step 5. Enter "bin" to set transfer mode to binary.

Step 6. Use "put" to transfer files from the computer to the Prestige, for example, "put firmware.bin ras" transfers the firmware on your computer (firmware.bin) to the Prestige and renames it "ras". Similarly, "put config.rom rom-0" transfers the configuration file on your computer (config.rom) to the Prestige and renames it "rom-0". Likewise "get rom-0 config.rom" transfers the configuration file on the Prestige to your computer and renames it "config.rom." See earlier in this chapter for more information on filename conventions.

Step 7. Enter "quit" to exit the ftp prompt.

The Prestige automatically restarts after a successful file upload.

21.4.4 FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 21-16 FTP Session Example of Firmware File Upload

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to *section 21.2.5* to read about configurations that disallow TFTP and FTP over WAN.

21.4.5 TFTP File Upload

The Prestige also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

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

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

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

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

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

Step 5. Use the TFTP client (see the example below) to transfer files between the Prestige and the computer. The file name for the firmware is "ras".

Note that the telnet connection must be active and the Prestige in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "get" to transfer from the Prestige to the computer, "put" the other way around, and "binary" to set binary transfer mode.

21.4.6 TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

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

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

21.4.7 Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your Prestige. However, in the event of your network being down, uploading files is only possible with a direct connection to your Prestige via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

21.4.8 Uploading Firmware File Via Console Port

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

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


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

        Warning: Proceeding with the upload will erase the current system
        firmware.
                         Do You Wish To Proceed:(Y/N)
```

Figure 21-17 Menu 24.7.1 as Seen Using the Console Port

Step 2. After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

21.4.9 Example Xmodem Firmware Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

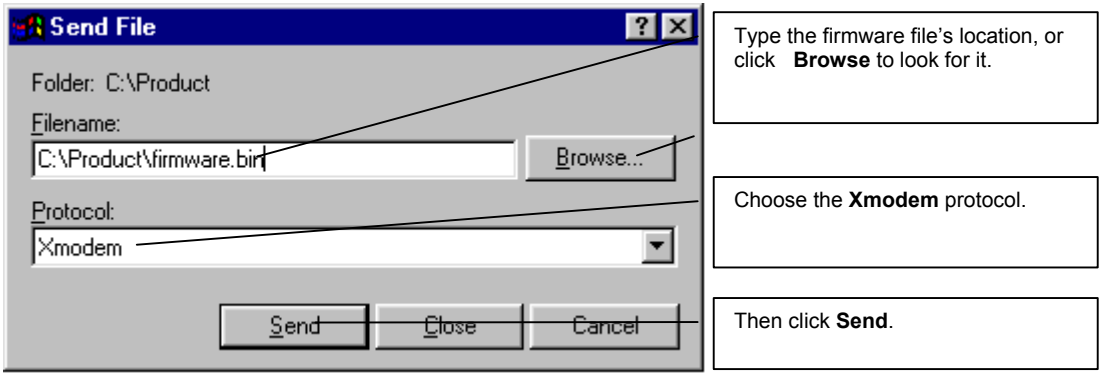


Figure 21-18 Example Xmodem Upload

After the configuration upload process has completed, restart the Prestige by entering "atgo".

21.4.10 Uploading Configuration File Via Console Port

Step 1. Select 2 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.2 - System Maintenance - Upload System Configuration File**. Follow the instructions as shown in the next screen.

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


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

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

Figure 21-19 Menu 24.7.2 as Seen Using the Console Port

Step 2. After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

Step 3. Enter "atgo" to restart the Prestige.

21.4.11 Example Xmodem Configuration Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

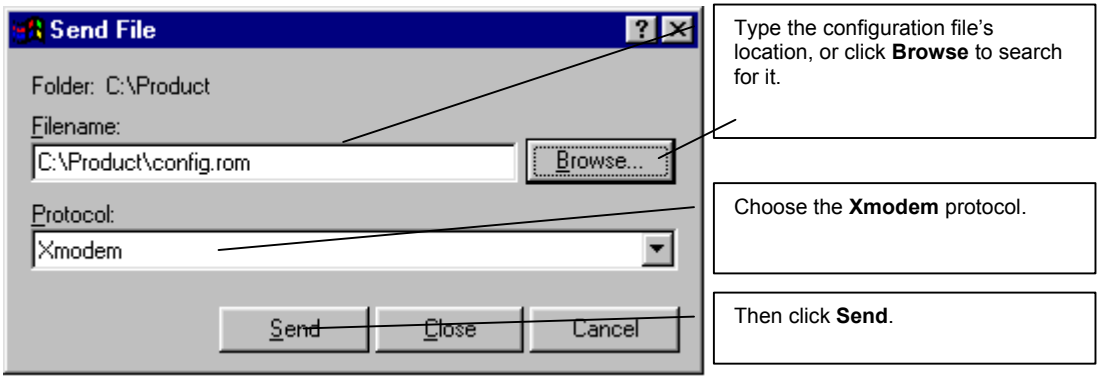


Figure 21-20 Example Xmodem Upload

After the configuration upload process has completed, restart the Prestige by entering "atgo".

Chapter 22
SMT Menus 24.8 to 24.10

This chapter leads you through System Maintenance SMT menus 24.8 to 24.10.

22.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. Access can be by Telnet or by a serial connection to the console port, although some commands are only available with a serial connection. See the included disk or the zyxel.com web site for more detailed information on CI commands. Enter 8 from **Menu 24 - System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type "exit" to return to the SMT main menu when finished.

```
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.  Firmware Update
8.  Command Interpreter Mode
9.  Call Control
10. Time and Date Setting



 Enter Menu Selection Number:
```

```
Copyright (c) 1994 - 2002 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            device          ether
config          isdn            radius          ip
ipsec           ppp             hdap
ras>
```

Figure 22-2 Valid Commands

22.2 Call Control Support

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

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

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

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

Call history chronicles preceding incoming and outgoing calls.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 - System Maintenance - Call Control**, as shown in the next table.

```
            Menu 24.9 - System Maintenance - Call Control

               1.  Call Control Parameters
               2.  Black List
               3.  Budget Management
               4.  Call History

                     Enter Menu Selection Number:
```

Figure 22-3 Menu 24.9 Call Control

22.2.1 Call Control Parameters

Menu 24.9.1 shows the call control parameters. Enter 1 from Menu 24.9 to bring up the following menu.

```
                Menu 24.9.1 - Call Control Parameters


                  Dialer Timeout:
                    Digital Call(sec)= 60

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


               Press ENTER to confirm or ESC to Cancel:
Please enter a number from 5 to 300
```

Figure 22-4 Menu 24.9.1Call Control Parameters

Table 22-1 Menu 24.9.1Call Control Parameters

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

22.2.2 Black List

Menu 24.9.2 shows the blacklist. The phone numbers on the blacklist are numbers that the Prestige had problems connecting to in the past. The only operation allowed is taking a number off the list by entering its index number. Enter 2 from Menu 24.9 to bring up the following menu.

```
                        Menu 24.9.2 - Blacklist

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

                        Remove Selection (1-14):
```

Figure 22-5 Menu 24.9.2 Blacklist

22.2.3 Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 3 from Menu 24.9 to bring up the following menu.

```
                    Menu 24.9.1 - Budget Management

  Remote Node        Connection Time/Total Budget     Elapsed Time/Total Period

1.ChangeMe                    No Budget                       No Budget
2.--------                       ---                             ---
3.--------                       ---                             ---
4.--------                       ---                             ---
5.--------                       ---                             ---
6.--------                       ---                             ---
7.--------                       ---                             ---
8.--------                       ---                             ---
9 Dial-in User                No Budget                       No Budget

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

Figure 22-6 Menu 24.9.1 Budget Management

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0.

hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node when PPPoE encapsulation is selected.

Table 22-2 Menu 24.9.1 Budget Management

FIELD	DESCRIPTION	EXAMPLE
Remote Node	Enter the index number of the remote node you want to reset (just one in this case).	1
Connection Time/Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1.	5/10 means that 5 minutes out of a total allocation of 10 minutes have lapsed.
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.	0.5/1 means that 30 minutes out of the 1 hour time period has lapsed.
Enter "0" to update the screen or press [ESC] to return to the previous screen.		

22.2.4 Call History

Menu 24.9.1 shows the call history for incoming and outgoing calls. Enter 4 from Menu 24.9 to bring up the following menu.

```
                        Menu 24.9.4 - Call History

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


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

Figure 22-7 Menu 24.9.4 Call History

Table 22-3 Menu 24.9.4 Call History

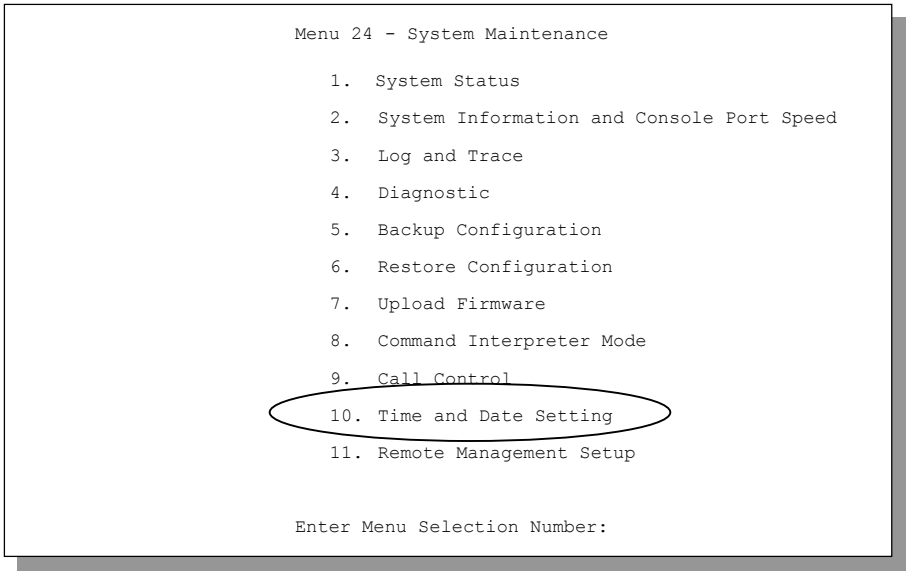
FIELD	DESCRIPTION
Phone Number	This is the telephone number of past incoming and outgoing calls.
Dir	This shows whether the call was incoming or outgoing.
Rate	This is the transfer rate of the call.
#call	This is the number of calls made to or received from that telephone number.
Max	This is the length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

22.3 Time and Date

There is a software mechanism to set the time manually or get the current time and date from an external server when you turn on your Prestige. Menu 24.10 allows you to update the time and date settings of your Prestige. The real time is then displayed in the Prestige error logs and firewall logs.

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

Figure 22-8 Menu 24: System Maintenance



Enter 10 to go to **Menu 24.10 - System Maintenance - Time and Date Setting** to update the time and date settings of your Prestige as shown in the following screen.

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


Use Time Server when Bootup= NTP (RFC-1305)
Time Server Address= tick.stdtime.gov.tw

Current Time:                           00 : 00 : 00
New Time (hh:mm:ss):                    11 : 23 : 16

Current Date:                           2000 - 01 - 01
New Date (yyyy-mm-dd):                  2001 - 03 - 01

Time Zone= GMT+0800



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

Figure 22-9 Menu 24.10 System Maintenance: Time and Date Setting

The following table describes the fields in this screen.

Table 22-4 Time and Date Setting Fields

FIELD	DESCRIPTION
Use Time Server when Bootup	Enter the time service protocol that your timeserver sends when you turn on the Prestige. Not all timeservers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** the default, is similar to **Time (RFC-868)**. **None** enter the time manually.

Table 22-4 Time and Date Setting Fields

FIELD	DESCRIPTION
Time Server Address	Enter the IP address or domain name of your timeserver. Check with your ISP/network administrator if you are unsure of this information. The default is tick.stdtime.gov.tw
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format.
Current Date	This field displays an updated date only when you reenter this menu.
New Date	Enter the new date in year, month and day format.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

22.3.1 Resetting the Time

The Prestige resets the time in three instances:

i. On leaving menu 24.10 after making changes.

ii. When the Prestige starts up, if there is a timeserver configured in menu 24.10.

iii. 24-hour intervals after starting.

Chapter 23
Call Scheduling

Call scheduling allows you to dictate when a remote node should be called and for how long.

23.1 Call Scheduling Overview

The call scheduling feature allows the Prestige to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a videocassette recorder (you can specify a time period for the VCR to record).

23.2 Configuring Call Scheduling

From the main menu, enter 26 to access **Menu 26 - Schedule Setup** as shown next. You can apply up to 4 schedule sets in **Menu 11.1 - Remote Node Profile**.

```
                        Menu 26 - Schedule Setup

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

                      Enter Schedule Set Number to Configure=0

                      Edit Name=N/A

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

Figure 23-1 Menu 26 Schedule Setup

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

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

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

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

```
                    Menu 26.1 - Schedule Set Setup

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

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

Figure 23-2 Menu 26.1 Schedule Set Setup

Table 23-1 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION	OPTIONS
Active	Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the schedule set.	**Yes** **No**
Start Date	Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-February-5.	
How Often	Should this schedule set recur weekly or be used just once only? Press [SPACE BAR] and then [ENTER] to select **Once** or **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A**. When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses.	**Once** **Weekly**
Once: Date	If you selected **Once** in the **How Often** field above, then enter the date the set should activate here in year-month-date format.	

Table 23-1 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION	OPTIONS
Weekday: Day	If you selected **Weekly** in the **How Often** field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select **Yes**, then press [ENTER].	**Yes** **No** **N/A**
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.	
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.	
Action	**Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the **Duration** field. **Forced Down** means that the connection is blocked whether or not there is a demand call on the line. **Enable Dial-On-Demand** means that this schedule permits a demand call on the line. **Disable Dial-On-Demand** means that this schedule prevents a demand call on the line.	**Forced On** **Forced Down** **Enable Dial-On-Demand** **Disable Dial-On-Demand**
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

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

23.3 Applying Schedule Sets

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the Main Menu and then enter the target remote node index. You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

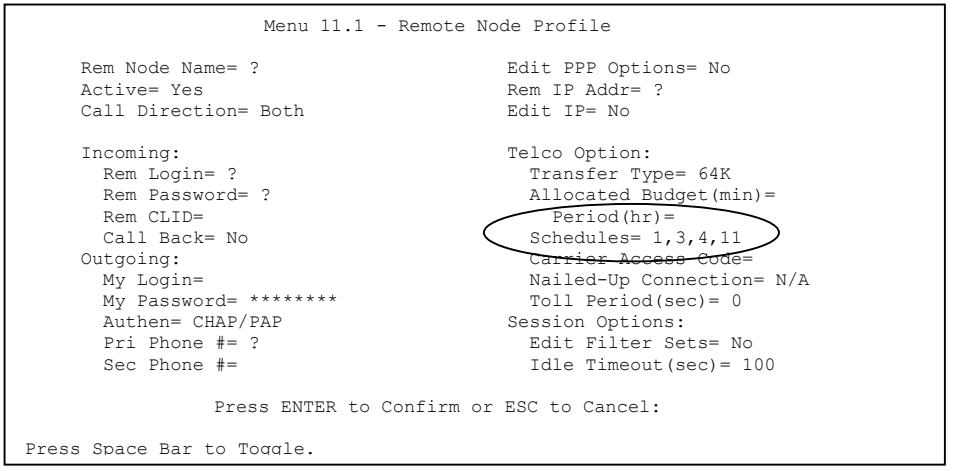


Figure 23-3 Applying Schedule Set(s)

Chapter 24
Remote Management

This chapter provides information on configuring remote management (SMT menu 24.11).

24.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which Prestige interface (if any) from which computers.

You may manage your Prestige from a remote location via:

- Internet (WAN only)
- LAN only
- ALL (LAN and WAN)
- Neither (Disable)

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

24.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

5. A filter in SMT menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
6. You have disabled that service in one of the remote management screens.
7. The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.
8. There is an SMT console session running.
9. There is already another remote management session of the same type (web, FTP or Telnet) running. You may only have one remote management session of the same type running at one time.
10. There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there already is a web session.

24.1.2 Remote Management and NAT

When NAT is enabled:

- Use the Prestige's WAN IP address when configuring from the WAN.

- Use the Prestige's LAN IP address when configuring from the LAN.

24.1.3 System Timeout

There is a system timeout of five minutes (three hundred seconds) for either the console port or telnet/web/FTP connections. Your Prestige automatically logs you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.

24.2 Telnet

You can configure your Prestige for remote Telnet access as shown next.

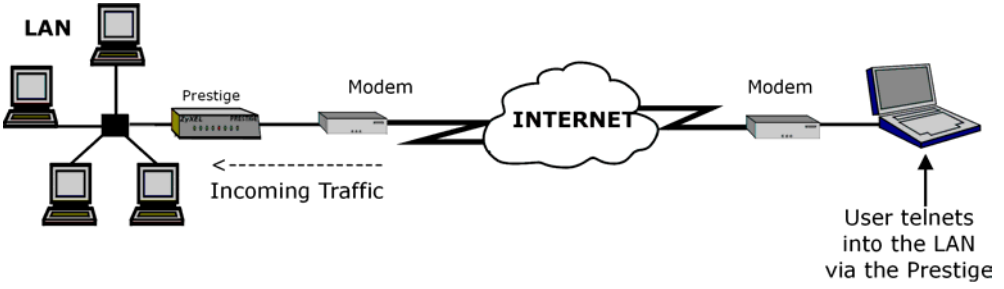


Figure 24-1 Telnet Configuration on a TCP/IP Network

24.3 FTP

You can upload and download Prestige firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

24.4 Web

You can use the Prestige's embedded web configurator for configuration and file management. See the online help for details.

24.5 Configuring Remote Management

Enter 11 from menu 24 to display **Menu 24.11 — Remote Management Control**.

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

```
                    Menu 24.11 - Remote Management Control


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

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

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


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

Figure 24-2 Remote Management

The following table describes the labels in this screen.

Table 24-1 Remote Management

FIELD	DESCRIPTION
Telnet Server FTP Server Web Server	Each of these read-only labels denotes a service that you may use to remotely manage the Prestige.
Port	This field shows the port number for the remote management service. You may change the port number for a service if needed, but you must use the same port number to use that service for remote management.
Access	Select the access interface (if any) by pressing the [SPACE BAR]. Choices are: **LAN only**, **WAN only**, **All** or **Disable**. The default is **LAN only**.
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the Prestige. Enter an IP address to restrict access to a client with a matching IP address.
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

Chapter 25
Introduction to VPN/IPSec

This chapter introduces the basics of IPSec VPNs.

25.1 VPN Overview

A VPN (Virtual Private Network) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

25.1.1 IPSec

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

25.1.2 Security Association

A Security Association (SA) is a contract between two parties indicating what security parameters, such as keys and algorithms they will use.

25.1.3 Other Terminology

- **Encryption**

  Encryption is a mathematical operation that transforms data from "plaintext" (readable) to "ciphertext" (scrambled text) using a "key". The key and clear text are processed by the encryption operation, which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is a mathematical operation that transforms "ciphertext" to plaintext. Decryption also requires a key.

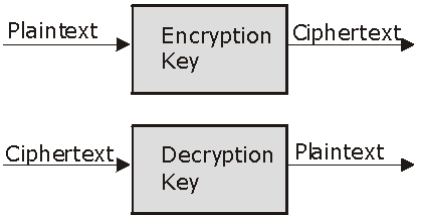


Figure 25-1 Encryption and Decryption

- **Data Confidentiality**

  The IPSec sender can encrypt packets before transmitting them across a network.

- **Data Integrity**

  The IPSec receiver can validate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.

- **Data Origin Authentication**

  The IPSec receiver can verify the source of IPSec packets. This service depends on the data integrity service.

25.1.4 VPN Applications

The Prestige supports the following VPN applications.

- **Linking Two or More Private Networks Together**

  Connect branch offices and business partners over the Internet with significant cost savings and improved performance when compared to leased lines between sites.

- **Accessing Network Resources When NAT Is Enabled**

  When NAT is enabled, remote users are not able to access hosts on the LAN unless the host is designated a public LAN server for that specific protocol. Since the VPN tunnel terminates inside the LAN, remote users will be able to access all computers that use private IP addresses on the LAN.

- **Unsupported IP Applications**

  A VPN tunnel may be created to add support for unsupported emerging IP applications.

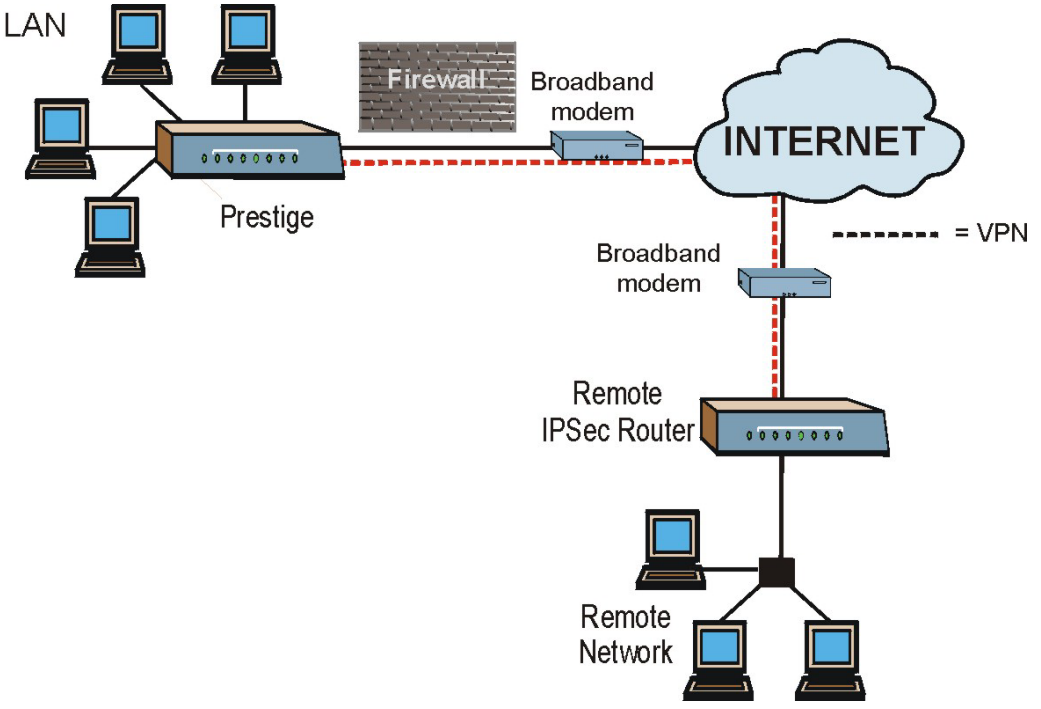


Figure 25-2 VPN Application

25.2 IPSec Architecture

The overall IPSec architecture is shown as follows.

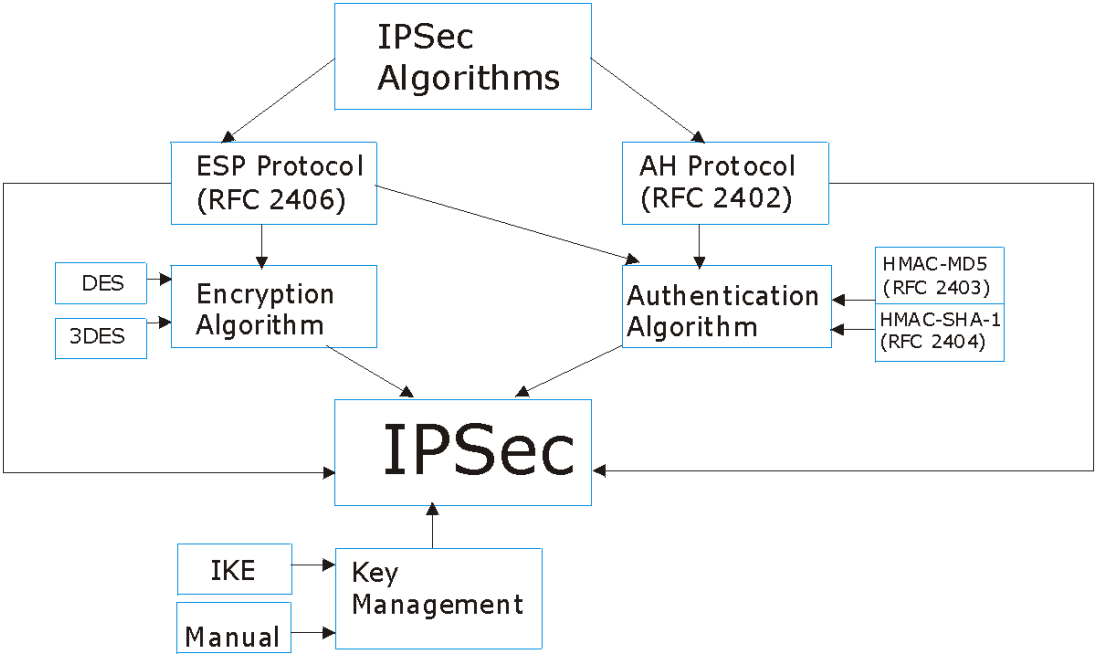


Figure 25-3 IPSec Architecture

25.2.1 IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols. Please see *section 26.2* for more information.

25.2.2 Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

25.3 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode.

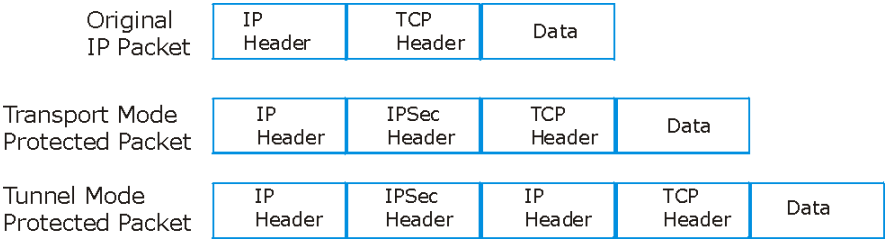


Figure 25-4 Transport and Tunnel Mode IPSec Encapsulation

25.3.1 Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

25.3.2 Tunnel Mode

Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

25.4 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the Prestige.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. **Transport** mode **ESP** with authentication is not compatible with NAT.

Table 25-1 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

Chapter 26
VPN/IPSec Setup

This chapter shows you how to set up VNP/IPSec on your Prestige.

26.1 VPN/IPSec Overview

Use the screens documented in this chapter to configure rules for VPN connections and manage VPN connections.

26.1.1 VPN/IPSec SMT Menus

The VPN/IPSec main SMT menu has three main submenus.

1. Define VPN policies in menu 27.1 submenus, including security policies, endpoint IP addresses, peer IPSec router IP address and key management.
2. Manage (refresh or disconnect) your SA connections in menu 27.2.
3. View the IPSec connection log in menu 27.4. This menu is also useful for troubleshooting.

This is an overview of the VPN menu tree.

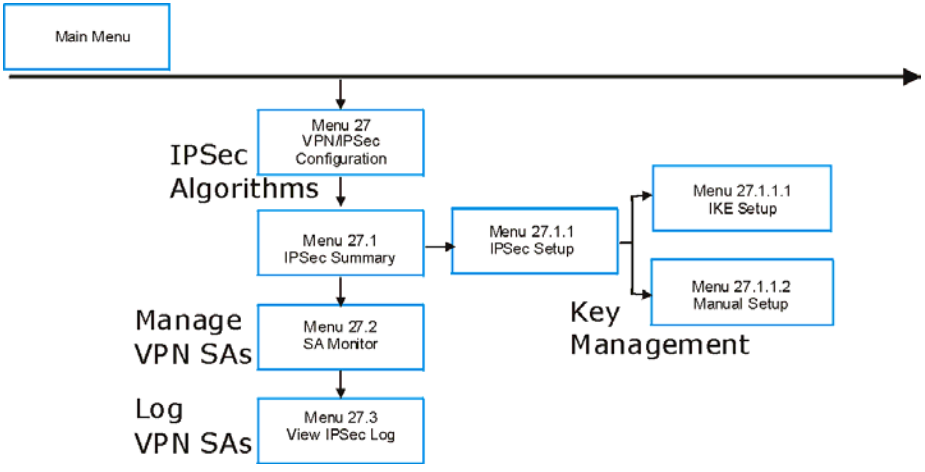


Figure 26-1 VPN SMT Menu Tree

From the main menu, enter 27 to display the first VPN/IPSec menu (shown next).

```
                    Menu 27 - VPN/IPSec Setup

              1. IPSec Summary
              2. SA Monitor
              3. View IPSec Log




                   Enter Menu Selection Number:
```

Figure 26-2 Menu 27 VPN/IPSec Setup

26.2 IPSec Algorithms

The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. An SA is built from the authentication provided by the **AH** and **ESP** protocols. The primary function of key management is to establish and maintain the SA between systems. Once the SA is established, the transport of data may commence.

26.2.1 AH (Authentication Header) Protocol

AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed.

In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an **AH** can be employed to ensure integrity. This type of implementation does not protect the information from dissemination but will allow for verification of the integrity of the information and authentication of the originator.

26.2.2 ESP (Encapsulating Security Payload) Protocol

The **ESP** protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process. However, **ESP** is sufficient if only the upper layer protocols need to be authenticated.

An added feature of the **ESP** is payload padding, which further protects communications by concealing the size of the packet being transmitted.

Table 26-1 AH and ESP

ESP	AH
Select **DES** for minimal security and **3DES** for maximum. Select **NULL** to set up a tunnel without encryption.	Select **MD5** for minimal security and **SHA-1** for maximum security.
DES (default) Data Encryption Standard (DES) is a widely used method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
3DES Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys (3 x 56 = 168 bits), effectively doubling the strength of DES.	**SHA1** SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.

26.3 My IP Address

My IP Addr is the WAN IP address of the Prestige. If this field is configured as 0.0.0.0, then the Prestige will use the current Prestige WAN IP address (static or dynamic) to set up the VPN tunnel. If the **My IP Addr** changes after setup, then the VPN tunnel will have to be rebuilt.

26.4 Secure Gateway Address

Secure Gateway Addr is the WAN IP address or domain name of the remote IPSec router (secure gateway). If the remote secure gateway has a static public IP address, enter it in the **Secure Gateway Addr** field. You may alternatively enter the remote secure gateway's domain name in the **Secure Gateway Addr** field. This also works when the remote secure gateway uses DDNS. This way your Prestige can find the remote secure gateway, even if it has a dynamic WAN IP address.

If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 in the **Secure Gateway Addr** field. In this case only the remote secure gateway can initiate SAs. This may be useful for telecommuters initiating a VPN tunnel to the company network. See the following table for an example configuration. You can configure multiple SAs to simultaneously connect through the same secure gateway. In this case, you must configure the SAs to have the same **Negotiation Mode** and **Pre-Shared Key** (**Menu 27.1.1.1 IKE Setup**).

The Secure Gateway IP Address may be configured as 0.0.0.0 only when using IKE **key management and not** Manual **key management.**

A Prestige with **Secure Gateway Address** set to 0.0.0.0 can receive multiple VPN connection requests using the same VPN rule at the same time.

26.4.1 Dynamic Secure Gateway Address

If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the secure gateway's address. In this case only the remote secure gateway can initiate SAs. This may be useful for telecommuters initiating a VPN tunnel to the company network. See *section 26.13* for configuration examples.

The Secure Gateway IP Address may be configured as 0.0.0.0 only when using IKE **key management and not** Manual **key management.**

26.5 IPSec Summary

Type 1 in menu 27 and then press [ENTER] to display **Menu 27.1 — IPSec Summary**. This is a summary read-only menu of your IPSec rules (tunnels). Edit or create an IPSec rule by selecting an index number and then configuring the associated submenus.

The following figure helps explain the main fields in menu 27.1.

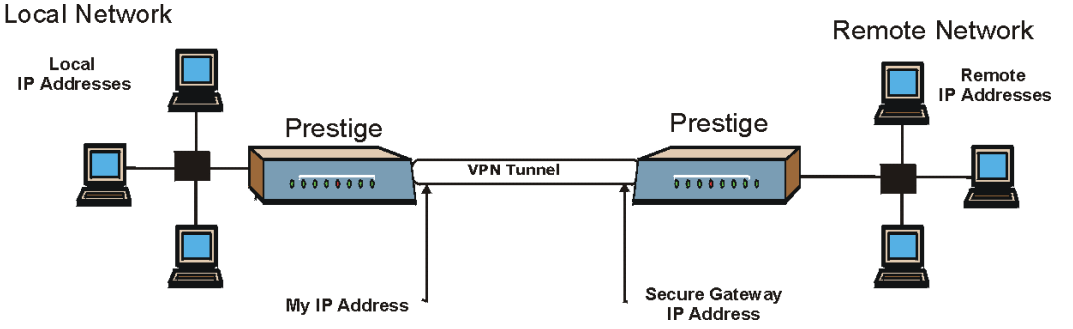


Figure 26-3 IPSec Summary Fields Illustration

Local and remote IP addresses must be static. The VPN initiator local IP address range should be identical to the peer remote IP address range. Similarly, the VPN initiator remote IP address range should be identical to the peer local IP address range. If they are not, the connection will fail and this will display in the IPSec log as a local or remote ID failure.

```
                                Menu 27.1 - IPSec Summary

#         Name      A  Local Addr Start       - Local Addr End       Encap     IPSec Algorithm
        Key Mgt        Remote Addr Start       - Remote Addr End               Secure Gw Addr
-       ------     -   -----------------       ---------------       ------    ------------------
001       Taiwan   Y   192.168.1.35            192.168.1.38          Tunnel    ESP DES MD5
             IKE       172.16.2.40             172.16.2.46                     193.81.13.2
002         zw50   N   1.1.1.1                 1.1.1.1               Tunnel    AH SHA1
             IKE       4.4.4.4                 255.255.0.0                     zw50test.zyxel.
003        China   N   192.168.1.40            192.168.1.42          Tunnel    ESP DES MD5
             IKE       N/A                     N/A                             0.0.0.0
004

005


              Select Command= None                                Select Rule= N/A
                          Press ENTER to Confirm or ESC to Cancel:
```

Figure 26-4 Menu 27.1 IPSec Summary

Table 26-2 Menu 27.1 IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
#	This is the VPN policy index number.	001
Name	This field displays the unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed here.	Taiwan
A	**Y** signifies that this VPN rule is active. **N** means inactive.	**Y**
Local Addr Start	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is a (static) IP address on the LAN behind your Prestige. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the beginning (static) IP address, in a range of computers on the LAN behind your Prestige. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a (static) IP address on the LAN behind your Prestige.	192.168.1.35

Table 26-2 Menu 27.1 IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
Local Addr End	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is the same (static) IP address as in the **Local Addr Start** field. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the end (static) IP address, in a range of computers on the LAN behind your Prestige. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a subnet mask on the LAN behind your Prestige.	192.168.1.38
Encap	This field displays **Tunnel** mode or **Transport** mode. You need to finish configuring the VPN policy in menu 27.1.1.1 or 27.1.1.2 if **???** is displayed.	**Tunnel**
IPSec Algorithm	This field displays the security protocols used for an SA. **ESP** provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit **DES** and 168-bit **3DES**. **NULL** denotes a tunnel without encryption. **AH** (Authentication Header) provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. **AH** choices are **MD5** (default - 128 bits) and **SHA -1**(160 bits)**.** Both **AH** and **ESP** increase the Prestige's processing requirements and communications latency (delay). You need to finish configuring the VPN policy in menu 27.1.1.1 or 27.1.1.2 if **???** is displayed.	**ESP DES MD5**
Key Mgt	This field displays the SA's type of key management, (**IKE** or **Manual**).	**IKE**

Table 26-2 Menu 27.1 IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
Remote Addr Start	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is a (static) IP address on the network behind the remote IPSec router. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a (static) IP address on the network behind the remote IPSec router. This field displays **N/A** when you configure the **Secure Gateway Addr** field in SMT 27.1.1 to 0.0.0.0.	172.16.2.40
Remote Addr End	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is the same (static) IP address as in the **Remote Addr Start** field. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a subnet mask on the network behind the remote IPSec router. This field displays **N/A** when you configure the **Secure Gateway Addr** field in SMT 27.1.1 to 0.0.0.0.	172.16.2.46
Secure GW Addr	This is the WAN IP address or the domain name (up to the first 15 characters are displayed) of the IPSec router with which you are making the VPN connection. This field displays **0.0.0.0** when you configure the **Secure Gateway Addr** field in SMT 27.1.1 to 0.0.0.0.	193.81.13.2
Select Command	Press [SPACE BAR] to choose from **None**, **Edit** or **Delete** and then press [ENTER]. You must select a rule in the next field when you choose the **Edit**, Delete or **Go To** commands. Select **None** and then press [ENTER] to go to the "Press ENTER to Confirm…" prompt. Use **Edit** to create or edit a rule. Use **Delete** to remove a rule. To edit or delete a rule, first make sure you are on the correct page. When a VPN rule is deleted, subsequent rules do not move up in the page list.	**None**

Table 26-2 Menu 27.1 IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
Select Rule	Type the VPN rule index number you wish to edit or delete and then press [ENTER].	3
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.		

26.6 Keep Alive

When you initiate an IPSec tunnel with keep alive enabled, the Prestige automatically renegotiates the tunnel when the IPSec SA lifetime period expires. In effect, the IPSec tunnel becomes an "always on" connection after you initiate it. Both IPSec routers must have a Prestige -compatible keep alive feature enabled in order for this feature to work. The Prestige has a maximum of 2 IPSec tunnels.

When there is outbound traffic with no inbound traffic, the Prestige automatically drops the tunnel after two minutes.

26.7 ID Type and Content

With aggressive negotiation mode (see *section 26.10.1*), the Prestige identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the Prestige to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the Prestige from IPSec routers with dynamic IP addresses (see *section 26.13.2* for a telecommuter configuration example).

With main mode (see *section 26.10.1*), the ID type and content are encrypted to provide identity protection. In this case the Prestige can only distinguish between up to eight different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The Prestige can distinguish up to eight incoming SAs because you can select between two encryption algorithms (DES and 3DES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule. The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 26-3 Local ID Type and Content Fields

LOCAL ID TYPE=	CONTENT=
IP	Type the IP address of your computer or leave the field blank to have the Prestige automatically use its own IP address.
DNS	Type a domain name (up to 31 characters) by which to identify this Prestige.
E-mail	Type an e-mail address (up to 31 characters) by which to identify this Prestige.
The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.	

Table 26-4 Peer ID Type and Content Fields

PEER ID TYPE=	CONTENT=
IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the Prestige automatically use the address in the **Secure Gateway** field.
DNS	Type a domain name (up to 31 characters) by which to identify the remote IPSec router.
E-mail	Type an e-mail address (up to 31 characters) by which to identify the remote IPSec router.
The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the **Secure Gateway Addr** field below.	

26.7.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two Prestiges in this example can complete negotiation and establish a VPN tunnel.

Table 26-5 Matching ID Type and Content Configuration Example

PRESTIGE A	PRESTIGE B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2

Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

The two Prestiges in this example cannot complete their negotiation because Prestige B's **Local ID type** is **IP**, but Prestige A's **Peer ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

Table 26-6 Mismatching ID Type and Content Configuration Example

PRESTIGE A	PRESTIGE B
Local ID type: IP	**Local ID type: IP**
Local ID content: 1.1.1.10	Local ID content: 1.1.1.10
Peer ID type: E-mail	Peer ID type: IP
Peer ID content: aa@yahoo.com	Peer ID content: N/A

26.8 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see *section 26.10* for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

26.9 IPSec Setup

Select **Edit** in the **Select Command** field, type the index number of a rule in the **Select Rule** field and press [ENTER] to edit the VPN using the menu shown next.

You must also configure menu 27.1.1.1 or menu 27.1.1.2 to fully configure and use a VPN.

```
                    Menu 27.1.1 - IPSec Setup

Index #= 1          Name= ?
Active= No          Keep Alive= No
Local ID type= IP          Content=
My IP Addr= 0.0.0.0
Peer ID type= IP           Content=
Secure Gateway Addr= 0.0.0.0
Protocol= 0
Local:  Addr Type= SINGLE
    IP Addr Start= 0.0.0.0          End/Subnet Mask= N/A
       Port Start= 0                End= N/A
Remote: Addr Type= N/A
    IP Addr Start= N/A              End/Subnet Mask= N/A
       Port Start= N/A              End= N/A
Enable Replay Detection= N/A
Key Management= N/A
Edit Key Management Setup= N/A

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

Figure 26-5 Menu 27.1.1 IPSec Setup

Table 26-7 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
Index	This is the VPN rule index number you selected in the previous menu.	**1**
Name	Enter a unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed in **Menu 27.1 - IPSec Summary**.	Taiwan
Active	Press [SPACE BAR] to choose either **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the VPN tunnel. This field determines whether a VPN rule is applied before a packet leaves the firewall.	**Yes**
Keep Alive	Press [SPACE BAR] to choose either **Yes** or **No**. Select **Yes** to have the Prestige automatically re-initiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work.	**No**
Local ID Type	Press [SPACE BAR] to choose **IP**, **DNS** or **E-MAIL**. Select **IP** to identify this Prestige by its IP address. Select **DNS** to identify this Prestige by a domain name. Select **E-mail** to identify this Prestige by an e-mail address.	**IP**

Table 26-7 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer or leave the field blank to have the Prestige automatically use its own IP address. When you select **DNS** in the **Local ID Type** field, type a domain name (up to 31 characters) by which to identify this Prestige. When you select **E-mail** in the **Local ID Type** field, type an e-mail address (up to 31 characters) by which to identify this Prestige. The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.	
My IP Addr	Enter the WAN IP address of your Prestige. The Prestige uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as 0.0.0.0. The VPN tunnel has to be rebuilt if this IP address changes.	0.0.0.0
Peer ID Type	Select **IP** to identify the remote IPSec router by its IP address. Select **DNS** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address.	**IP**
Content	When you select **IP** in the **Peer ID Type** field, type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the Prestige automatically use the address in the **Secure Gateway field**. When you select **DNS** in the **Peer ID Type** field, type a domain name (up to 31 characters) by which to identify the remote IPSec router. When you select **E-mail** in the **Peer ID Type** field, type an e-mail address (up to 31 characters) by which to identify the remote IPSec router. The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the **Secure Gateway Addr** field below.	

Table 26-7 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
Secure Gateway Addr	Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address (the **Key Management** field must be set to **IKE**, see later). See the *Secure Gateway Address* section for more details.	Zw50test.com.tw
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.	0
Local	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.	
Addr Type	Press [SPACE BAR] to choose **SINGLE**, **RANGE**, or **SUBNET** and press [ENTER]. Select **SINGLE** with a single IP address. Select **RANGE** for a specific range of IP addresses. Select **SUBNET** to specify IP addresses on a network by their subnet mask.	**SINGLE**
IP Addr Start	When the **Addr Type** field is configured to **Single**, enter a (static) IP address on the LAN behind your Prestige. When the **Addr Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on your LAN behind your Prestige. When the **Addr Type** is configured to **SUBNET**, this is a (static) IP address on the LAN behind your Prestige.	192.168.1.35
End/Subnet Mask	When the **Addr Type** field is configured to **Single**, this field is **N/A**. When the **Addr Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the LAN behind your Prestige. When the **Addr Type** field is configured to **SUBNET**, this is a subnet mask on the LAN behind your Prestige.	192.168.1.38
Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3	0

Table 26-7 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is **N/A** when 0 is configured in the **Port Start** field.	N/A
Remote	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields are **N/A** when the **Secure Gateway Addr** field is configured to 0.0.0.0. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.	
Addr Type	Press [SPACE BAR] to choose **SINGLE**, **RANGE**, or **SUBNET** and press [ENTER]. Select **SINGLE** with a single IP address. Use **RANGE** for a specific range of IP addresses. Use **SUBNET** to specify IP addresses on a network by their subnet mask.	**SUBNET**
IP Addr Start	When the **Addr Type** field is configured to **Single**, enter a (static) IP address on the network behind the remote IPSec router. When the **Addr Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Addr Type** field is configured to **SUBNET**, enter a (static) IP address on the network behind the remote IPSec router. This field displays **N/A** when you configure the **Secure Gateway Addr** field to 0.0.0.0.	4.4.4.4
End/Subnet Mask	When the **Addr Type** field is configured to **Single**, this field is **N/A**. When the **Addr Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Addr Type** field is configured to **SUBNET**, enter a subnet mask on the network behind the remote IPSec router. This field displays **N/A** when you configure the **Secure Gateway Addr** field to 0.0.0.0.	255.255.0.0
Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.	0

Table 26-7 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is **N/A** when 0 is configured in the **Port Start** field.	
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by setting this field to **Yes**. Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to enable replay detection.	**No**
Key Management	Press [SPACE BAR] to choose either **IKE** or **Manual** and then press [ENTER]. **Manual** is useful for troubleshooting if you have problems using **IKE** key management.	**IKE**
Edit Key Management Setup	Press [SPACE BAR] to change the default **No** to **Yes** and then press [ENTER] to go to a key management menu for configuring your key management setup (described later). If you set the **Key Management** field to **IKE**, this will take you to **Menu 27.1.1.1 – IKE Setup**. If you set the **Key Management** field to **Manual**, this will take you to **Menu 27.1.1.2 – Manual Setup**.	**No**
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.		

26.10 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

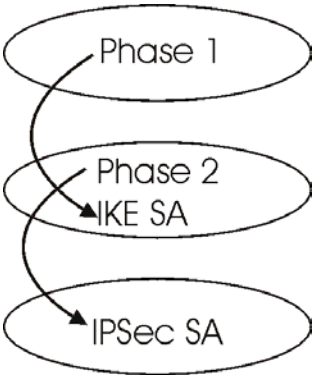


Figure 26-6 Two Phases to Set Up the IPSec SA

In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography – see *section 26.10.3*. Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The Prestige automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The Prestige also automatically renegotiates the IPSec SA So, what's the catch? XAUTH is vulnerable to man-in-the-middle attacks,

especially when used with "main mode" IKE and a group pre-shared key as described above. XAUTH also carries known plaintext (name and password prompts) as encrypted payload—hints an attacker might use to try to "crack" the encryption key. if both IPSec routers have keep alive enabled, even if there is no traffic. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

26.10.1 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

26.10.2 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - **DH1**) and 1024-bit (Group 2 – **DH2**) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

26.10.3 Perfect Forward Secrecy (PFS)

Enabling PFS means that the key is transient. The key is thrown away and replaced by a brand new key using a new Diffie-Hellman exchange for each new IPSec SA setup. With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time-consuming) Diffie-Hellman exchange is the trade-off for this extra security.

This may be unnecessary for data that does not require such security, so PFS is disabled (**None**) by default in the Prestige. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).

26.11 Configuring IKE Settings

This may be unnecessary for data that does not require such security, so PFS is disabled (**None**) by default in the Prestige. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).

```
                    Menu 27.1.1.1 - IKE Setup

          Phase 1
            Negotiation Mode= Main
            Pre-Shared Key= ?
            Encryption Algorithm = DES
            Authentication Algorithm = MD5
            SA Life Time (Seconds)= 28800
            Key Group= DH1

          Phase 2
            Active Protocol  = ESP
            Encryption Algorithm  = DES
            Authentication Algorithm  = SHA1
            SA Life Time (Seconds)= 28800
            Encapsulation  = Tunnel
            Perfect Forward Secrecy (PFS)= None


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

Figure 26-7 Menu 27.1.1.1 IKE Setup

Table 26-8 Menu 27.1.1.1 IKE Setup

FIELD	DESCRIPTION	EXAMPLE
Phase 1		
Negotiation Mode	Press [SPACE BAR] to choose from **Main** or **Aggressive** and then press [ENTER]. Multiple SAs connecting through a secure gateway must have the same negotiation mode.	**Main**
Pre-Shared Key	Prestige gateways authenticate an IKE VPN session by matching pre-shared keys. Pre-shared keys are best for small networks with fewer than ten nodes. Enter your pre-shared key here. Enter up to 31 characters. Any character may be used, including spaces, but trailing spaces are truncated. Multiple SAs connecting through a secure gateway must have the same pre-shared key.	

Table 26-8 Menu 27.1.1.1 IKE Setup

FIELD	DESCRIPTION	EXAMPLE
Encryption Algorithm	When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. Prestige **DES** encryption algorithm uses a 56-bit key. Triple DES (**3DES**), is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in slightly increased latency and decreased throughput. Press [SPACE BAR] to choose from **3DES** or **DES** and then press [ENTER].	**DES**
Authentication Algorithm	**MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slightly slower. Press [SPACE BAR] to choose from **SHA1** or **MD5** and then press [ENTER].	**MD5**
SA Life Time (Seconds)	Define the length of time before an IKE Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short **SA Life Time** increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.	28800 (default)
Key Group	You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.	**DH1**
Phase 2		
Active Protocol	Press [SPACE BAR] to choose from **ESP** or **AH** and then press [ENTER]. See earlier for a discussion of these protocols.	**ESP**
Encryption Algorithm	Press [SPACE BAR] to choose from **NULL**, **3DES** or **DES** and then press [ENTER]. Select **NULL** to set up a tunnel without encryption.	**DES**
Authentication Algorithm	Press [SPACE BAR] to choose from **SHA1** or **MD5** and then press [ENTER].	**SHA1**
SA Life Time (Seconds)	Define the length of time before an IKE Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days).	28800 (default)
Encapsulation	Press [SPACE BAR] to choose from **Tunnel** mode or **Transport** mode and then press [ENTER]. See earlier for a discussion of these.	**Tunnel**

Table 26-8 Menu 27.1.1.1 IKE Setup

FIELD	DESCRIPTION	EXAMPLE
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Press [SPACE BAR] and choose from **DH1** or **DH2** to enable PFS. **DH1** refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower).	**None**
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.		

26.12 Manual Key Setup

You only configure **Menu 27.1.1.2 – Manual Setup** when you select **Manual** in the **Key Management** field in **Menu 27.1.1 – IPSec Setup**. Manual key management is useful if you have problems with **IKE** key management.

26.12.1 Active Protocol

This field is a combination of mode and security protocols used for the VPN. These parameters were discussed earlier.

Table 26-9 Active Protocol: Encapsulation and Security Protocol

MODE	SECURITY PROTOCOL
Tunnel	ESP
Transport	AH

26.12.2 Security Parameter Index (SPI)

An SPI is used to distinguish different SAs terminating at the same destination and using the same IPSec protocol. This data allows for the multiplexing of SAs to a single gateway. The **SPI** (Security Parameter Index) along with a destination IP address uniquely identify a particular Security Association (SA). The **SPI** is transmitted from the remote VPN gateway to the local VPN gateway. The local VPN gateway then uses the network, encryption and key values that the administrator associated with the SPI to establish the tunnel.

Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

To edit this menu, move the cursor to the **Edit Manual Setup** field in **Menu 27.1.1 – IPSec Setup** press [SPACE BAR] to select **Yes** and then press [ENTER] to go to **Menu 27.1.1.2 – Manual Setup**.

```
                Menu 27.1.1.2 - Manual Setup
Active Protocol= ESP Tunnel

ESP Setup
  SPI (Decimal)=
  Encryption Algorithm= DES
    Key1=
    Key2= N/A
    Key3= N/A
  Authentication Algorithm= SHA1
    Key=

AH Setup
  SPI (Decimal)= N/A
  Authentication Algorithm= N/A
    Key= N/A

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

Figure 26-8 Menu 27.1.1.2 Manual Setup

Table 26-10 Menu 27.1.1.2 Manual Setup

FIELD	DESCRIPTION	EXAMPLE
Active Protocol	Press [SPACE BAR] to choose from **ESP Tunnel**, **ESP Transport**, **AH Tunnel** or **AH Transport** and then press [ENTER]. Choosing an **ESP** combination causes the **AH Setup** fields to be non-applicable (**N/A**)	**ESP Tunnel**
ESP Setup	The **ESP Setup** fields are **N/A** if you chose an **AH Active Protocol**.	
SPI (Decimal)	The **SPI** must be unique and from one to four integers ("0" to "9").	1234
Encryption Algorithm	Press [SPACE BAR] to choose from **NULL**, **3DES** or **DES** and then press [ENTER]. Fill in the **Key1** field below when you choose **DES** and fill in fields **Key1** to **Key3** when you choose **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter any encryption keys.	**DES**
Key1	Enter a unique eight-character key. Any character may be used, including spaces, but trailing spaces are truncated. Fill in the **Key1** field when you choose **DES** and fill in fields **Key1** to **Key3** when you choose **3DES**.	89abcde
Key2	Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated).	
Key3	Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated).	
Authentication Algorithm	Press [SPACE BAR] to choose from **MD5** or **SHA1** and then press [ENTER].	**SHA1**

Table 26-10 Menu 27.1.1.2 Manual Setup

FIELD	DESCRIPTION	EXAMPLE
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for **MD5** authentication and 20 characters for **SHA-1** authentication. Any character may be used, including spaces, but trailing spaces are truncated.	123456789abcde
AH Setup	The **AH Setup** fields are **N/A** if you chose an **ESP Active Protocol**.	
SPI (Decimal)	The **SPI** must be from one to four unique decimal characters ("0" to "9") long.	**N/A**
Authentication Algorithm	Press [SPACE BAR] to choose from **MD5** or **SHA1** and then press [ENTER].	**N/A**
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for **MD5** authentication and 20 characters for **SHA-1** authentication. Any character may be used, including spaces, but trailing spaces are truncated.	**N/A**
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.		

26.13 Telecommuter VPN/IPSec Examples

The following examples show how multiple telecommuters can make VPN connections to a single Prestige at headquarters from remote IPSec routers that use dynamic WAN IP addresses.

26.13.1 Telecommuters Sharing One VPN Rule Example

Multiple telecommuters can use one VPN rule to simultaneously access a Prestige at headquarters. They must all use the same IPSec parameters (including the pre-shared key) but the local IP addresses (or ranges of addresses) cannot overlap. See the following table and figure for an example.

Having everyone use the same pre-shared key may create a vulnerability. If the pre-shared key is compromised, all of the VPN connections using that VPN rule are at risk. A recommended alternative is to use a different VPN rule for each telecommuter and identify them by unique IDs (see *section 26.13.2* for an example).

Table 26-11 Telecommuter and Headquarters Configuration Example

	TELECOMMUTER	HEADQUARTERS
My IP Address:	0.0.0.0 (dynamic IP address assigned by the ISP)	Public static IP address
Secure Gateway IP Address:	Public static IP address or domain name.	0.0.0.0 With this IP address only the telecommuter can initiate the IPSec tunnel.

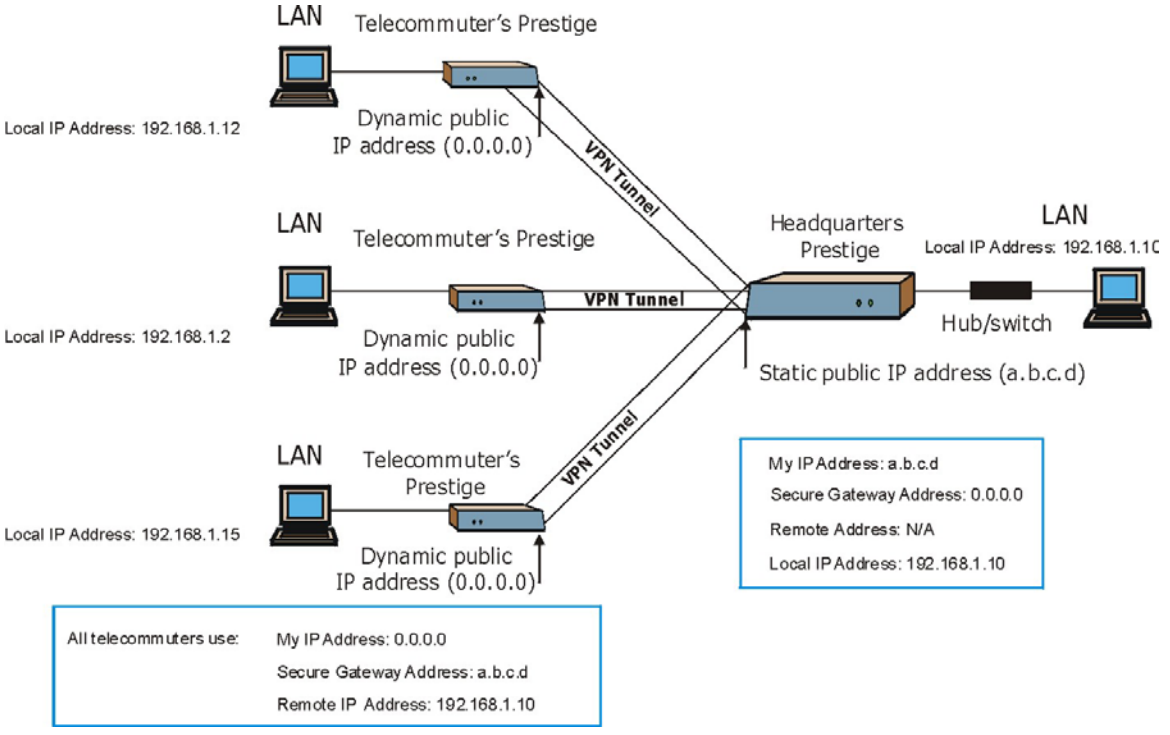


Figure 26-9 Telecommuters Sharing One VPN Rule Example

26.13.2 Telecommuters Using Unique VPN Rules Example

With aggressive negotiation mode (see section *26.10.1Negotiation Mode*) the Prestige can use the ID types and contents to distinguish between VPN rules. Telecommuters can each use a separate VPN rule to simultaneously access a Prestige at headquarters. They can use different IPSec parameters (including the pre-shared key) and the local IP addresses (or ranges of addresses) can overlap.

See the following graphic for an example where three telecommuters each use a different VPN rule to initiate a VPN connection to a Prestige located at headquarters. The Prestige at headquarters identifies each by its ID type and contents and uses the appropriate VPN rule to establish the VPN connection.

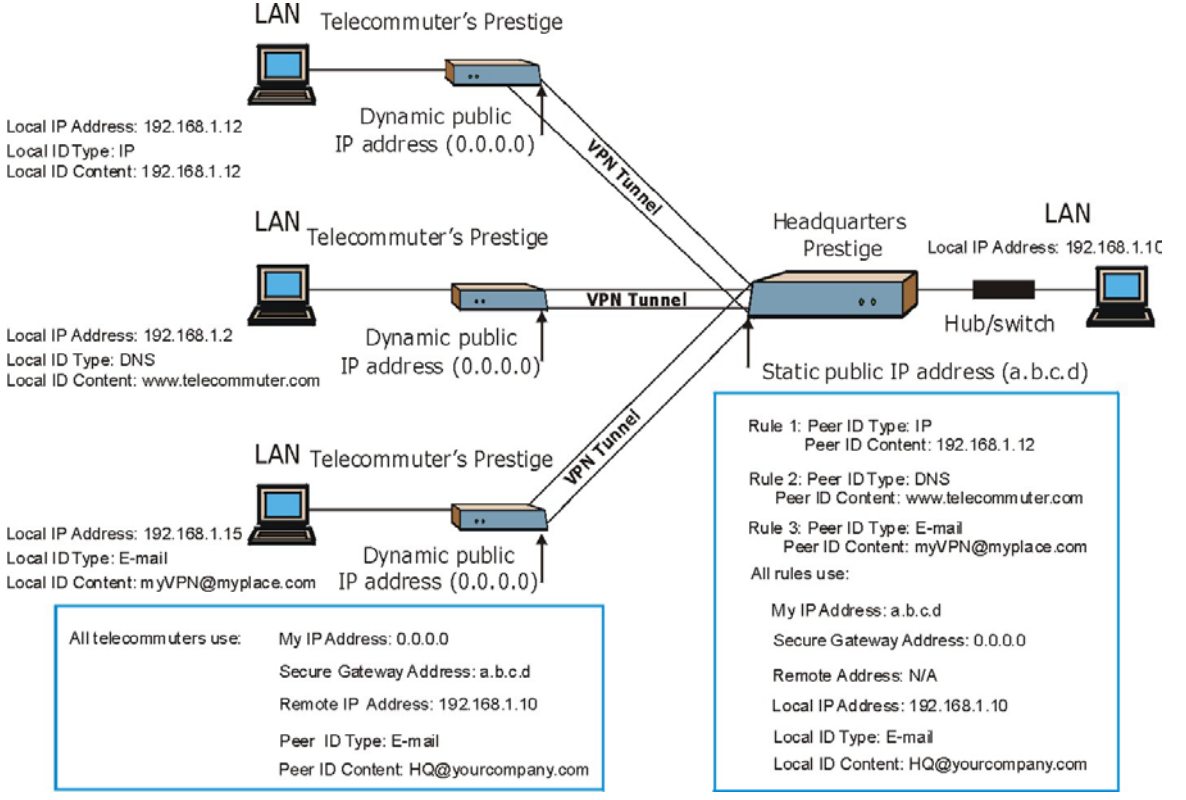


Figure 26-10 Telecommuters Using Unique VPN Rules Example

Chapter 27
SA Monitor

This chapter teaches you how to manage your SAs by using the SA Monitor in SMT menu 27.2.

27.1 SA Monitor Overview

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This menu (shown next) displays active VPN connections.

An SA times out automatically after one minute if there is no traffic.

1. Use the **Refresh** function to display active VPN connections.
2. Use the **Disconnect** function to cut off active connections.

Type 2 in **Menu 27 - VPN/IPSec Setup**, and then press [ENTER] to go to **Menu 27.2 - SA Monitor**.

```
                          Menu 27.2 - SA Monitor

 #                    Name                     Encap.      IPSec Algorithm
---    -------------------------------       ---------     ---------------
1          Taiwan : 3.3.3.1 - 3.3.3.3.100        Tunnel     ESP DES MD5
2
3
4
5
6
7
8
9
10
                     Select Command= Refresh
                     Select Connection= N/A

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

Figure 27-1 Menu 27.2 SA Monitor

Table 27-1 Menu 27.2 SA Monitor

FIELD	DESCRIPTION	EXAMPLE
#	This is the security association index number.	1
Name	This field displays the identification name for this VPN policy. This name is unique for each connection where the secure gateway IP address is a public static IP address. When the secure gateway IP address is 0.0.0.0 (as discussed in the last chapter), there may be different connections using this same VPN rule. In this case, the name is followed by the remote IP address as configured in **Menu 27.1.1. – IPSec Setup**. Individual connections using the same VPN rule may be terminated without affecting other connections using the same rule.	**Taiwan**
Encap.	This field displays **Tunnel** mode or **Transport** mode. See previous for discussion.	**Tunnel**
IPSec Algorithm	This field displays the security protocols used for an SA. **ESP** provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit **DES** and 168-bit **3DES**. **NULL** denotes a tunnel without encryption. An incoming SA may have an **AH** in addition to **ESP**. The Authentication Header provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. **AH** choices are **MD5** (default - 128 bits) and **SHA -1**(160 bits). Both **AH** and **ESP** increase Prestige processing requirements and communications latency (delay).	**ESP DES MD5**
Select Command	Press [SPACE BAR] to choose from **Refresh**, **Disconnect** or **None** and then press [ENTER]. You must select a connection in the next field when you choose the **Disconnect** command. **Refresh** displays current active VPN connections. **None** allows you to jump to the "Press ENTER to Confirm…" prompt.	**Refresh**
Select Connection	Type the VPN connection index number that you want to disconnect and then press [ENTER].	**1**
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.		

Chapter 28
IPSec Log

This chapter interprets common IPSec log messages.

28.1 IPSec Logs

To view the IPSec and IKE connection log, type 3 in menu 27 and press [ENTER] to display the IPSec log as shown next. The following figure shows a typical log from the initiator of a VPN connection.

```
Index:    Date/Time:              Log:
------------------------------------------------------------
 001    01 Jan 08:02:22    Send Main Mode request to <192.168.100.101>
 002    01 Jan 08:02:22    Send:<SA>
 003    01 Jan 08:02:22    Recv:<SA>
 004    01 Jan 08:02:24    Send:<KE><NONCE>
 005    01 Jan 08:02:24    Recv:<KE><NONCE>
 006    01 Jan 08:02:26    Send:<ID><HASH>
 007    01 Jan 08:02:26    Recv:<ID><HASH>
 008    01 Jan 08:02:26    Phase 1 IKE SA process done
 009    01 Jan 08:02:26    Start Phase 2: Quick Mode
 010    01 Jan 08:02:26    Send:<HASH><SA><NONCE><ID><ID>
 011    01 Jan 08:02:26    Recv:<HASH><SA><NONCE><ID><ID>
 012    01 Jan 08:02:26    Send:<HASH>
 Clear IPSec Log (y/n):
```

Figure 28-1 Example VPN Initiator IPSec Log

The following figure shows a typical log from the VPN connection peer.

```
Index:    Date/Time:              Log:
-----------------------------------------------------------
 001    01 Jan 08:08:07    Recv Main Mode request from <192.168.100.100>
 002    01 Jan 08:08:07    Recv:<SA>
 003    01 Jan 08:08:08    Send:<SA>
 004    01 Jan 08:08:08    Recv:<KE><NONCE>
 005    01 Jan 08:08:10    Send:<KE><NONCE>
 006    01 Jan 08:08:10    Recv:<ID><HASH>
 007    01 Jan 08:08:10    Send:<ID><HASH>
 008    01 Jan 08:08:10    Phase 1 IKE SA process done
 009    01 Jan 08:08:10    Recv:<HASH><SA><NONCE><ID><ID>
 010    01 Jan 08:08:10    Start Phase 2: Quick Mode
 011    01 Jan 08:08:10    Send:<HASH><SA><NONCE><ID><ID>
 012    01 Jan 08:08:10    Recv:<HASH>
 Clear IPSec Log (y/n):
```

Figure 28-2 Example VPN Responder IPSec Log

This menu is useful for troubleshooting. A log index number, the date and time the log was created and a log message are displayed.

Double exclamation marks (!!) denote an error or warning message.

The following table shows sample log messages during IKE key exchange.

Table 28-1 Sample IKE Key Exchange Logs

LOG MESSAGE	DESCRIPTION
Cannot find outbound SA for rule <#d>	The packet matches the rule index number (#d), but Phase 1 or Phase 2 negotiation for outbound (from the VPN initiator) traffic is not finished yet.
Send Main Mode request to <IP> Send Aggressive Mode request to <IP>	The Prestige has started negotiation with the peer.
Recv Main Mode request from <IP> Recv Aggressive Mode request from <IP>	The Prestige has received an IKE negotiation request from the peer.
Send:<Symbol><Symbol> Recv:<Symbol><Symbol>	IKE uses the ISAKMP protocol (refer to RFC2408 – ISAKMP) to transmit data. Each ISAKMP packet contains payloads of different types that show in the log - see *Table 28-3*.
Phase 1 IKE SA process done	Phase 1 negotiation is finished.

Table 28-1 Sample IKE Key Exchange Logs

LOG MESSAGE	DESCRIPTION
Start Phase 2: Quick Mode	Phase 2 negotiation is beginning using Quick Mode.
!! IKE Negotiation is in process	The Prestige has begun negotiation with the peer for the connection already, but the IKE key exchange has not finished yet.
!! Duplicate requests with the same cookie	The Prestige has received multiple requests from the same peer but it is still processing the first IKE packet from that peer.
!! No proposal chosen	The parameters configured for Phase 1 or Phase 2 negotiations don't match. Please check all protocols and settings for these phases. For example, one party may be using 3DES encryption, but the other party is using DES encryption, so the connection will fail.
!! Verifying Local ID failed !! Verifying Remote ID failed	During IKE Phase 2 negotiation, both parties exchange policy details, including local and remote IP address ranges. If these ranges differ, then the connection fails.
!! Local / remote IPs of incoming request conflict with rule <#d>	If the security gateway is "0.0.0.0", the Prestige will use the peer's "Local Addr" as its "Remote Addr". If this IP (range) conflicts with a previously configured rule then the connection is not allowed.
!! Invalid IP <IP start>/<IP end>	The peer's "Local IP Addr" range is invalid.
!! Remote IP <IP start> / <IP end> conflicts	If the security gateway is "0.0.0.0", the Prestige will use the peer's "Local Addr" as its "Remote Addr". If a peer's "Local Addr" range conflicts with other connections, then the Prestige will not accept VPN connection requests from this peer.
!! Active connection allowed exceeded	The Prestige limits the number of simultaneous Phase 2 SA negotiations. The IKE key exchange process fails if this limit is exceeded.
!! IKE Packet Retransmit	The Prestige did not receive a response from the peer and so retransmits the last packet sent.
!! Failed to send IKE Packet	The Prestige cannot send IKE packets due to a network error.
!! Too many errors! Deleting SA	The Prestige deletes an SA when too many errors occur.

The following table shows sample log messages during packet transmission.

Table 28-2 Sample IPSec Logs During Packet Transmission

LOG MESSAGE	DESCRIPTION
!! WAN IP changed to <IP>	If the Prestige's WAN IP changes, all configured "My IP Addr" are changed to b "0.0.0.0".. If this field is configured as 0.0.0.0, then the Prestige will use the current Prestige WAN IP address (static or dynamic) to set up the VPN tunnel.
!! Cannot find Phase 2 SA	The Prestige cannot find a phase 2 SA that corresponds with the SPI of an inbound packet (from the peer); the packet is dropped.
!! Discard REPLAY packet	If the Prestige receives a packet with the wrong sequence number it will discard it.
!! Inbound packet authentication failed	The authentication configuration settings are incorrect. Please check them.
!! Inbound packet decryption failed	The decryption configuration settings are incorrect. Please check them.
Rule <#d> idle time out, disconnect	If an SA has no packets transmitted for a period of time (configurable via CI command), the Prestige drops the connection.

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

Table 28-3 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature

Table 28-3 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

Part V:

Appendices and Index

This part provides appendices and an index of key terms.

Appendix A Troubleshooting

This Appendix covers potential problems and the corresponding remedies.

Problems Starting Up the Prestige

Chart 1 Troubleshooting the Start-Up of Your Prestige

PROBLEM	CORRECTIVE ACTION	
None of the LEDs turn on when you turn on the Prestige.	Make sure that you have the included power adaptor connected to the Prestige and to an appropriate power source.	
	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.	
Cannot access the Prestige via the console port.	1. Check to see if the Prestige is connected to your computer's console port.	
	2. Check to see if the communications program is configured correctly. The communications software should be configured as follows:	VT100 terminal emulation
		9600 bps is the default speed on leaving the factory. Try other speeds in case the speed has been changed.
		No parity, 8 data bits, 1 stop bit, data flow set to none.

Problems With the ISDN Line

Chart 2 Troubleshooting the ISDN Line

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

Problems With a LAN Interface

Chart 3 Troubleshooting the LAN Interface

PROBLEM	CORRECTIVE ACTION
Cannot access the Prestige from the LAN.	Check your Ethernet cable type and connections. Refer to the *Rear Panel and Connections* section for LAN connection instructions.
	Make sure your Ethernet card is installed and functioning properly.
Cannot ping any computer on the LAN.	Check the Ethernet LEDs on the front panel. One of these LEDs should be on. If they are all off, check the cables between your Prestige and hub or the station.
	Verify that the IP address and the subnet mask of the Prestige and the computers are on the same subnet.

Problems Connecting to a Remote Node or ISP

Chart 4 Troubleshooting a Connection to a Remote Node or ISP

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

Remote User Dial-in Problems

Chart 5 Troubleshooting Remote User Dial-in Problems

PROBLEM	CORRECTIVE ACTION
A remote user cannot dial-in.	First verify that you have configured the authentication parameters in Menu 13. These would be CLID Authen and Recv. Authen.
	In Menu 14.1, verify the user name and password for the remote dial-in user.
	If the remote dial-in user is negotiating IP, verify that the IP address is supplied correctly in Menu 13. Check that either the remote dial-in user is supplying a valid IP address, or that the Prestige is assigning a valid address from the IP pool.
	If the remote dial-in user is negotiating IPX, verify that the IPX network number is valid from the IPX pool (if it is being used).

Problems With the Password

Chart 6 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
Cannot access the Prestige	The password field is case sensitive. Make sure that you enter the correct password using the proper casing.
	See the *Resetting the Prestige* section for details on restoring all of the factory default settings.

Problems With Remote Management

Chart 7 Troubleshooting Telnet

PROBLEM	CORRECTIVE ACTION
Cannot access the Prestige from the LAN or WAN.	When NAT is enabled: ➢ Use the Prestige's WAN IP address when configuring from the WAN. ➢ Use the Prestige's LAN IP address when configuring from the LAN.
	Refer to the *Problems with the LAN Interface* section for instructions on checking your LAN connection.

Appendix B
Power Adapter Specifications

NORTH AMERICAN PLUG STANDARDS	
AC Power Adapter Model	DV-121AACS
Input Power	AC120Volts/60Hz/23W max
Output Power	AC12Volts/1.0A
Power Consumption	8 W
Safety Standards	UL, CUL (UL 1310, CSA C22.2 No.223)
NORTH AMERICAN PLUG STANDARDS	
AC Power Adapter Model	AA-121A
Input Power	AC120Volts/60Hz/18W max
Output Power	AC12Volts/1.0A
Power Consumption	8 W
Safety Standards	UL, CUL (UL 1310, CSA C22.2 No.223)
NORTH AMERICAN PLUG STANDARDS	
AC Power Adapter Model	DSA-009F-12A
Input Power	AC100-250V/47-63Hz/0.3A
Output Power	DC 12 Volts/0.75A
Power Consumption	8 W
Safety Standards	UL, CUL, T-mark (UL 1950, CSA C22.2 No.950)
UNITED KINGDOM PLUG STANDARDS	
AC Power Adapter Model	AA-121AD
Input Power	AC230Volts/50Hz/140mA
Output Power	AC12Volts/1.0A
Power Consumption	8 W
Safety Standards	ITS-GS, CE (EN 60950, BS 7002)

EUROPEAN PLUG STANDARDS	
AC Power Adapter Model	DV-121AACCP-5716
Input Power	AC230Volts/50Hz/100mA
Output Power	AC12Volts/1.0A
Power Consumption	8W
Safety Standards	TUV-GS, CE (EN 60950)
EUROPEAN PLUG STANDARDS	
AC Power Adapter Model	AA-121ABN
Input Power	AC230Volts/50Hz/140mA
Output Power	AC12Volts/1.0A
Power Consumption	8 W
Safety Standards	ITS-GS, CE (EN 60950)
china Standards	
AC Power Adapter Model	DV-121AACCP-5720
Input Power	AC220Volts/50Hz/18W
Output Power	AC12Volts/1.0A
Power Consumption	8 W
Safety Standards	CCEE (GB8898)
china Standards	
AC Power Adapter Model	BH-48 (AA-121AP)
Input Power	AC220Volts/50Hz
Output Power	AC12Volts/1.0A
Power Consumption	8 W
Safety Standards	CCEE (GB8898)

Index

Number

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

Z