Prestige 100L

IDSL Router

User's Guide

Version 2.40

June, 2000

ZyXEL

TOTAL INTERNET ACCESS SOLUTION

Prestige 100L

IDSL Router

COPYRIGHT

DISCLAIMER

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

TRADEMARKS

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

Federal Communications Commission (FCC) Interference Statement

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

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

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

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

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

NOTICE 1

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

NOTICE 2

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

DECLARATION OF CONFORMITY

Per FCC Part 2 Section 2. 1077(a)

The following equipment:

Product Name : IDSL Hub Router

Trade Name : ZyXEL

Model Number : PRESTIGE 100L

Is herewith confirmed to comply with the requirements of FCC Part 15 Rules.
Operation is subject to the following two conditions:

(1)This device may not cause harmful interference, and

(2)This device must accept any interference received, including interference that may cause undesired operation.

The result of electromagnetic emission has been evaluated by QuieTek EMC laboratory (NVLAP Lab. Code : 200347-0) and showed in the test report.
(Report No. : QTK-003H028F)

It is understood that each unit marketed is identical to the device as tested, and Any changes to the device that could adversely affect the emission Characteristics will require retest.

The following importer / manufacturer is responsible for this declaration:

Company Name ZyXEL COMMUNICATIONS, INC

Company Address 1650 MICALONA AVENUE PLACENTIA CA 92870

Telephone (714) 632-0882 Facsimile : (714) 632-0858

Person is responsible for marking this declaration:

GORDON YANG — Name (Full name)

VICE PRESIDENT — Position / Title

04/13/00 — Date

Gordyang — Legal Signature

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.

CE

Declaration of Conformity

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

The following Equipment:

Product	:	IDSL Hub Router
Model Number	:	PRESTIGE 100L

RFI Emission: Limit class B according to EN 55022:1994
Limits class B for harmonic current emission according to EN 61000-3-2/1995
Limitation of voltage fluctuation and flicker in low-voltage supply system according to EN 61000-3-3/1995

Immunity : Generic immunity standard according to EN 50082-1:1997
Electrostatic Discharge according to EN 61000-4-2:1995
Contact Discharge: 4 kV, Air Discharge : 8 kV
Radio-frequency electromagnetic field according to EN 61000-4-3:1995
80 – 1000MHz with 1kHz AM 80% Modulation: 3V/m
Electromagnetic field from digital telephones according to ENV 50204:1995
900 ±5MHz with 200Hz rep. Frequency ,Duty Cycle 50%
Electrical fast transient/burst according to EN 61000-4-4:1995
AC/DC power supply: 1kV, Data/Signal lines : 0.5kV
Surge immunity test according to EN 61000-4-5:1995
AC/DC Line to Line: 1kV, AC/DC Line to Earth : 2kV
Immunity to conducted disturbances, Induced by radio-frequency fields: EN 61000-4-6:1995
0.15 – 80MHz with 1kHz AM 80% Modulation: 3V/m
Power frequency magnetic field immunity test according to EN 61000-4-8:1993
3A/m at frequency 50Hz
Voltage dips, short interruptions and voltage variations immunity test according to EN 61000-4-11:1994
30% Reduction @ 10ms, 60% Reduction @100ms, >95%Reduction @5000ms

The following importer/manufacturer is responsible for this declaration:

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

Person is responsible for marking this declaration:

Manfred RECLA — Name (Full Name)
ZyXEL European Techn. Support — Position/ Title
Vienna, April 12, 2000 — Date
Manfred Recla — Legal Signature

Declaration of Conformity

We, the Manufacturer/Importer,

ZyXEL Communications Corp.
No. 6, Innovation Road II,
Science-Based Industrial Park,
Hsinchu, Taiwan, 300 R.O.C

declare that the product

Prestige 100L

is in conformity with
(reference to the specification under which conformity is declared)

	STANDARD	STANDARD ITEM	VERSION
•	EN 50082-1	Generic immunity standard	1997
•	EN 55022	Radio disturbance characteristics – Limits and method of measurement.	1994
•	EN 61000-3-2	Disturbance in supply system caused by household appliances and similar electrical equipment “Harmonics”.	1995
•	EN 61000-3-3	Disturbance in supply system caused by household appliances and similar electrical equipment “Voltage fluctuations”.	1995
•	EN 61000-4-2	Electrostatic discharge immunity test – Basic EMC Publication	1995
•	EN 61000-4-3	Radiated, radio-frequency, electromagnetic field immunity test	1995
•	EN 61000-4-4	Electrical fast transient / burst immunity test - Basic EMC Publication	1995
•	EN 61000-4-5	Surge immunity test	1995
•	EN 61000-4-6	Immunity to conducted disturbances, induced by radio-frequency fields	1995
•	EN 61000-4-8	Power magnetic test	1993
•	EN 61000-4-11	Voltage dips, short interruptions and voltage variations immunity tests	1994
•	ENV 50204	Electromagnetic field from digital telephones test	1995

NOTE: The TCF file can be obtained at: **ZyXEL Communications Services, GmbH.**
Thaliastrasse 125a/2/2/4
A-1160 Vienna, AUSTRIA.

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

Online Registration

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

Customer Support

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

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

Table of Contents

Declaration of Conformity ..... **vii**
Cutomer Support ..... **ix**
Table of Contents ..... **xi**
List of Figures ..... **xv**
List of Tables ..... **xvii**
Preface ..... **xix**
Chapter 1 : Getting to Know Your Prestige **1-1**
1.1 The Prestige 100L IDSL Router 1-1
1.2 Features of the Prestige 100L 1-1
Chapter 2 : Hardware Installation and Initial Setup **2-1**
2.1 Front Panel LEDs and Back Panel Ports 2-1
2.1.1 Front Panel LEDs 2-1
2.2 Prestige 100L Rear Panel and Connections 2-2
2.3 Housing 2-3
2.4 Power Up Your Prestige 2-4
2.5 Navigating the SMT (System Management Terminal) Interface 2-4
2.5.1 Main Menu 2-5
2.5.2 System Management Terminal Interface Summary 2-6
2.6 Changing the System Password 2-7
2.6.1 Resetting the Prestige 2-7
2.7 General Setup 2-8
2.8 IDSL Setup 2-9
2.9 Ethernet Setup 2-9
2.9.1 General Setup 2-10
Chapter 3 : Internet Access **3-1**

3.1 TCP/IP and DHCP for LAN 3-1
3.1.1 Factory LAN Defaults 3-1
3.1.2 IP Address and Subnet Mask 3-1
3.1.3 Private IP Addresses 3-2
3.1.4 RIP (Routing Information Protocol) Setup 3-2
3.1.5 DHCP (Dynamic Host Configuration Protocol) Configuration 3-3
3.2 TCP/IP and DHCP Ethernet Setup 3-4
3.3 Internet Access Setup 3-6
3.4 Single User Account (SUA) 3-7
3.4.1 Advantages of SUA 3-7
3.4.2 Single User Account Configuration 3-8
3.5 Multiple Servers Behind the SUA 3-8
3.5.1 Configuring a Server Behind the SUA 3-9
Chapter 4 : Remote Node Setup 4-1
4.1 Remote Node Profile 4-1
4.1.1 Editing PPP Options 4-3
4.2 Editing TCP/IP Options 4-3
4.3 Remote Node Filter 4-7
Chapter 5 : IP Static Route Setup 5-1
5.1 IP Static Route Setup 5-2
Chapter 6 : Filter Configuration 6-1
6.1 About Filtering 6-1
6.1.1 The Filter Structure of the Prestige 6-2
6.2 Configuring a Filter Set 6-4
6.2.1 Filter Rules Summary Menu 6-6
6.2.2 Configuring a Filter Rule 6-7
6.2.3 TCP/IP Filter Rule 6-7
6.2.4 Generic Filter Rule 6-11

6.3 Example Filter 6-13
6.4 Applying a Filter and Factory Defaults 6-16
6.4.1 Ethernet Traffic 6-16
6.4.2 Remote Node Filters 6-16
Chapter 7 : SNMP (Simple Network Management Protocol) 7-1
Chapter 8 : System Security 8-1
Chapter 9 : Telnet Configuration and Capabilities 9-1
9.1 About Telnet Configuration 9-1
9.2 Telnet Capabilities 9-1
9.2.1 Single Administrator 9-1
9.2.2 System Timeout 9-1
Chapter 10 : System Information and Diagnosis 10-1
10.1 System Status 10-2
10.2 System Information and Console Port Speed 10-4
10.2.1 System Information 10-4
10.2.2 Console Port Speed 10-5
10.3 Log and Trace 10-6
10.3.1 Viewing Error Log 10-6
10.3.2 Syslog Server 10-7
10.4 Diagnostic 10-8
Chapter 11 : Transferring Files 11-1
11.1 Filename Conventions 11-1
11.2 Backup Configuration 11-2
11.3 Restore Configuration 11-2
11.4 Upload Firmware 11-3
11.4.1 Uploading the Router Firmware 11-3
11.4.2 Uploading Router Configuration File 11-4
11.5 TFTP File Transfer 11-5

11.5.1 Using the FTP command from the DOS Prompt 11-6
11.6 Command Interpreter Mode 11-8
Chapter 12 : Troubleshooting 12-1
12.1 Problems Starting Up the Prestige 12-1
12.2 Problems with the LAN Interface 12-2
12.3 Problems with the WAN interface 12-2
Glossary ..... A
Appendix A Important Safety Instructions ..... M
Appendix B Power Adapter Specifications ..... N
Index ..... O

List of Figures

Figure 2-1 Front Panel 2-1
Figure 2-2 Prestige 100L Rear Panel and Connections 2-2
Figure 2-3 Initial Screen 2-4
Figure 2-4 Password Screen 2-4
Figure 2-5 Prestige 100L Main Menu 2-6
Figure 2-6 Menu 23 – System Security 2-7
Figure 2-7 Menu 1 – General Setup 2-8
Figure 2-8 Menu 2 – IDSL Setup 2-9
Figure 2-9 Menu 3 – Ethernet Setup 2-10
Figure 2-10 Menu 3.1 – General Ethernet Setup 2-10
Figure 3-1 Menu 3 – Ethernet Setup Screen 3-4
Figure 3-2 Menu 3.2 – TCP/IP and DHCP Ethernet Setup Screen 3-4
Figure 3-3 Menu 4 – Internet Access Setup 3-6
Figure 3-4 Example of a SUA Topology 3-9
Figure 3-5 Multiple Server Configuration 3-10
Figure 4-1 Menu 11.1 – Remote Node Profile 4-1
Figure 4-2 Menu 11.2 – Remote Node PPP Options 4-3
Figure 4-3 Remote Node Filter 4-7
Figure 5-1 Example of an IP Static Route Setup 5-1
Figure 5-2 Menu 12 – IP Static Route Setup 5-2
Figure 5-3 Menu 12. 1 – Edit IP Static Route 5-2
Figure 6-1 Outgoing Packet Filtering Process 6-1
Figure 6-2 Filter Rule Process 6-3
Figure 6-3 Menu 21.1.1 – TCP/IP Filter Rule 6-8
Figure 6-4 Executing an IP Filter 6-10

Figure 6-5 Menu 21.4.1.1 – Generic Filter Rule....6-11
Figure 6-6 Telnet Filter Example....6-13
Figure 6-7 Example Filter – Menu 21.1.1....6-14
Figure 6-8 Example Filter Rules Summary – Menu 21.1.3....6-15
Figure 7-1 Menu 22 – SNMP Configuration....7-1
Figure 8-1 Menu 23 – System Password....8-1
Figure 9-1 Telnet Configuration on a TCP/IP Network....9-1
Figure 10-1 Menu 24 – System Maintenance....10-1
Figure 10-2 Menu 24.1 – System Maintenance – Status....10-2
Figure 10-3 Menu 24.2 – System Information and Console Port Speed....10-4
Figure 10-4 Menu 24.2.1 – System Maintenance – Information....10-4
Figure 10-5 Menu 24.2.2 – System Maintenance – Change Console Port Speed....10-5
Figure 10-6 Menu 24.3 – System Maintenance – Log and Trace....10-6
Figure 10-7 Examples of Error and Information Messages....10-6
Figure 10-8 Menu 24.3.2 – System Maintenance – Syslog and Accounting....10-7
Figure 10-9 Menu 24.4 – System Maintenance – Diagnostic....10-8
Figure 11-1 Menu 24.5 – System Maintenance – Backup Configuration....11-2
Figure 11-2 Menu 24.6 – System Maintenance – Restore Configuration....11-2
Figure 11-3 Menu 24.7 – System Maintenance – Upload Firmware....11-3
Figure 11-4 Menu 24.7.1 – System Maintenance – Upload Router Firmware....11-4
Figure 11-5 Menu 24.7.2 – System Maintenance – Upload Router Configuration File....11-5
Figure 11-6 FTP Session Example....11-6
Figure 11-7 Command Mode....11-8

List of Tables

Table 2-1 LED Functions 2-1
Table 2-2 Main Menu Commands 2-5
Table 2-3 Main Menu Summary 2-6
Table 2-4 General Setup Menu Field 2-8
Table 2-5 IDSL Setup Menu Fields 2-9
Table 3-1 LAN DHCP Setup Menu Fields 3-5
Table 3-2 LAN TCP/IP Setup Menu Fields 3-6
Table 3-3 Internet Access Setup Menu Fields 3-7
Table 3-4 Single User Account Menu Fields 3-8
Table 3-5 Services as Compared to Port Number 3-10
Table 4-1 Fields in Menu 11.1 4-2
Table 4-2 Fields in Menu 11.2 (PPP Options) 4-3
Table 4-3 Protocol-dependent Parameters for Remote Node Setup 4-4
Table 4-4 Remote Node Network Layer Options Menu Fields 4-5
Table 5-1 IP Static Route Menu Fields 5-3
Table 6-1 Abbreviations Used in the Filter Rules Summary Menu 6-6
Table 6-2 Abbreviations Used If Filter Type Is IP 6-7
Table 6-3 Abbreviations Used If Filter Type Is GEN 6-7
Table 6-4 TCP/IP Filter Rule Menu Fields 6-8
Table 6-5 Generic Filter Rule Menu Fields 6-12
Table 7-1 Fields in Menu 22 (SNMP Configuration) 7-2
Table 10-1 System Maintenance – Status Menu Fields 10-3
Table 10-2 Fields in System Maintenance 10-5
Table 10-3 System Maintenance Menu Syslog Parameters 10-7
Table 10-4 System Maintenance Menu Diagnostic 10-8

Table 11-1 Filename Conventions 11-1
Table 11-2 Third Party TFTP Clients 11-7
Table 11-3 Third Party TFTP Clients – General Fields 11-7
Table 12-1 Troubleshooting Starting Up Your Prestige 12-1
Table 12-2 Troubleshooting the LAN Interface 12-2
Table 12-3 Troubleshooting the WAN interface 12-2

Preface

About Your Router

Congratulations on your purchase of the Prestige 100L IDSL Router. Do not forget to register your Prestige (fast, easy online registration at www.zyxel.com) for free future product updates and information.
The Prestige 100L is the perfect companion to the Prestige 1600, offering inexpensive yet complete telecommunications and internetworking solutions for your home or branch office. The Prestige is ideal for everything from Internet access, to making LAN-to-LAN connections, to Remote Nodes. Distinguishing features include:

- Support for a full range of networking protocols such as TCP/IP (Transmission Control Protocol/Internet Protocol),
- Simple Network Management,
- Solid security features that give it the flexibility to provide a complete networking solution for Internet access and business users.

Ease of Installation

The Prestige is a self-contained unit that is quick and easy to install.

Additional Installation Requirements

Your Prestige 100L is easy to install and to configure. In addition, there are other hardware and software requirements you need before you can install and use your Prestige. These requirements include:

- IDSL service provided by local telephone company.
- An Ethernet connection to your computer.
- A computer equipped with communications software configured to the following parameters:
  - VT100 terminal emulation.
  - 9600 Baud rate (or 19200, 38400, 57600, 115200).
  - No parity, 8 Data bits, 1 Stop bit and no flow control.

After the Prestige has been successfully connected to your network, you can make future changes to the configuration by using the console port or telnet.

About This User's Manual

This manual is designed to guide you through the SMT configuration of your Prestige 100L for its various applications.

Structure of this Manual

This manual is structured as follows:

Part I. *Getting Started* (Chapters 1 to 3) is structured as a step-by-step guide to help you connect, install, and setup your Prestige to operate on your network and access the Internet.

Part II. *Advanced Applications* (Chapters 4 and 5) describe the advanced applications of your Prestige, such as Remote Node Setup and IP Static routes.

Part III. *Advanced Management* (Chapters 6 to 12) provides information on Prestige Filtering, System Information and Diagnosis, Transferring Files and Telnet.

Part IV. *Troubleshooting* (Chapter 13), provides information about solving common problems as well as some Appendices.

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

Related Documentation

➢ Quick Start Manual

Our Quick Start Manual is designed to help you get your Prestige up and running right away. It contains a detailed easy to follow connection diagram, Prestige default settings, handy checklists and information on setting up your PC.

➢ Packing List Card

Finally, you should have a Packing List Card which lists all items that should have come with your Prestige 100L.

Syntax Conventions

- "Enter" means for you to type one or more characters and press the carriage return. "Select" or "Choose" means for you to select one from the predefined choices.
- The SMT menu titles and labels are in **Bold Times** font. The choices of a menu item are in **Bold Arial** font. A single keystroke is in Arial font and enclosed in square brackets, for instance, [Enter] means the Enter or carriage return key; [Esc] means the Escape Key.
- For brevity's sake, we will use "e.g.," as a shorthand for "for instance" and "i.e.," for "that is" or "in other words" throughout this manual.
- The word "Prestige" mentioned in this User's Guide refers to the Prestige 100L unless otherwise stated.

Part I:

GETTING STARTED

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

Chapter 1
Getting to Know Your Prestige

This chapter introduces the main features and applications of the Prestige.

1.1 The Prestige 100L IDSL Router

The Prestige 100L is the perfect IDSL Client for the Prestige 1600, offering inexpensive yet complete telecommunications and internetworking solutions for your home or branch office. The Prestige is ideal for everything from Internet access, LAN-to-LAN connections or Remote Access. ZyXEL's Prestige 100L provides not only ease of installation and Internet access, but also a complete security solution to protect your Intranet and efficiently manage data traffic on your network.

1.2 Features of the Prestige 100L

The following are the essential features of the Prestige 100L.

ISDN Digital Subscriber Line (IDSL)

IDSL is a digital subscriber service that uses a subset of the existing ISDN standard. It offers speed up to 128 kbps over a single twisted copper pair wire for distance up to 18,000 feet. Because IDSL uses the same standard as ISDN, users can use the existing ISDN terminal adapters, routers and bridges for IDSL connections. IDSL is the easiest and the least expensive to deploy among DSL technologies since a majority of the local loops are "ISDN-ready" and thus "IDSL-ready" as well.

Full Network Management

The Prestige incorporates SNMP (Simple Network Management Protocol) support and menu-driven network management via an RS-232C or telnet connection. All functions of the Prestige 100L are also software configurable via the SMT (System Management Terminal) interface. The SMT is a menu-driven interface that you can access from a terminal emulator through the console port or over a telnet connection.

PPP Security

The Prestige supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol).

Dynamic Host Configuration Protocol (DHCP)

DHCP allows you to assign dynamically and automatically IP address settings to hosts on your network.

Data Compression

The Prestige incorporates Stac Data Compression and Compression Control Protocol.

Internet Access

The Prestige supports TCP/IP protocol. It is also compatible with other IDSL access servers manufactured by vendors such as Ascend.

Single User Account (SUA)

This allows multiple users to access the LAN simultaneously using a single IP address. SUA address mapping can also be used for LAN to LAN.

Integrated 4-Port Ethernet Hub

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

Upgrade Prestige Firmware via LAN

You can upgrade the Prestige firmware over the local LAN.

Chapter 2
Hardware Installation and Initial Setup

This chapter shows you how to connect the hardware and perform the initial setup.

2.1 Front Panel LEDs and Back Panel Ports

2.1.1 Front Panel LEDs

The LEDs on the front panel indicate the operational status of the Prestige.

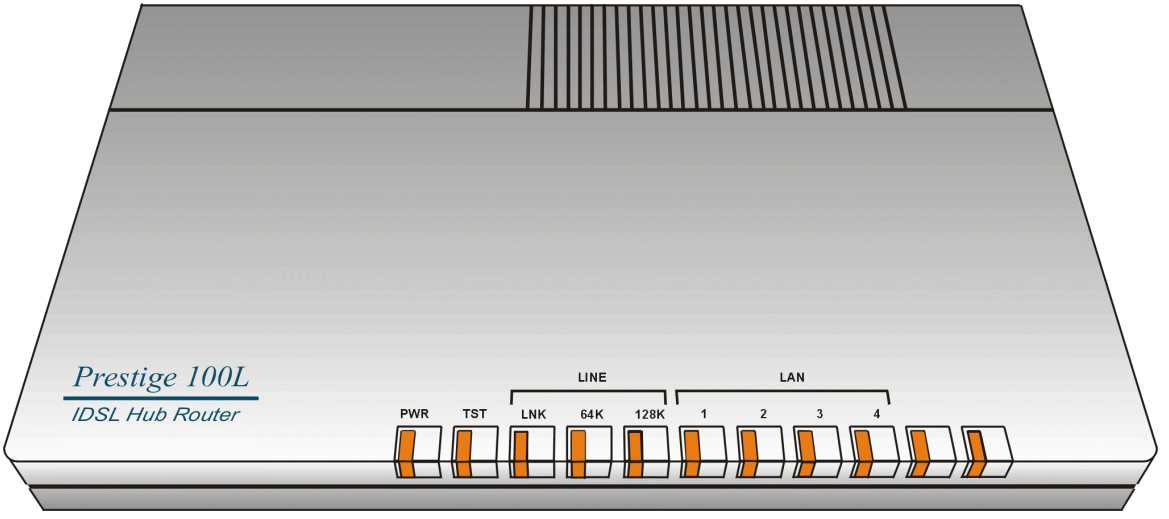

Figure 2-1 Front Panel

The following table describes the LED functions:

Table 2-1 LED Functions

FUNCTION	LEDs	ACTIVE	DESCRIPTION
Power	PWR	On	The power is on.
System Test	TST	Off	The system is not ready or malfunctioning.

FUNCTION	LEDs	ACTIVE	DESCRIPTION
		Flashing	The system is ready and functioning properly.
IDSL Line	LNK	Off	IDSL link is not ready or failed.
		On	IDSL link is functioning properly.
	64K	On	The Prestige is connected at 64K bps line speed.
	128K	On	The Prestige is connected at 128K bps line speed.
LAN	1, 2, 3, 4	Off	The Ethernet port is not connected, not ready or has failed.
		On	The Ethernet port is connected and functioning properly.
		Flashing	Sending or receiving.

2.2 Prestige 100L Rear Panel and Connections

The following figure shows the rear panel of your Prestige 100L and the connection diagram.

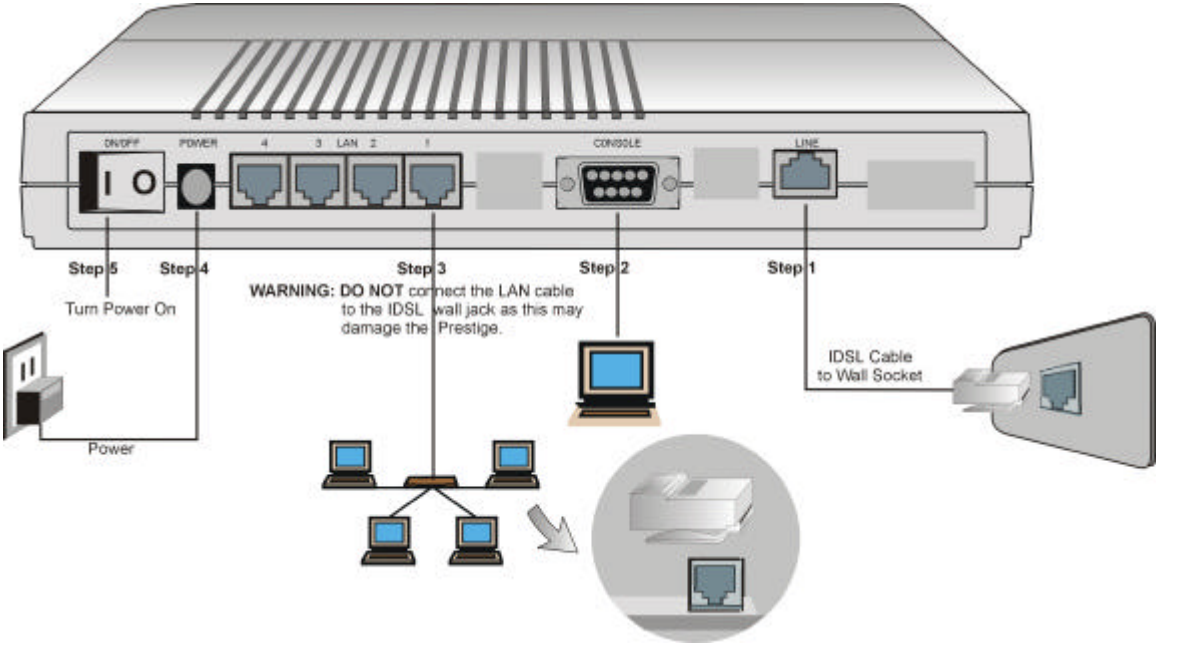

Figure 2-2 Prestige 100L Rear Panel and Connections

This section outlines how to connect your Prestige 100L to the LAN and the IDSL line. Refer to the above diagram to identify all of the ports on your device when you attempt to make the various connections.

NOTE: The IDSL line and Ethernet cable are very similar to each other. It is important that you use the correct cable for each connection; otherwise, your Prestige could be damaged.

Connecting Your Computer and Your Prestige

For the initial configuration of your Prestige, use the provided RS-232C cable and communications software to configure your Prestige. After your Prestige has been successfully installed, you can modify the configuration through a console port as well as a remote telnet connection.

Step 1. Connecting an IDSL Line to Your Prestige

Plug one end of the IDSL line included in your package into the socket on the rear panel of your Prestige labeled **LINE**, and the other end into the IDSL wall jack or another Prestige.

NOTE: The IDSL jack is for IDSL line connection only. Connecting it to a regular phone line may result in damage to your Prestige.

Step 2. Connecting the RS-232C Cable to Your Prestige

One 9-25 pin adapter is included with your Prestige. To connect an RS-232C cable, connect the 9-pin end of the cable to the console port on the back panel of the Prestige. Connect the other end to the RS-232C cable connected to the serial port (COM1, COM2, or any other COM port) of your computer.

Step 3. Connecting an Ethernet Cable to Your Prestige

The Prestige is equipped with a 4-port hub for you to build a 10Base-T Local Area Network (LAN). 10Base-T networks use UTP (Unshielded Twisted Pair) cable and RJ-45 connectors that look like a bigger telephone plug with 8 pins. Two types of Ethernet cables come with the package:

- Straight through cable (white tag) — connect your computers to your Prestige.
- Crossover cable (red tag) — connect your Prestige to another 10Base-T hub.

Step 4. Connecting the Power Adapter to Your Prestige

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

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

At this point you should have connected the RS-232C cable, the ISDN phone line, the Ethernet cable, and the power supply.

Step 5. Powering On

You can now power on your Prestige.

2.3 Housing

Your Prestige's ventilated housing has clip-out legs that fit snugly into grooves, enabling compact, sturdy stacking with airflow between routers. You should not stack more than 4 routers for maximum stability.

2.4 Power Up Your Prestige

When you power on your Prestige, it performs several internal tests and also does an IDSL line initialization. After this initialization, your Prestige asks you to press the [Enter] key to continue as shown on the initial screen.

Initial Screen

```
Copyright (c) 1994 - 2000 ZyXEL Communications Corp.
ethernet address: 00:a0:c5:01:23:45
Resetting IDSL Firmware.(2) IDSL Firmware Rev : V 09E
.............................
Press ENTER to continue...
```

Figure 2-3 Initial Screen

Entering Password

The login screen appears after you press the [Enter] key, prompting you to enter the password as shown on the next screen.
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 longer than 5 minutes after you log in, your Prestige automatically logs you out and displays a blank screen. If you see a blank screen, press the [Enter] key to bring up the login screen again.

```
Enter Password: XXXX
```

Figure 2-4 Password Screen

2.5 Navigating the SMT (System Management Terminal) Interface

The SMT is the interface that you use to configure your Prestige.
Several operations that you should be familiar with before you attempt to modify the configuration are listed in the following table.

Table 2-2 Main Menu Commands

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

2.5.1 Main Menu

After you enter the password, the SMT displays the **Prestige 100L Main Menu**, as shown in the following figure.

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

                  Prestige 100L Main Menu
Getting Started             Advanced Management
  1. General Setup            21. Filter Set Configuration
  2. WAN Port Setup           22. SNMP Configuration
  3. Ethernet Setup           23. System Password
  4. Internet Access Setup    24. System Maintenance

Advanced Applications
  11. Remote Node Setup
  12. Static Routing Setup

  15. SUA Server Setup        99. Exit

                  Enter Menu Selection Number:
```

Figure 2-5 Prestige 100L Main Menu

2.5.2 System Management Terminal Interface Summary

Table 2-3 Main Menu Summary

No.	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to setup general information and enable routing of specific protocols.
2	WAN Port Setup	Use this menu to setup the IDSL.
3	Ethernet Setup	Use this menu to setup the Ethernet LAN.
4	Internet Access Setup	A quick and easy way to setup Internet connection.
11	Remote Node Setup	Use this menu to setup remote node for LAN-to-LAN connection including Internet connection. Your Prestige has only one remote node.
12	Static Routing Setup	Use this menu to setup static route for different protocols. There are four static routes for each protocol.
15	SUA Server Setup	Use this menu to specify inside servers when SUA is enabled.
21	Filter Set Configuration	Use this menu to setup filters to provide security.
22	SNMP	Use this menu to setup SNMP-related parameters.
23	System Security	Use this menu to setup security-related parameters.
24	System Maintenance	This menu provides system status, diagnostics, firmware upload, etc.
99	Exit	To exit from SMT and return to the blank (initial) screen.

2.6 Changing the System Password

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

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

```
                    Menu 23 - System Password


          Old Password= ?
          New Password= ?
          Retype to confirm= ?




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

Figure 2-6 Menu 23 – System Security

Step 2. Enter your existing password and press the [Enter] key.

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

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

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

2.6.1 Resetting the Prestige

You should already have downloaded the correct file from your nearest ZyXEL FTP server site. *See Chapter 11* for more information on how to transfer the configuration file to your Prestige.

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

Turn off the Prestige and begin a Terminal session with the current console port settings. Turn on the Prestige again. When you see the message "Press Any key to enter Debug Mode within 3 seconds", press any key to enter debug mode.

2.7 General Setup

Menu 1 – **General Setup** contains administrative and system-related information.
To enter Menu 1 and fill in the required information, follow these steps:

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

Step 2. The **Menu 1 – General Setup** screen appears, as shown below. Fill in the required fields.

```
                        Menu 1 - General Setup

            System Name= xxx
            Location=
            Contact Person's Name=




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

Figure 2-7 Menu 1 – General Setup

The fields for General Setup are as shown below. **System Name** is for identification purposes. The **Location** is used to enter the geographic location (up to 31 characters) of your Prestige, e.g., San Jose. The **Contact Person's Name** is used to enter the name (up to 30 characters) of the person in charge of your Prestige, e.g., John Doe. Both the **Location** and **Contact Person's Name** fields are optional.

Table 2-4 General Setup Menu Field

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.	P100L
Location	Enter the geographic location (up to 31 characters) of your Prestige (optional field).	San Jose
Contact Person's Name	Enter the name (up to 30 characters) of the person-in-charge of your Prestige (optional field).	John Doe

2.8 IDSL Setup

This section describes how to configure the IDSL using **Menu 2 – IDSL Setup**. From the Main Menu, enter 2 to open Menu 2.

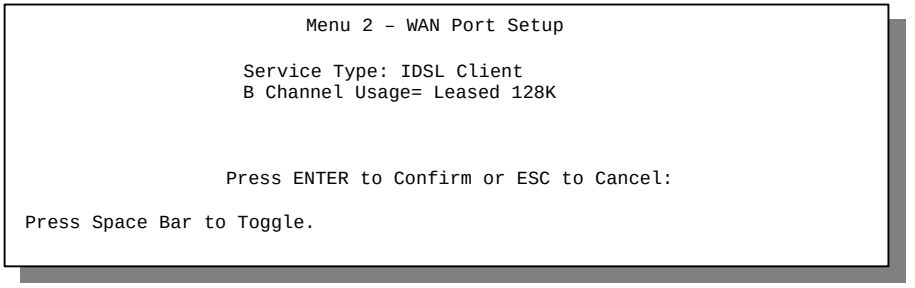

Figure 2-8 Menu 2 – IDSL Setup

The following table contains instructions on how to configure your IDSL setup.

Table 2-5 IDSL Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLES
Service Type	Since the Prestige can only act as an IDSL Client, there is only one option available: **IDSL Client**.	**IDSL Client**
B Channel Usage	There are three options available: **Leased 128K** and **Leased 64K**, which is used to decide the IDSL line's speed; or **Switch 64K** for Ascend MAX TNT IDSL-module. When the P100L is connected to the P1600 as the Client router, then this option cannot be set by the user as it is set on the P1600.	**Leased 128K / Leased 64K / Switch 64K**

2.9 Ethernet Setup

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

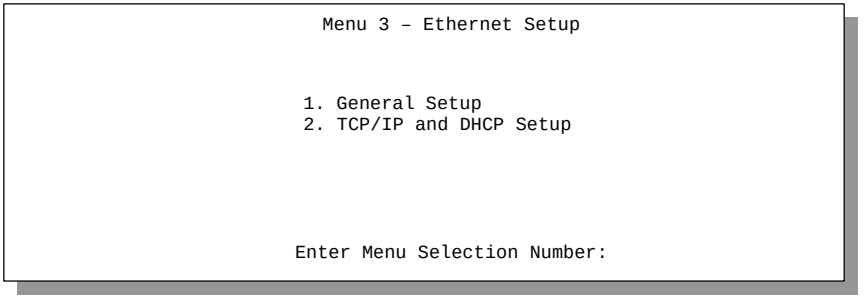

Figure 2-9 Menu 3 – Ethernet Setup

2.9.1 General Setup

This menu allows you to specify the filter sets you wish to implement on your Ethernet traffic. From Menu 3 – Ethernet Setup, enter **1** to go to Menu 3.1 – General Ethernet Setup.

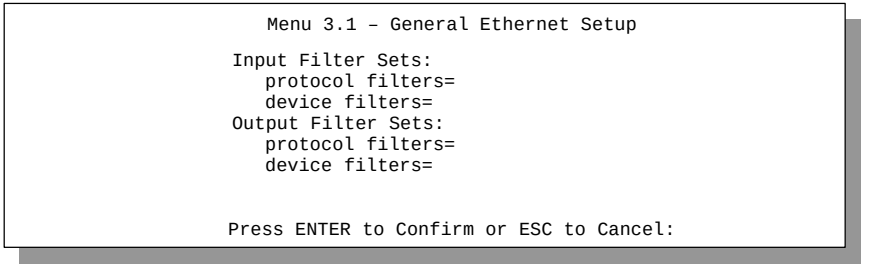

Figure 2-10 Menu 3.1 – General Ethernet Setup

NOTE: You may apply up to four filter sets separated by commas.

Input and Output Filter Sets

Filter sets are used to block certain packets to reduce traffic and to prevent a security breach. Filtering is a very involved subject, so leave these fields blank for the time being. After you have studied filtering in Chapter 6, come back and define the filter sets. Menu 3.2 is discussed in the next part of the manual. Please read on.

Chapter 3
Internet Access

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

3.1 TCP/IP and DHCP for LAN

The Prestige has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

3.1.1 Factory LAN Defaults

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

1. IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits).

2. DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

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

3.1.2 IP Address and Subnet Mask

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

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP assigns 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 feature of the Prestige. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do *not* use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first 3 numbers specify the network number while the last number identifies an individual workstation on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, e.g., 192.168.1.1 (default), for your Prestige. If you chose this then the other default settings are enabled.

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

3.1.3 Private IP Addresses

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

```
10.0.0.0      -  10.255.255.255

172.16.0.0    -  172.31.255.255

192.168.0.0   -  192.168.255.255
```

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

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

3.1.4 RIP (Routing Information Protocol) Setup

RIP 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** or **Out Only**, the Prestige broadcasts its routing table periodically. When set to **Both** or **In Only**, it incorporates the RIP information that it receives; when set to **None**, it does not send any RIP packets and ignores any RIP packets received.
The **Version** field controls the format and the broadcasting method of the RIP packets that the Prestige sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.
Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so does not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.
By default, **RIP direction** is set to **Both** and the **Version** set to **RIP-1**.

3.1.5 DHCP (Dynamic Host Configuration Protocol) Configuration

DHCP allows the individual clients (workstations) to obtain the TCP/IP configuration at start-up from a server. Unless you are instructed by your ISP, leave the DHCP at the **Server** default value. You can configure the Prestige as a DHCP server or disable it. When configured as a server, the Prestige provides the TCP/IP configuration for the clients.

IP Pool Setup

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

DNS (Domain Name System) Server Address

DNS is for mapping a domain name to its corresponding IP address and vice versa, e.g., the IP address of *www.zyxel.com* is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.
There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP does give you the DNS server addresses, enter them in the **DNS Server** fields in **DHCP Setup**. The second is to leave this field blank, i.e., 0.0.0.0, – in this case the Prestige acts as a DNS proxy.

IP Subnet Mask

A subnet mask is a 32-bit quantity that, when logically ANDed with an IP address, yields the network number. For instance, the subnet masks for Class A, B, and C without subnetting are 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively. To create more network numbers, you shift some bits from the host ID to the network ID. For instance, to partition a Class C network number 192.68.135.0 into two, you shift 1 bit from the host ID to the network ID. Thus the new subnet mask is 255.255.255.128; the first subnet have a network number of 192.68.135.0 with hosts 192.68.135.1 to 192.68.135.126 and the second subnet have a network number of 192.68.135.128 with hosts 192.68.135.129 to 192.68.135.254. It is recommended that you use the same subnet mask for all physical networks that share an IP network number. The following table lists the additional subnet mask bits in dot decimal notations. To use the following table, write down the original subnet mask and substitute the higher order “0”s with the dot decimal of the additional subnet bits. For instance, to partition your Class C network 204.247.203.0 with subnet mask 255.255.255.0 into 16 subnets (4 bits), the new subnet mask becomes 255.255.255.240.

NUMBER OF BITS	DOT DECIMAL
1	128
2	192
3	224
4	240
5	248
6	252
7	254
8	255

Example of Network Properties For LAN Servers With Fixed IP#:

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

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

To edit the TCP/IP and DHCP configuration, enter 2 to open **Menu 3.2 – TCP/IP and DHCP Ethernet Setup** as shown in the following figure.

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

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

        TCP/IP Setup:
           IP Address= 192.168.1.1
           IP Subnet Mask= 255.255.255.0
           RIP Direction= Both
             Version= RIP-1

              Press ENTER to Confirm or ESC to CANCEL:

Press Space Bar to Toggle.
```

Figure 3-2 Menu 3.2 – TCP/IP and DHCP Ethernet Setup Screen

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

Table 3-1 LAN DHCP Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
DHCP	This field enables/disables the DHCP server. If it is set to **Server**, your Prestige acts as a DHCP server. If set to **None**, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the workstation must be manually configured. When DHCP is set to **Server**, the following four items need to be set. If set to **Relay**, the Prestige acts as a surrogate DHCP server and relays requests and responses between the remote server and the clients.	**None / Relay / Server** (default)
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size, or count, of the IP address pool.	32
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	
Relay Server Address	When the DHCP is set to **Relay**, the Prestige relays the DHCP requests/responses between the PCs and the real DHCP server.	

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

Table 3-2 LAN TCP/IP Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
IP Address	Enter the IP address of your Prestige in dotted decimal notation.	192.168.1.1 (default)
IP Subnet Mask	Your Prestige automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige.	255.255.255.0
RIP Direction	Press [space bar] to select the RIP direction from **Both/In Only/Out Only/None.**	**Both** (default)
Version	Press [space bar] to select the RIP version from **RIP-1 / RIP-2B / RIP-2M.**	**RIP-1** (default)
When you have completed this menu, press the [Enter] key at the prompt [Press ENTER to Confirm . . .] to save your configuration, or press the [Esc] key at any time to cancel.		

3.3 Internet Access Setup

The following steps describe the set-up procedure to configure your Prestige for Internet access.

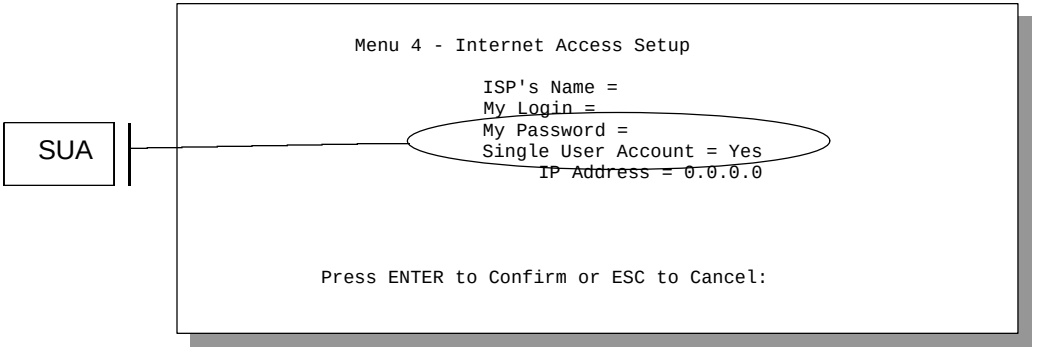

Figure 3-3 Menu 4 – Internet Access Setup

The following table describes this screen.

Table 3-3 Internet Access Setup Menu Fields

FIELD	DESCRIPTION
ISP's Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.
My Login	Enter the login name given to you by your ISP.
My Password	Enter the password associated with the login name above.
Single User Account	Please refer to the following section for a more detailed discussion on the Single User Account feature. The default value is **Yes**.
IP Address	Please refer to the following section for a more detailed discussion on setting the IP Address under a Single User Account.

3.4 Single User Account (SUA)

Typically, if there are multiple users on the LAN wanting to concurrently access the Internet, you have to lease a block of legal, or globally unique, IP addresses from the ISP.
The Single User Account (SUA) feature allows you to have the same benefits as having multiple legal addresses, but only pay for one IP address, thus saving significantly on the subscription fees. (Check with your ISP before you enable this feature). SUA supports popular Internet applications such as MS traceroute, CuSeeMe, IRC, RealAudio, VDOLive, Quake and PPTP with no extra configuration needed.
The IP address for the SUA can be either fixed or dynamically assigned by the ISP. In addition, you can designate servers, e.g., a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any server, SUA offers the additional benefit of firewall protection. If no server is defined, all incoming inquiries are filtered out by your Prestige, thus preventing intruders from probing your network. Your Prestige accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. For more information on IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT).*

3.4.1 Advantages of SUA

- SUA is an ideal, cost-effective solution for small offices to access the Internet or other remote TCP/IP networks.
- SUA supports servers to be accessible to the outside world.
- SUA can provide firewall protection if you do not specify a server. All incoming inquiries are filtered out by your Prestige.
- UDP and TCP packets can be routed. In addition, partial ICMP, including echo and traceroute, is also supported.

3.4.2 Single User Account Configuration

The steps for configuring your Prestige for Single User Account are identical to the conventional Internet access with the exception that you need to fill in two extra fields in Menu 4 – Internet Access Setup (please refer to Figure 3-3). To enable the SUA feature in Menu 4, move the cursor to the **Single User Account** field and select **Yes** (or **No** to disable SUA). Then follow the instructions on how to configure the SUA fields.

Table 3-4 Single User Account Menu Fields

FIELD	DESCRIPTION
Single User Account	Select **Yes** to enable SUA.
IP Address	If your ISP did *not* assign you a static IP address, enter [0.0.0.0] here; otherwise, enter that IP address here.
Press the [Enter] key at the message [Press ENTER to Confirm . . .] to save your configuration, or press the [Esc] key at any time to cancel.	

3.5 Multiple Servers Behind the SUA

If you wish, you can make inside servers for different services, e.g., web or FTP, visible to the outside users, even though SUA makes your whole internal network appear as a single machine to the outside world. A service is identified by the port number, e.g., web service is on port 80 and FTP on port 21.
As an example (see the following figure), if you have a web server at 192.168.1.36 and an FTP server at 192.168.1.33, then you need to specify for port 80 (web) the server at IP address 192.168.1.36 and for port 21 (FTP) another at IP address 192.168.1.33.
Please note that a server can support more than one service, e.g., a server can provide both FTP and DNS service, while another provides only web service. Also, since you need to specify the IP address of a server in the Prestige, a server must have a fixed IP address and not be a DHCP client whose IP address potentially changes each time it is powered on.
In addition to the servers for specific services, SUA 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 server is not defined, the service request is simply discarded.

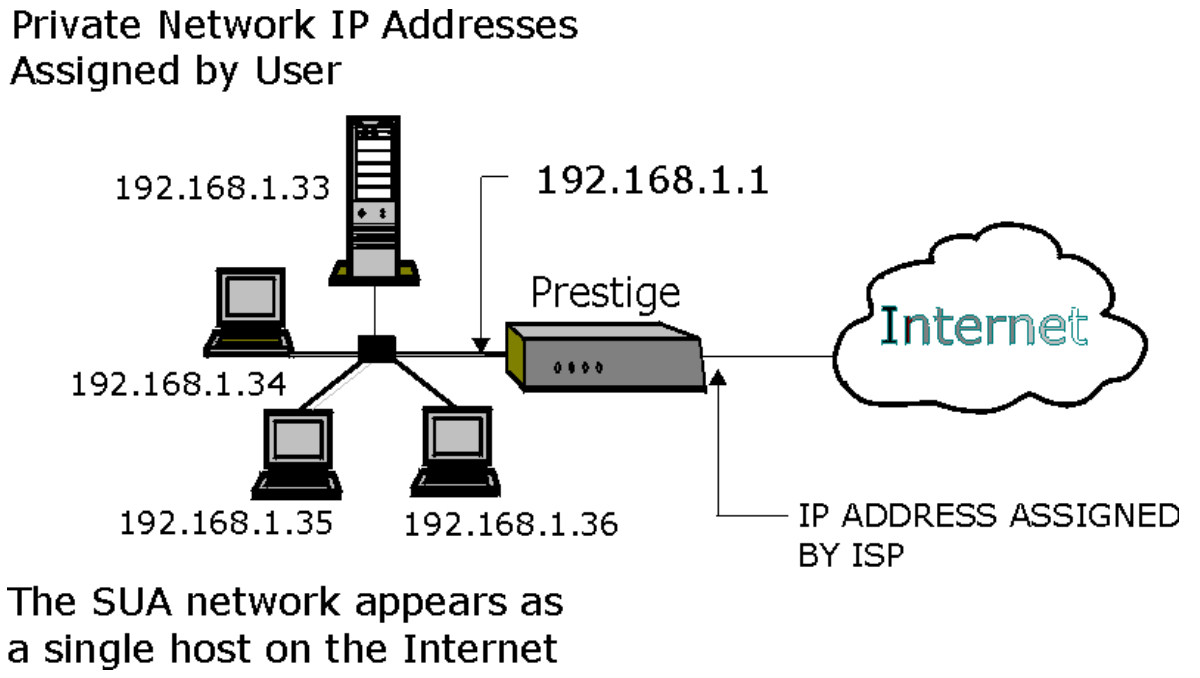

Figure 3-4 Example of a SUA Topology

To make a server visible to the outside world, specify the port number of the service and the inside IP address of the server in **Menu 15 – SUA Server Setup**.

3.5.1 Configuring a Server Behind the SUA

Do the following steps to configure a server behind SUA:

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

Step 2. Enter the service port number in the **Port #** field and the inside IP address of the server in the **IP Address** field.

Step 3. Press the [Enter] key at the "Press ENTER to confirm …" prompt to save your configuration after you define all the servers or press the [Esc] key at any time to cancel.

```
Menu 15 - Multiple Server Configuration
   Port #             IP  Address
   ------            ---------------
 1.Default           0.0.0.0
 2.21                192.168.1.33
 3.23                192.168.1.34
 4.25                192.168.1.35
 5.80                192.168.1.36
 6. 0                0.0.0.0
 7. 0                0.0.0.0
 8. 0                0.0.0.0




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

Figure 3-5 Multiple Server Configuration

The most often used port numbers are shown in the next table. Please refer to RFC 1700 for further information about port numbers.

Table 3-5 Services as Compared to Port Number

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

Part II:

ADVANCED APPLICATIONS

Advanced Applications (Chapters 4 and 5) describe the advanced applications of your Prestige, such as Remote Node Setup and IP Static routes.

Chapter 4
Remote Node Setup

This chapter shows you how to configure a remote node.

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 an IDSL connection. Note that when you use Menu 4 to set up Internet access, you are actually configuring a remote node.
Even though you can configure up to four remote nodes, the first active remote node is used to connect to the remote LAN. It is good practice to keep only one active remote node for your Prestige.
In this chapter, we discuss the parameters that are protocol independent. The protocol dependent configuration is covered in subsequent chapters. You are also shown how to configure **Menu 11.1 Remote Node Profile, Menu 11.2 – Remote Node PPP Options, Menu 11.3 – Remote Node Network Layer Options** and **Menu 11.5 – Remote Node Filter**.

4.1 Remote Node Profile

From the Main Menu, select menu option 11 to open **Menu 11.1 – Remote Node Profile**.

```
                    Menu 11.1 - Remote Node Profile

Rem Node Name=                          Edit PPP Options= No
Active =Yes                             Rem IP Addr= 0.0.0.0
                                        Edit IP= No
Incoming:
  Rem Login=                            Session Options:
  Rem Password=                           Edit Filter Sets= No

Outgoing:
  My Login=
  My Password=
  Authen= CHAP/PAP




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

Figure 4-1 Menu 11.1 – Remote Node Profile

Table 4-1 Fields in Menu 11.1

FIELD	DESCRIPTION	EXAMPLES
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.	**LAoffice**
Active	Press the [space bar] to toggle between **Yes** and **No** and activate (deactivate) the remote node.	**Yes/No**
Incoming: Rem Login	Enter the Login name that this Remote Node uses when it calls into your Prestige. The login name in this field combined with the Rem Node Password is used to authenticate the incoming calls from this node.	
Incoming: Rem Password	Enter the password used when this Remote Node calls into your Prestige.	**Standard**
Outgoing: My Login	This is a required field if Call Direction is either Both or Out. Enter the login name for your Prestige when it calls this Remote Node.	**jim**
Outgoing: My Password	This is a required field if Call Direction is either Both or Out. Enter the password for your Prestige when it calls this Remote Node.	*****
Outgoing: Authen	This field sets the authentication protocol used for outgoing calls. Your Prestige supports two authentication protocols: PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). • **PAP** sends the user name and password in plain text. • **CHAP** scrambles the password before it is sent over the wire. Generally speaking, CHAP is more secure than PAP, however, PAP is readily available on more platforms. The recommendation is to use CHAP whenever possible. Turning off the authentication is STRONGLY discouraged. Options for this field are: • **CHAP/PAP** – your Prestige tries CHAP when CHAP is requested by the Remote Node or PAP when PAP is requested by the Remote Node. • **CHAP** – use CHAP only. • **PAP** – use PAP only.	**CHAP/PAP / CHAP / PAP**
Edit PPP Options	To edit the PPP options for this Remote Node, move the cursor to this field, use [space bar] to select **Yes** and press the [Enter] key. This brings you to Menu 11.2 – Remote Node PPP Options for more information on configuring PPP options. See the section Editing PPP Options.	**No/Yes**
Rem IP Addr	This is a required field if Route is set to IP. Enter the IP address of this Remote Node.	
Edit IP	To edit the parameters of the protocols, go to this field, select **Yes** and press the [Enter] key. This brings you to Menu 11.3 – Remote Node Network Layer Options. For more information on filling out this screen, please refer to the chapter pertaining to your specific protocol.	**Yes/No**

Session Options: Edit Filter Sets	In these fields, select which filter set(s) you would like to implement to filter the incoming and outgoing traffic between this Remote Node and your Prestige. You can choose from 12 different filter sets. In addition, you can link up to 4 filter sets together for further customization (e.g., 1, 5, 9, 12). Note that spaces and "," are accepted in this field. For more information on customizing your filter sets, see Chapter 6. The default is blank, i.e., no filters defined.	**No/Yes**

4.1.1 Editing PPP Options

```
                        Menu 11.2 - Remote Node PPP Options

                        Encapsulation = Standard PPP
                        Compression = No



                    Press ENTER to Confirm or ESC to Cancel:

  Press Space Bar to Toggle.
```

Figure 4-2 Menu 11.2 Remote Node PPP Options

Table 4-2 Fields in Menu 11.2 (PPP Options)

FIELD	DESCRIPTION	EXAMPLES
Encapsulation	Select CCP (Compression Control Protocol) for the PPP or MP link. There are two options in this field: • Standard PPP – Standard PPP options is used. • CISCO PPP – CISCO PPP options is used.	**Standard PPP / CISCO PPP**
Compression	Turns on Stac Compression. The default for this field is Off.	**No/Yes**

Once you have completed Menu 11.2 – Remote Node PPP Options, press the [Enter] key at the message "Press ENTER to Confirm . . . to confirm your selections or press ESC to cancel your selections".

4.2 Editing TCP/IP Options

Move the cursor to the **Edit IP** field in **Menu 11.1**, then press the [space bar] to toggle and set the value to **Yes**. Press the [Enter] key to open **Menu 11.3 – Remote Node Network Layer Options**.
This section shows you how to configure your Prestige for TCP/IP. Depending on your particular applications, you need to configure different menus. For instance, Internet access is the most common application of TCP/IP. For this application, you should configure Menu 4. Configuration for other applications is shown in the following sections.

LAN-to-LAN Application

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

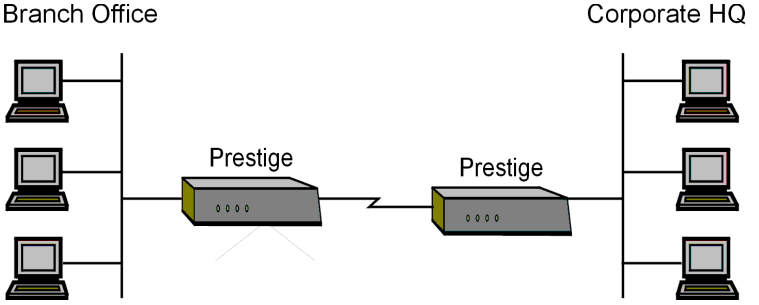

Figure 4-3 LAN-to-LAN Application

For the branch office, you need to configure a Remote Node in order to dial out to headquarters. Additionally, you may also need to configure Static Routes if some services reside beyond the immediate remote LAN.

Remote Node Setup

Follow the procedure in the preceding Chapter to fill the protocol-independent parameters in Menu 11, Remote Node Profile. For the protocol-dependent parameters, follow the instructions below.

Table 4-3 Protocol-dependent Parameters for Remote Node Setup

FIELD	DESCRIPTION	EXAMPLES
IP Address	Enter the IP address of the gateway at the remote site (in this case, headquarters). If the remote router is using a different IP address than the one entered here, your Prestige drops the call.	
Edit IP	Press [space bar] to change it to Yes and press the [Enter] key to go to Menu 11.3 – Remote Node Network Layer Options menu as shown in the following figure.	**No/Yes**

```
Menu 11.3 - Remote Node Network Layer Options

        Rem IP Addr: 0.0.0.0
        Rem Subnet Mask = 0.0.0.0
        My WAN Addr = 0.0.0.0
        Single User Account = Yes

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

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

Figure 4-4 Remote Node Network Layer Options

The next table gives you instructions about configuring remote node network layer options.

Table 4-4 Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Rem IP Addr	This shows 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 hosts on both ends of the ISDN link to have separate addresses from the LAN, and that the addresses must have the same network number. If this is the case, enter the IP address assigned to the WAN.	
Single User Account	This field set to **Yes** to enable the Single User Account (Network Address Translation) feature for this site. Use [space bar] to toggle between **Yes** and **No**.	**Yes/No**
Metric	Metric represents the “costs” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 16. In practice, 2 or 3 is usually a good number.	
Private	This parameter determines if your Prestige includes 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 is propagated to other hosts through RIP broadcasts.	**No/Yes**
RIP Direction	This parameter determines how your Prestige handles RIP (Routing	**Both/In**

FIELD	DESCRIPTION	EXAMPLE
	Information Protocol), and the default is **Both**. If set to **Both**, your Prestige broadcasts its routing table on the WAN, and incorporate RIP broadcasts by the other router into its routing table. If set to **In Only**, your Prestige does not broadcast its routing table on the WAN; if set to **Out Only**, your Prestige broadcasts its routing table but ignores any RIP broadcast packets that it receives. If set to **None**, your Prestige does not participate in any RIP exchange with other routers. Usually, you should leave this parameter at its default of **Both** and RIP propagates the routing information automatically.	**Only/Out Only/None**
Version	Press [space bar] to select the RIP version from **RIP-1, RIP-2B and RIP-2M.**	**RIP-2B/ RIP-2M/ RIP-1**
Once you have completed filling in the Remote Node Network Layer Options Menu, press the [Enter] key to return to Menu 11. Press the [Enter] key at the message [Press ENTER to Confirm . . .] to save your configuration, or press the [Esc] key at any time to cancel.		

4.3 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in **Menu 11.1**, then press [space bar] to toggle and set the value to **Yes**. Press the [Enter] key to open **Menu 11.5 – Remote Node Filter**.
Use **Menu 11.5** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige and to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by a comma, e.g., 1, 5, 9, 12, in each **filter** field. The default is no filters.
Note that spaces are accepted in this field.

```
                    Menu 11.5 - Remote Node Filter

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

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

Figure 4-3 Remote Node Filter

Chapter 5
IP Static Route Setup

This chapter shows you how to configure static routes with your Prestige.

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

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

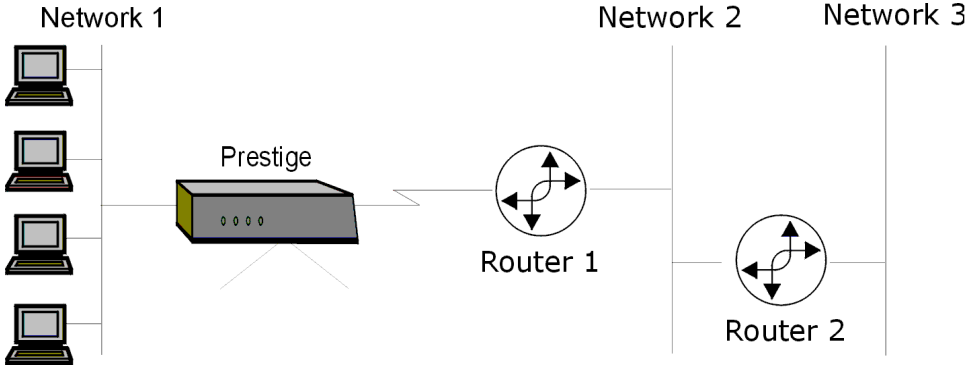

Figure 5-1 Example of an IP Static Route Setup

5.1 IP Static Route Setup

You configure IP static routes in **Menu 12.1**, by selecting one of the IP static routes as shown below. Enter 12 from the Main Menu.

```
                    Menu 12 - IP Static Route Setup


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




                                Enter selection number:
```

Figure 5-2 Menu 12 – IP Static Route Setup

Now, enter the index number of one of the static routes you want to configure.

```
                    Menu 12.1 - Edit IP Static Route


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

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

Figure 5-3 Menu 12. 1 – Edit IP Static Route

`The following table describes the IP Static Route Menu fields.

Table 5-1 IP Static Route Menu Fields

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in Menu 12.
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.
IP Subnet Mask	Enter the IP subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Prestige that forwards the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Prestige; over the 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 are usually good numbers.
Private	This parameter determines if the Prestige includes 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 is propagated to other hosts through RIP broadcasts.
Once you have completed filling in this menu, press the [Enter] key at the message [Press ENTER to Confirm . . .] to save your configuration, or press the [Esc] key to cancel.	

Part III:

ADVANCED MANAGEMENT

Chapters 6 to 11 provide information on Prestige Filtering, Simple Network Management Protocol (SNMP), System Security, System Information and Diagnosis, Transferring Files and Telnet Configuration and Capabilities.

Chapter 6
Filter Configuration

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

6.1 About Filtering

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

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

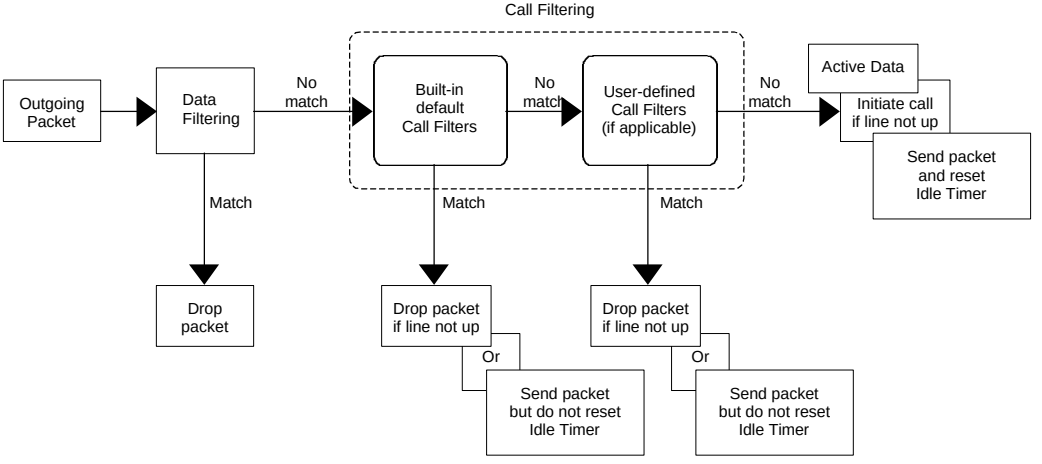

Figure 6-1 Outgoing Packet Filtering Process

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

6.1.1 The Filter Structure of the Prestige

A filter set consists of one or more filter rules. Usually, you would group related rules, e.g., all the rules for NetBIOS, into a single set and give it a descriptive name. The Prestige allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You cannot mix device filter rules and protocol filter rules within the same set. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

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

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

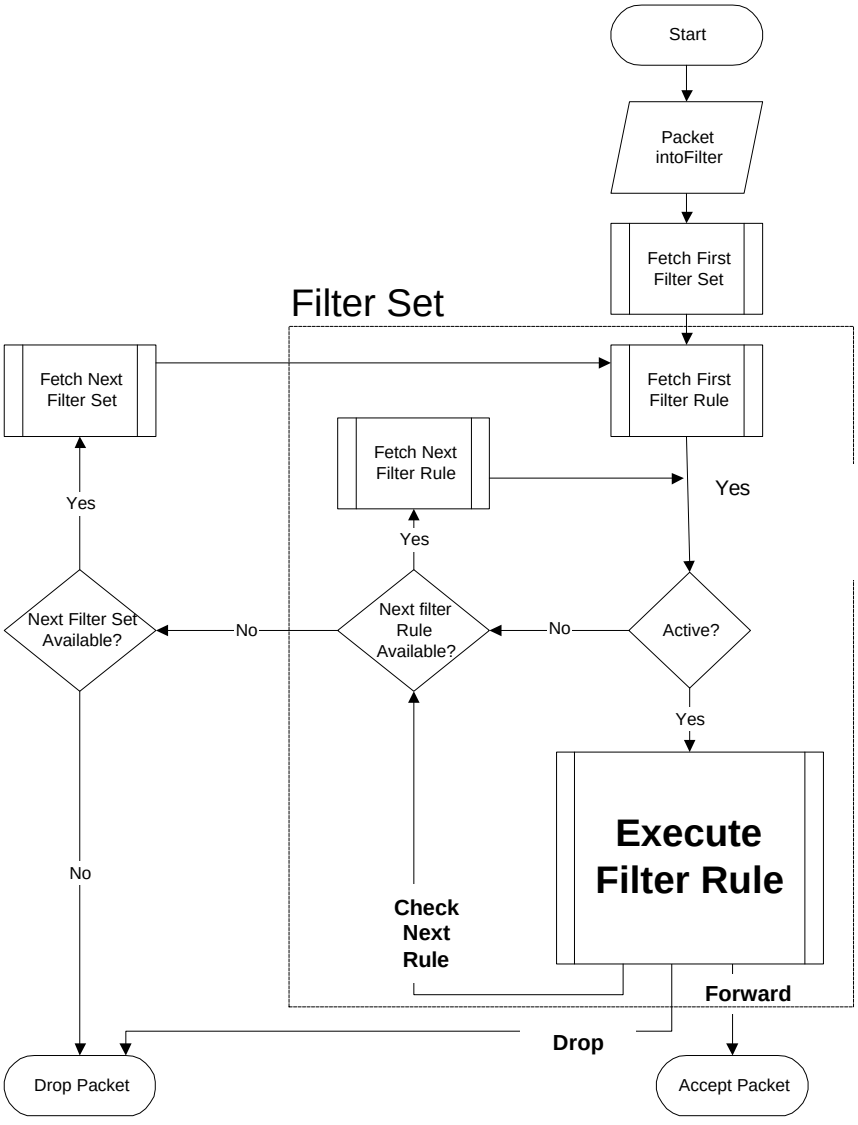

Figure 6-2 Filter Rule Process

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

6.2 Configuring a Filter Set

To configure a filter set, follow the procedure below.

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

```
                    Menu 21 - Filter Set Configuration

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

                  Enter Filter Set Number to Configure= 0

                  Edit Comments=

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

Figure 6-3 Menu 21 – Filter Set Configuration

Step 2. Select the filter set you wish to configure (nos. 1-12) and press the [Enter] key.

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

Step 4. Press the [Enter] key at the message: [Press ENTER to confirm] to open **Menu 21.1.1 – Filter Rules Summary**.

```
                    Menu 21.1 - Filter Rules Summary

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


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

Figure 6-4 Filter Rules Summary

6.2.1 Filter Rules Summary Menu

This screen shows the summary of the existing rules in the filter set. The following tables contain a brief description of the abbreviations used in the previous menus.

Table 6-1 Abbreviations Used in the Filter Rules Summary Menu

ABBREVIATIONS	DESCRIPTION	DISPLAY
#	Refers to the filter rule number (1 to 6).	
A	Shows whether the rule is active or not.	[Y] means the filter rule is active. [N] means the filter rule is inactive.
Type	Refers to the type of filter rule. This shows GEN for generic, IP for TCP/IP	[GEN] for Generic [IP] for TCP/IP
Filter Rules	The filter rule parameters are displayed here (see the following).	
M	Refers to **More**. [Y] means an action cannot yet be taken as there are more rules to check, which are concatenated with the present rule to form a rule chain. When the rule chain is complete an action can be taken. [N] means you can now specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked. If More is **Yes**, then **Action Matched** and **Action Not Matched** is **N/A.**	[Y] means there are more rules to check. [N] means there are no more rules to check.
m	Refers to **Action Matched**. [F] means to forward the packet immediately and skip checking the remaining rules.	[F] means to forward the packet. [D] means to drop the packet. [N] means check the next rule.
n	Refers to **Action Not Matched.** [F] means to forward the packet immediately and skip checking the remaining rules.	[F] means to forward the packet. [D] means to drop the packet. [N] means check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

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

Table 6-2 Abbreviations Used If Filter Type Is IP

ABBREVIATION	DESCRIPTION
Pr	Protocol
SA	Source Address
SP	Source Port number
DA	Destination Address
DP	Destination Port number

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

Table 6-3 Abbreviations Used If Filter Type Is GEN

ABBREVIATION	DESCRIPTION
Off	Offset
Len	Length

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

6.2.2 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1 - Filter Rules Summary** and press the [Enter] key to open **Menu 21.1.1** for the rule.
To speed up filtering, all rules in a filter set must be of the same class, i.e., protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filter field or vice versa, the Prestige warns you and you are not allowed to save.

6.2.3 TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, e.g., UDP and TCP, headers.
To configure a TCP/IP rule, select TCP/IP Filter Rule from the Filter Type field and press the [Enter] key to open **Menu 21.1.1.1 – TCP/IP Filter Rule**, as shown in the following figure.

```
                    Menu 21.1.1 - TCP/IP Filter Rule

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

                 Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 6-3 Menu 21.1.1 – TCP/IP Filter Rule

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

Table 6-4 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTION
Active	This field activates/deactivates the filter rule.	**Yes/No**
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. This value must be between 0 and 255.	0 to 255
IP Source Route	If **Yes**, the rule applies to packet with IP source route option; else the packet must not have source route option. The majority of IP packets do not have source route.	**Yes/No**
Destination: IP Address	Enter the destination IP Address of the packet you wish to filter. This field is disregarded if it has a 0.0.0.0 value.	IP address
Destination: IP Mask	Enter the IP mask to apply to the Destination: IP Addr.	IP address
Destination: Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is disregarded if it has a 0 value.	0 to 65535

FIELD	DESCRIPTION	OPTION
Destination: Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in Destination: Port #.	**None/Less/Greater/ Equal/Not Equal**
Source: IP Address	Enter the source IP Address of the packet you wish to filter. This field is disregarded if it has a 0.0.0.0 value.	IP Address
Source: IP Mask	Enter the IP mask to apply to the Source: IP Addr.	IP Mask
Source: Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is disregarded if it has a 0 value.	0 to 65535
Source: Port # Comp	Select the comparison to apply to the source port in the packet against the value given in Source: Port #.	**None/Less/Greater/ Equal/Not Equal**
TCP Estab	This field is applicable only when IP Protocol field is 6, TCP. If **Yes**, the rule matches only established TCP connections; or else the rule matches all TCP packets.	**Yes/No**
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken; or else the packet is disposed of according to the action fields. If More is **Yes**, then **Action Matched** and **Action Not Matched** is **N/A**.	**Yes/No**
Log	Select the logging option from the following: ● **None** – No packet is logged. ● **Action Matched** – Only packets that match the rule parameters are logged. ● **Action Not Matched** – Only packets that do not match the rule parameters are logged. ● **Both** – All packets are logged.	**None** **Action Matched** **Action Not Matched** **Both**
Action Matched	Select the action for a matching packet.	**Check Next Rule** **Forward** **Drop**
Action Not Matched	Select the action for a packet not matching the rule.	**Check Next Rule** **Forward** **Drop**
Once you have completed filling in **Menu 21.1.1.1 - TCP/IP Filter Rule**, press the [Enter] key at the message [Press Enter to Confirm] to save your configuration, or press the [Esc] key to cancel. This data is displayed on **Menu 21.1.1 - Filter Rules Summary**.		

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

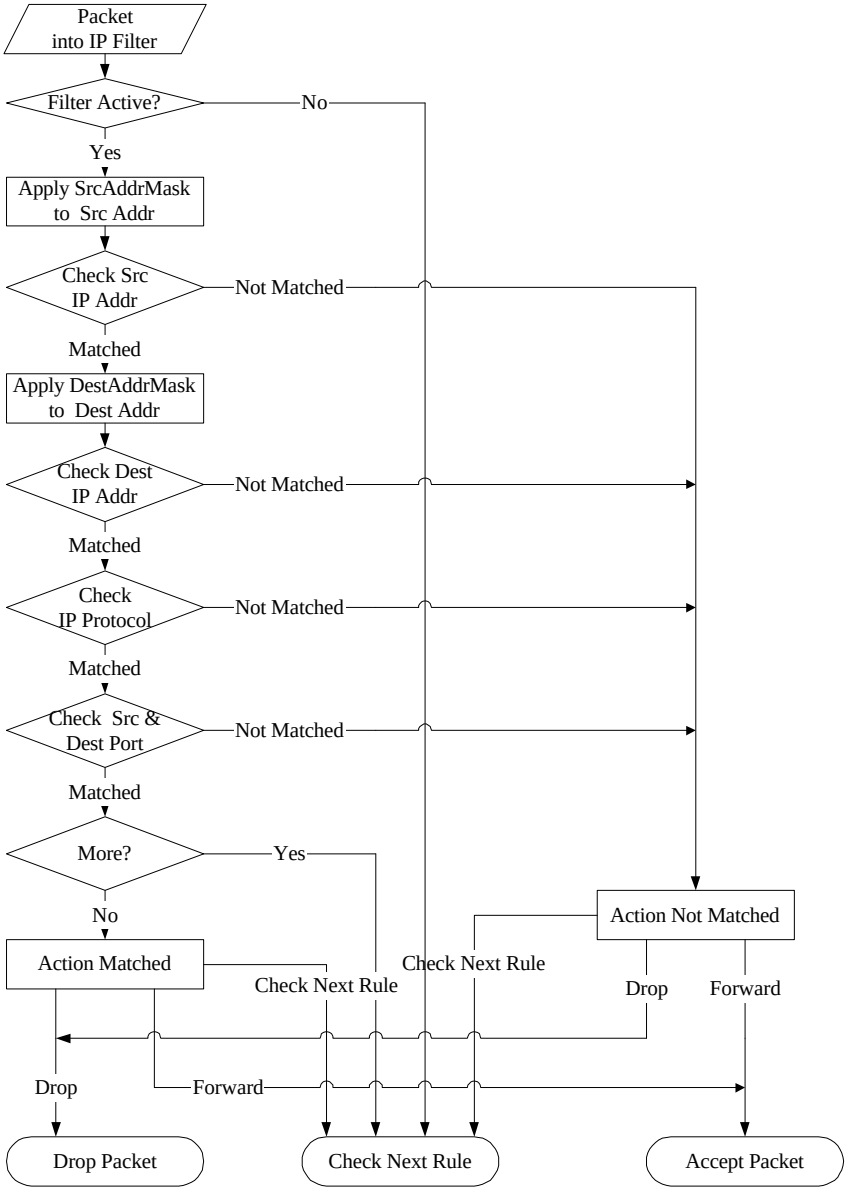

Figure 6-4 Executing an IP Filter

6.2.4 Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.
For generic rules, the Prestige treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the Offset (from 0) and the Length fields, both in bytes. The Prestige applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The Mask and Value are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field takes 8 digits, e.g., FFFFFFFF.
To configure a generic rule, select Generic Filter Rule in the Filter Type field in the **Menu 21.3.1** and press the [Enter] key to open Generic Filter Rule, as shown below.

```
                    Menu 21.3.1 - Generic Filter Rule

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



                 Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 6-5 Menu 21.3.1 – Generic Filter Rule

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

Table 6-5 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTION
Filter #	This is the filter set, filter rule coordinates, i.e., 2,3 refers to the second filter set and the third rule of that set.	
Filter Type	Use [space bar] to toggle between both types of rules. Parameters displayed below each type are different.	**Generic Filter Rule / TCP/IP Filter Rule**
Active	Select **Yes** to turn on the filter rule.	**Yes/No**
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.	Default = 0
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.	Default = 0
Mask	Enter the mask (in Hexadecimal) to apply to the data portion before comparison.	
Value	Enter the value (in Hexadecimal) to compare with the data portion.	
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** are **N/A**.	**Yes/No**
Log	Select the logging option from the following: ● **None** – No packet is logged. ● **Action Matched** – Only packets that match the rule parameters are logged. ● **Action Not Matched** – Only packets that do not match the rule parameters are logged. ● **Both** – All packets are logged.	**None** **Action Matched** **Action Not Matched** **Both**
Action Matched	Select the action for a matching packet.	**Check Next Rule** **Forward** **Drop**
Action Not Matched	Select the action for a packet not matching the rule.	**Check Next Rule** **Forward** **Drop**
Once you have completed filling in **Menu 21.4.1.1 – Generic Filter Rule**, press the [Enter] key at the message [Press Enter to Confirm] to save your configuration, or press the [Esc] key to cancel. This data is now displayed on **Menu 21.1.1 – Filter Rules Summary**.		

6.3 Example Filter

Let us look at the third default ZyXEL filter, TELNET_WAN as an example. This filter is designed to block outside users telnetting into the Prestige.

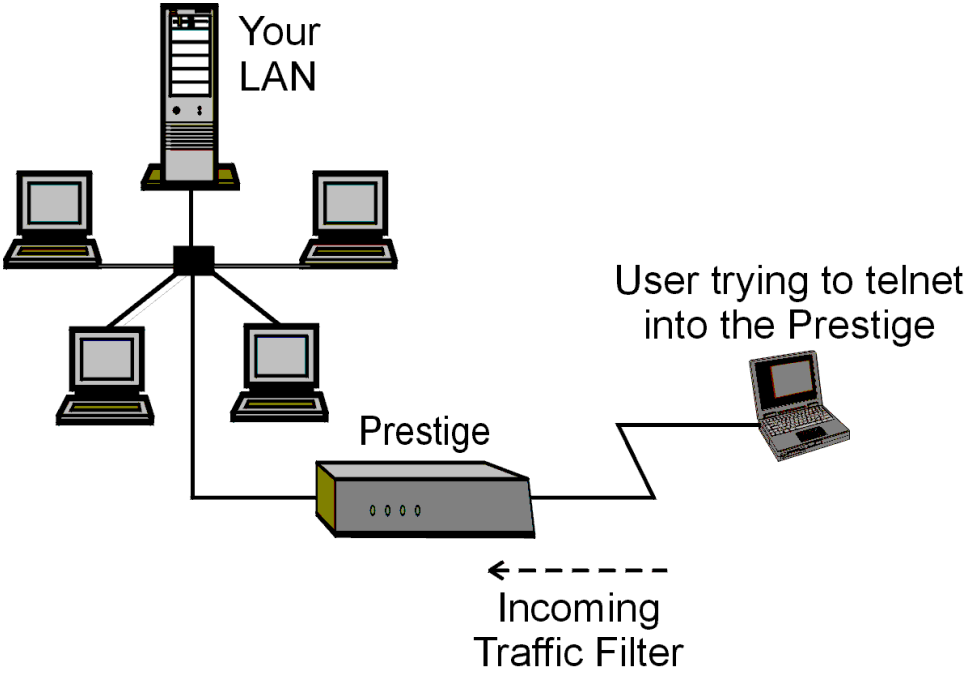

Figure 6-6 Telnet Filter Example

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

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

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

Step 4. Press the [Enter] key at the message: [Press ENTER to confirm] to open **Menu 21.1.1 – Filter Rules Summary**.

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

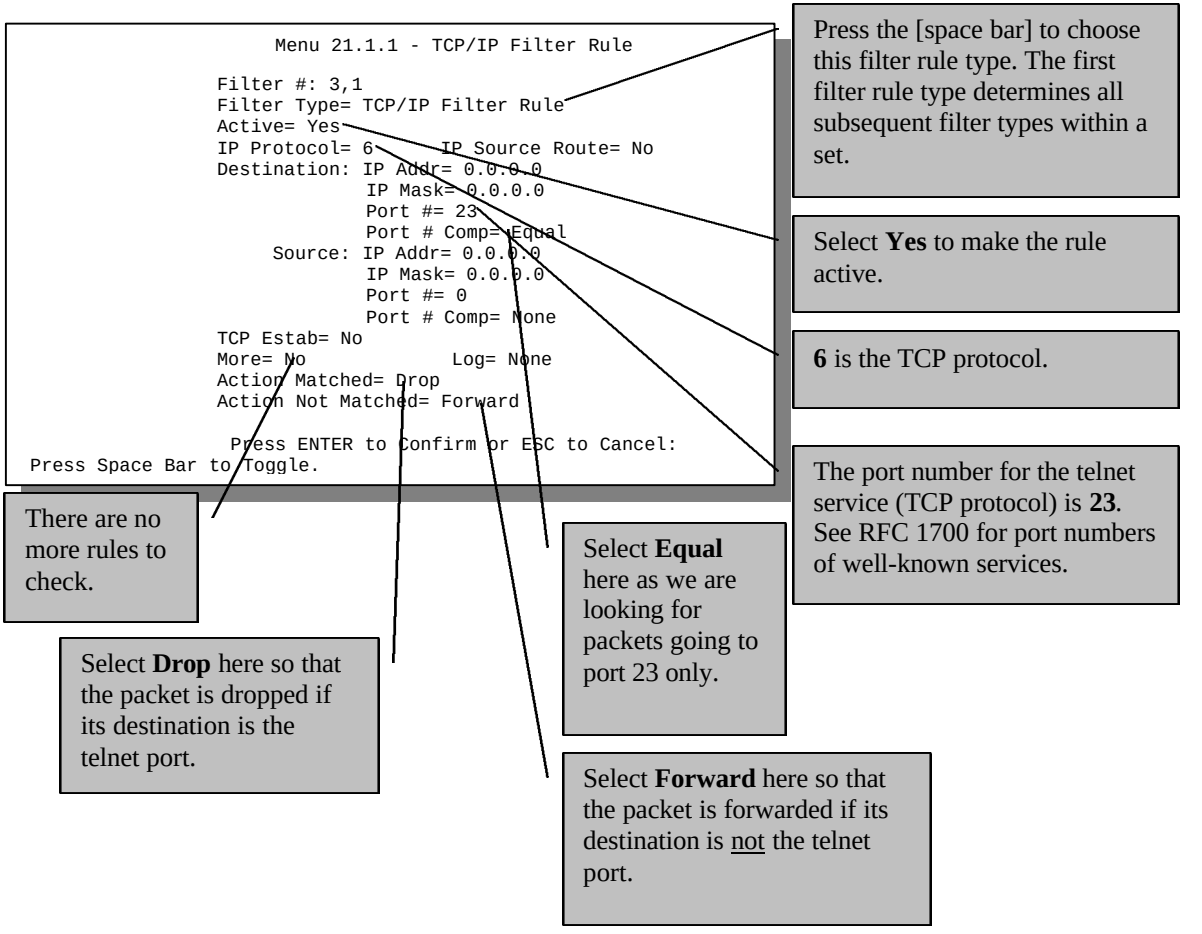

Figure 6-7 Example Filter – Menu 21.1.1

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

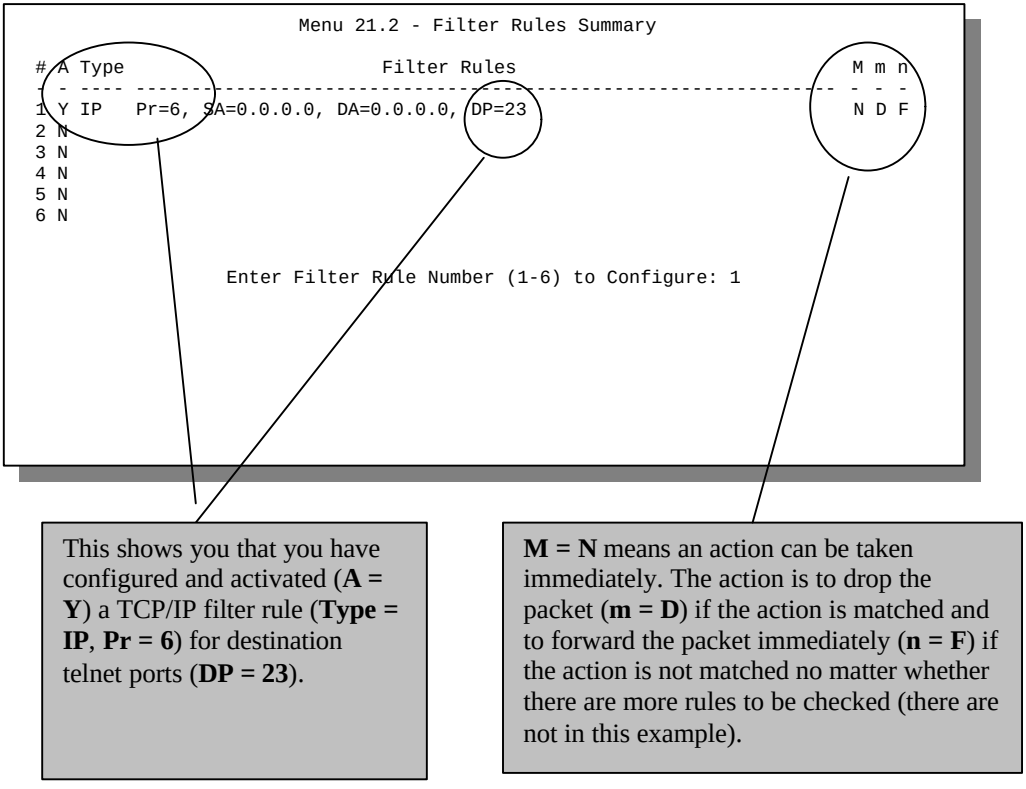

Figure 6-8 Example Filter Rules Summary – Menu 21.1.3

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

Step 1. Enter **11** from the main menu to go to Menu 11.

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

Step 3. This brings you to Menu 11.5. Apply the TELNET_WAN filter set (filter set 3) as shown in *Figure 6-10*.

6.4 Applying a Filter and Factory Defaults

This section shows you where to apply the filter(s) after you designed it (them). Three sets of factory default filter rules have been configured in Menu 21 to prevent NetBIOS traffic from triggering calls and to prevent incoming telnetting.

6.4.1 Ethernet Traffic

You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to **Menu 3.1** (shown below) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. **Input filter sets** filter incoming traffic to the Prestige and **Output filter sets** filter outgoing traffic from the Prestige. The factory default set, NetBIOS_LAN, is inserted in **protocol filters** field under **Input Filter Sets** in **Menu 3.1** to block NetBIOS traffic to the Prestige from the LAN.

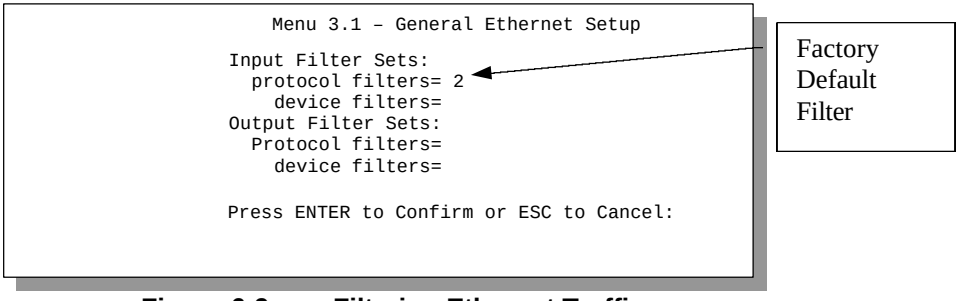

Figure 6-9 Filtering Ethernet Traffic

6.4.2 Remote Node Filters

Go to Menu 11.5 (shown below) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas. The factory default filter set, NetBIOS_WAN, is inserted in the **protocol filters** field under **Call Filter Sets** in Menu 11.5 to block local NetBIOS traffic from triggering calls to the ISP. Filter set three, Telnet_WAN, blocks telnet connections from the WAN Port to help prevent security breaches. When you cannot connect using telnet service from the WAN Port, you can disable the telnet filter in **Menu 4.1.**

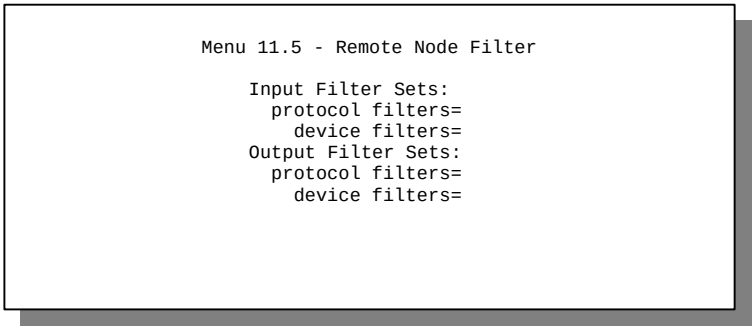

Figure 6-10 Filtering Remote Node Traffic

Chapter 7
SNMP (Simple Network Management Protocol)

This chapter takes you through SNMP Configuration Menu 22.

The SNMP is a protocol governing network management and the monitoring of network devices and their functions. The Prestige 100L supports the utilization of SNMP to regulate the communication that occurs between the manager station and the agent stations in a network. Basically, your Prestige, when connected to the LAN, acts as an agent station. In this way, the manager station on your LAN can monitor your Prestige as it would another station on the network. Keep in mind that SNMP is only available if TCP/IP is configured.

Configuring Your Prestige For SNMP Support

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

```
                    Menu 22 – SNMP Configuration

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



                    Press ENTER to Confirm or ESC to Cancel
```

Figure 7-1 Menu 22 – SNMP Configuration

1. From the Main Menu, select option 22. SNMP Configuration. This brings you to Menu 22 – SNMP Configuration.
2. You are prompted to enter the following information. Steps 3 to 7 describe the specific parameters involved in the configuration. The parameters you have to fill in are indicated in **bold** type.

Table 7-1 Fields in Menu 22 (SNMP Configuration)

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

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

Chapter 8
System Security

This chapter talks you through System Password Menu 23.

The Prestige 100L incorporates a number of security measures to prevent unauthorized access to your network. For example, your Prestige supports both PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol) in authenticating a Remote Node.
In addition, your Prestige also implements a user password to get into the SMT screen. You have three attempts to enter the correct system password. If all three attempts fail, the SMT logs out. In addition, your Prestige only supports one user in the SMT at one time.

Configuring the SMT Password

```
                    Menu 23 - System Password

                      Old Password= ?
                      New Password= ?
                      Retype to Confirm= ?



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

Figure 8-1 Menu 23 – System Password

The following steps describe a simple setup procedure for configuring the SMT password.

Step 1. From the Main Menu, select option 23. System Password. This brings you to **Menu 23 – System Password**.

Step 2. From this menu, type in your previous system password and press the [Enter] key.

Step 3. Type in your new system password and press the [Enter] key.

Step 4. Re-type your new system password for confirmation purposes and press the [Enter] key.

You now need to enter in this password when you try to get into the SMT. In addition, this password is also used when a network administrator attempts to telnet to your Prestige.

Chapter 9
Telnet Configuration and Capabilities

This chapter covers the Telnet Configuration and Capabilities of the Prestige.

9.1 About Telnet Configuration

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

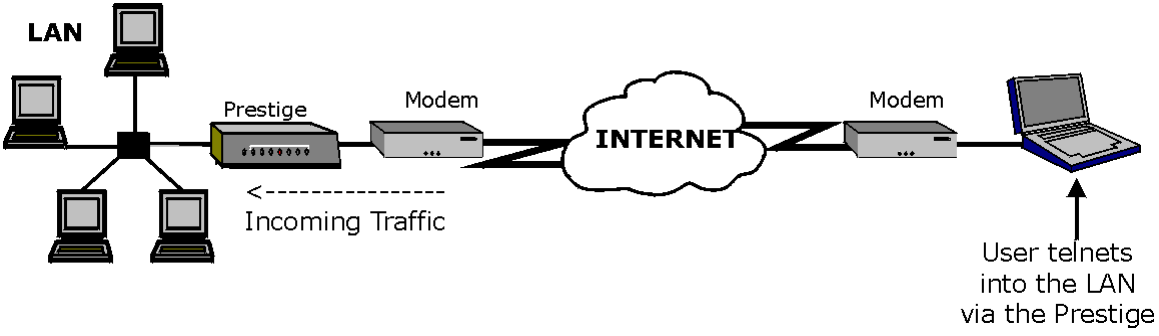

Figure 9-1 Telnet Configuration on a TCP/IP Network

9.2 Telnet Capabilities

9.2.1 Single Administrator

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

9.2.2 System Timeout

There is a system timeout of 5 minutes (300 seconds) for either the console port or telnet. 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**.

Chapter 10
System Information and Diagnosis

This chapter talks you through SMT Menu 24.

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

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

```
                    Menu 24 - System Maintenance

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



                    Enter Menu Selection Number:
```

Figure 10-1 Menu 24 – System Maintenance

10.1 System Status

The first selection, System Status, gives you information on the version of your system firmware and the status and statistics of the ports, as shown in the following figure. System Status is a tool that can be used to monitor your Prestige. Specifically, it gives you information on your system firmware version, number of packets sent and number of packets received.
To get to the System Status:

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

Step 2. In this menu, enter number 1 to open **System Maintenance – Status**.

Step 3. There are two commands in **Menu 24.1 – System Maintenance – Status**. Entering **3** resets the counters and the [Esc] key takes you back to the previous screen.

```
                    Menu 24.1 - System Maintenance – Status

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


    Total Up Time:     0:00:00    CPU load:   19.34%

    Ethernet:                     WAN
      Status: 10M/Half Duplex       IP Address: 202.132.154.179
      TX Pkts: 1538
      RX Pkts: 66734
      Collisions: 23




                                  Press Command:
                    COMMANDS:   3-Reset Counters   ESC-Exit
```

Figure 10-2 Menu 24.1 – System Maintenance – Status

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

Table 10-1 System Maintenance – Status Menu Fields

FIELD	DESCRIPTION
Chan	Shows the statistics for logical channels.
Link	Shows the Remote Node the channel is currently connected to or the status of the channel (Idle, Calling, or Answering).
Type	Shows the current connecting speed (64K or 128K).
TXPkts	Shows the number of transmitted packets on this channel.
RXPkts	Shows the number of received packets on this channel.
Errors	Shows the number of error packets on this channel.
CLU (Current Line Utilization)	Shows the percentage of current bandwidth used on this channel.
ALU (Average Line Utilization)	Shows the average CLU for this channel.
Up Time	Shows the time this channel has been connected to the current Remote Node.
Total Up Time	Shows the total time this channel has been connected to the current Remote Node.
CPU Load	Specifies the percentage of CPU utilization.
Ethernet	Shows the current status of the LAN connection on your Prestige.
Status	Shows the current status of the LAN that is 10M/Half Duplex. Left hand side of the "**/**" is the speed of the Ethernet and the right hand side is the mode of the Ethernet.
TX Pkts	Shows the number of transmitted packets to LAN.
RX Pkts	Shows the number of received packets from LAN.
Collisions	Shows the number of collisions.
WAN	
IP Address	Shows the IP address of the current channel.

10.2 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 4. Enter **24** to go to **Menu 24 – System Maintenance**.

Step 5. Enter **2** to open, **Menu 24.2 – System Information and Console Port Speed**.

Step 6. 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 10-3 Menu 24.2 – System Information and Console Port Speed

10.2.1 System Information

System Information gives you information about your system as shown below. More specifically, it gives you information on your routing protocol, country code, Ethernet address, IP address, etc.

```
                Menu 24.2.1 - System Maintenance – Information

                           Name:
                           Routing: IP
                           ZyNOS F/W Version: V2.40(AI.0)b06 | 5/19/2000
                           IDSL F/W Version: V 09E
                           Country Code: 225

                           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 ENTER to Exit
```

Figure 10-4 Menu 24.2.1 System Maintenance – Information

Table 10-2 Fields in System Maintenance

FIELD	DESCRIPTION
Name	This is the Prestige's system name.
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the current version of the RAS software.
IDSL F/W Version	Refers to the version of the current IDSL firmware.
Country Code	Refers to the one byte country code value (in decimal notation).
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) address of your Prestige.
IP Address	This is the IP address of the Prestige in dotted decimal notation.
IP Mask	This shows the subnet mask of the Prestige.
DHCP	This field shows the DHCP setting of the Prestige.

10.2.2 Console Port Speed

You can change the speed of the console port through **Menu 24.2.2 – Console Port Speed**. Your Prestige supports 9600 (default), 19200, 38400, 57600, and 115200 bps for the console port. Use [space bar] to select the desired speed in **Menu 24.2.2**, as shown below.

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

                  Console Port Speed: 115200




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

Figure 10-5 Menu 24.2.2 – System Maintenance – Change Console Port Speed

10.3 Log and Trace

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

10.3.1 Viewing Error Log

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

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

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

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

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

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


                 1. View Error Log
                 2. Syslog Server



                          Please enter selection
```

Figure 10-6 Menu 24.3 – System Maintenance – Log and Trace

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

```
59 Thu Jan  1 00:00:03 1970 PINI  INFO  SMT Session Begin
  60 Thu Jan  1 00:05:11 1970 PINI  INFO  SMT Session End
  61 Thu Jan  1 00:17:59 1970 PINI  INFO  SMT Session Begin
  62 Thu Jan  1 00:24:40 1970 PINI  INFO  SMT Session End
  63 Thu Jan  1 00:35:32 1970 PINI  INFO  SMT Session Begin
Clear Error Log (y/n):
```

Figure 10-7 Examples of Error and Information Messages

10.3.2 Syslog Server

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

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

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



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

Figure 10-8 Menu 24.3.2 – System Maintenance – Syslog and Accounting

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

Table 10-3 System Maintenance Menu Syslog Parameters

PARAMETER	DESCRIPTION
Syslog:	
Active	Press [space bar] to turn on (**Yes**) or off (**No**) syslog.
Syslog IP Address	Enter the IP address that you wish to send your syslog to. The address is usually written in dotted decimal notation such as a.b.c.d where a, b, c, and d are numbers between 0 and 255.
Log Facility	Press [space bar] to toggle between the 7 different Local options. The log facility allows you to log the message to different files in the server. Please refer to your UNIX manual for more details.

NOTE: Your Prestige sends two different types of syslog messages: Error Information Messages and Session Information Messages.

10.4 Diagnostic

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

```
                Menu 24.4 - System Maintenance - Diagnostic


TCP/IP                                  System
   12.  Ping Host                         21. Reboot System
                                          22. Command Mode


              Enter Menu Selection Number:

              Host IP Address= N/A
```

Figure 10-9 Menu 24.4 – System Maintenance – Diagnostic

Follow the procedure below to get to **Menu 24.4 – System Maintenance – Diagnostic.**

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

Step 2. From this menu, select option 4. Diagnostic. This opens **Menu 24.4 – System Maintenance – Diagnostic**.

Table 10-4 System Maintenance Menu Diagnostic

NUMBER	FIELD	DESCRIPTION
12	Ping Host	Enter 1 to ping any machine (with an IP address) on your LAN or WAN. Enter its IP address in the **Host IP Address=** field below.
21	Reboot System	Enter 21 to reboot the Prestige.
22	Command Mode	This option allows the user to enter the command mode. This mode allows you to diagnose and test your Prestige using a specified set of commands.
	Host IP Address	Enter the IP address of the host you want to ping.

Chapter 11
Transferring Files

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

11.1 Filename Conventions

The configuration file (sometimes called the romfile or romfile-0) contains the settings in the menus such as password, DHCP Setup defaults, TCP/IP Setup defaults, etc. The external (i.e., not on the Prestige) configuration filename is usually the router model name with a *.rom extension, e.g., P100L.rom. The RAS firmware file is the file that contains the ZyXEL Network Operating System firmware and the external firmware file is usually called the router model name with a *.bin extension, e.g., P100L.bin. Rename the configuration filename to "rom-0" and the firmware filename to "ras" when transferring files to the Prestige (i.e., the internal filenames on the Prestige). Renaming the files is not necessary when you transfer files to the Prestige using the X-Modem protocol.
The following table is a summary. Please note that the internal filename refers to the filename on the Prestige and the external filename refers to the filename not on the Prestige, i.e., on your workstation, local network or ftp site and so the name (but not the extension) varies. The AT command is the command you enter after you press "**Y**" when prompted in the SMT menu to go into debug mode. After uploading new firmware see the **ZyNOS F/W Version** field in **Menu 24.2.1** to check if you have uploaded the correct firmware version.

Table 11-1 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION	AT COMMAND
Configuration File	rom-0	*.rom	This is the router configuration filename on the Prestige. Uploading the rom-0 file replaces the entire ROM file system, including your Prestige configurations, system-related data (including the baud rate and default password), the error log and the trace log.	ATUR3
Firmware	ras	*.bin	This is the generic name for the RAS firmware on the Prestige.	ATUR

11.2 Backup Configuration

Option 5 from **Menu 24 – System Maintenance** allows you to backup the current Prestige configuration to your workstation. Backup is highly recommended once your Prestige is functioning properly. TFTP is the preferred method for backing up your current workstation configuration to your computer since TFTP 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 do not have to rename the files (*see Section 11.1).*
Please note that terms “download” and “upload” are relative to the workstation. Download means to transfer from another machine to the your workstation, while upload means from your workstation to another machine.

```
              Menu 24.5 - System Maintenance - Backup Configuration

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

Figure 11-1 Menu 24.5 – System Maintenance – Backup Configuration

11.3 Restore Configuration

Menu 24.6 – System Maintenance – **Restore Configuration** allows you to restore the configuration via the console port. Note that this function erases the current configuration before restoring to the previous back up configuration; please do not attempt to restore unless you have a backup configuration stored on disk.
TFTP is the preferred methods for restoring your current workstation configuration to your Prestige since TFTP is faster. Please note that the system reboots automatically after the file transfer is complete.

```
              Menu 24.6 - System Maintenance - Restore Configuration

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

Figure 11-2 Menu 24.6 – System Maintenance – Restore Configuration

11.4 Upload Firmware

Menu 24.7 – System Maintenance – **Upload Firmware** allows you to upgrade the firmware and the configuration file via the console port. Note that this function erases the old data before installing the new one; please do not attempt to update unless you have the new firmware at hand. There are two components in the system: the router firmware and the configuration file, as shown in the following figure.

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

     1. Upload Router Firmware
     2. Upload Router Configuration File


          Enter Menu Selection Number:
```

Figure 11-3 Menu 24.7 – System Maintenance – Upload Firmware

11.4.1 Uploading the Router Firmware

Menu 24.7.1 shows you the instructions for uploading the router firmware. Follow the procedure below to upload the file:

Step 1. Enter **y** at the prompt to go into debug mode.

Step 2. Enter **atur** after the **Enter Debug Mode** message.

Step 3. Wait for the **Starting XMODEM upload** message before activating Xmodem upload on your terminal.

Step 4. After successful firmware upload, enter **atgo** to restart the Prestige.

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

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

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

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

Figure 11-4 Menu 24.7.1 – System Maintenance – Upload Router Firmware

11.4.2 Uploading Router Configuration File

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

Menu 24.7.2 shows you the instructions for uploading the Router Configuration file. Follow the procedure below to upload the configuration file:

Step 1. Enter **`y`** at the prompt to go into debug mode.

Step 2. Enter **`atur3`** after the **`Enter Debug Mode`** message.

Step 3. Wait for the **`Starting XMODEM upload`** message before activating Xmodem upload on your terminal.

Step 4. After successful firmware upload, enter **`atgo`** to restart the Prestige.

If you replace the current configuration file with the default configuration file, i.e., P100L.rom, you loose all configurations that you had before and the speed of the console port is reset to the default of 9600 bps with 8 data bit, no parity, 1 stop bit (8n1) and no Flow Control. You need to change your serial communications software to the default before you can connect to the Prestige again. The password is reset to the default of 1234, also.

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

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

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

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

Figure 11-5 Menu 24.7.2 – System Maintenance – Upload Router Configuration File

11.5 TFTP File Transfer

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

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

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

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

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

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

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

NOTE: If you upload the firmware to the Prestige, it reboots automatically when the file transfer is completed (the SYS LED flashes).

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

11.5.1 Using the FTP Command From the DOS Prompt

Step 1. Launch the FTP client on your workstation.

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

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

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

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

Step 6. Use **`put`** to transfer files from the workstation to the Prestige, e.g., **`put p100l.bin ras`** transfers the firmware on your computer (p100l.bin) to the Prestige and renames it "ras". Similarly **`put p100l.rom rom`** transfers the configuration file on your computer (p100l.rom) to the Prestige and renames it "rom".

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

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

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

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

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

Figure 11-6 FTP Session Example

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

Table 11-2 Third Party FTP Clients

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 works only if your ISP or service administrator has enabled this option. • Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

The following is an example tftp command:

`TFTP [-i] host put p100l.bin ras`
where "**i**" specifies binary image transfer mode (use this mode when transferring binary files), "**host**" is the Prestige IP address, "**put**" transfers the file source on the workstation (p100l.bin – name of the firmware on the workstation) to the file destination on the remote host (ras – name of the firmware on the Prestige).
The following table describes some of the fields that you may see in third party TFTP clients.

Table 11-3 Third Party TFTP Clients – General Fields

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

11.6 Command Interpreter Mode

This option allows you to enter command interpreter mode, a “DOS prompt” type command interface, which allows more advanced system diagnosis and troubleshooting (beyond the scope of this guide). See the ZyXEL web site at www.zyxel.com 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.

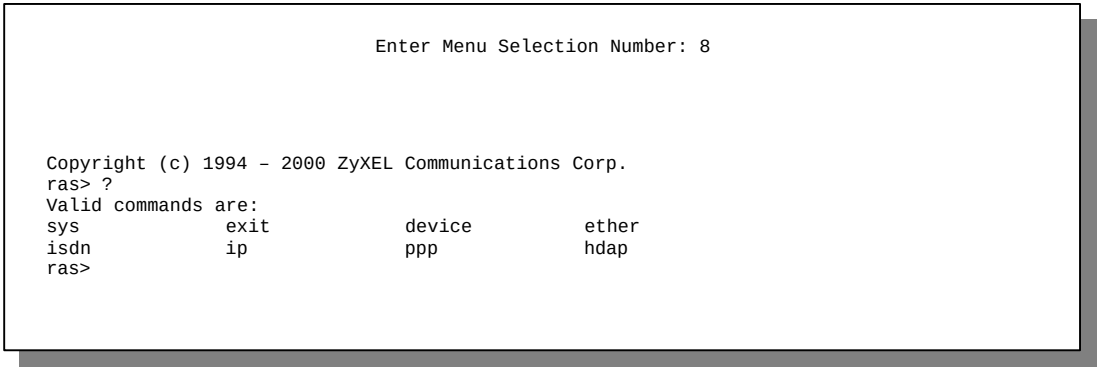

Figure 11-7 Command Mode

Part IV:

TROUBLESHOOTING

Chapter 12 provides information about solving common problems, Appendices, as well as an Index.

Chapter 12
Troubleshooting

This chapter covers the potential problems you may run into and the possible remedies. After each problem description, some instructions are provided to help you to diagnose and to solve the problem. Please see our supporting disk for further information.

12.1 Problems Starting Up the Prestige

Table 12-1 Troubleshooting Starting Up Your Prestige

PROBLEM	CORRECTIVE ACTION	
None of the LEDs are on when you power on the Prestige	Check the connection between the AC adapter and the Prestige. Check the connection between your two routers. When they are connected, the LNK and 128K LED should be on if the transfer type is 128K; and the LNK and 64K LED are on if the transfer type is 64K. Check the IDSL line if it is a single line to connect to a pair of routers. Check with the phone company if the IDSL line is connected to their company. If the error persists, you may have a hardware problem. In this case, you should contact technical support.	
Cannot access the Prestige via the console port.	1. Check to see if the Prestige is connected to your computer's serial port.	
	2. Check to see if the communications program is configured correctly. The communications software should be configured as follows:	VT100 terminal emulation.
		9600 bps is the default speed on leaving the factory. Try other speeds, e.g., 19200, 38400, 57600, 115200; in case it has been changed.
		No parity, 8 Data bits, 1 Stop bit, no Flow Control.

12.2 Problems With the LAN Interface

Table 12-2 Troubleshooting the LAN Interface

PROBLEM	CORRECTIVE ACTION
Cannot ping any workstation on the LAN	Check the four LAN 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.
	Check the physical Ethernet cable and make sure that the connections on your Prestige and the hub are secure.
	Verify that the IP address and the subnet mask are consistent between the Prestige and the workstations.

12.3 Problems with the WAN interface

Table 12-3 Troubleshooting the WAN Interface

PROBLEM	CORRECTIVE ACTION
Cannot get WAN IP from the ISP	If the ISP checks the User ID, make sure that you have entered the correct **User Name** and **Password** in **Menu 4 – Internet Access Setup**.
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 11.1**, verify your login name and password for the remote node.

Glossary

2B+D	The Basic Rate Interface (BRI) in ISDN. A single ISDN circuit is divided into two 64kbps digital channels for voice or data and one 16kbps channel for low speed data and signaling. In ISDN, 2B+D is carried on one or two pairs of wires (depending on the interface), the same wire pairs that today bring a single voice circuit into your home or office.
10BaseT	The 10-Mbps baseband Ethernet specification that uses two pairs of twisted-pair cabling (Category 3 or 5): one pair for transmitting data and the other for receiving data.
Analog	An electrical circuit that is represented by means of continuous, variable physical quantities (such as voltages and frequencies), as opposed to discrete representations (like the 0/1, off/on representation of digital circuits).
ANSA	(Alternate Network Service Agreement): Under ANSA, customers who reside in areas where the central office switch does not support ISDN can be serviced from a neighboring central office at no additional charge. From the customer's perspective, ISDN is readily available and affordable, but the customer MUST agree to migrate to the local central office if and when service becomes available. In most cases this involves a change in phone number. This agreement pertains to Bell South customers only.
Architecture	A design. The term *architecture* can refer to either hardware or software, or to a combination of hardware and software. The architecture of a system always defines its broad outlines, and may define precise mechanisms as well.
ARP	Address Resolution Protocol is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.
AT&T 5ESS	A digital central office switching system made by AT&T.
Authenticity	Proof that the information came from the person or location that reportedly sent it. One example of authenticating software is through digital signatures.
Backbone	A high-speed line or series of connections that forms a major pathway within a network.
Bandwidth	This is the capacity on a link usually measured in bits-per-second (bps).
B Channel	This is an ISDN communication channel that bears or carries voice, circuit or packet conversations. The B-channel is the fundamental component of ISDN interfaces. It carries 64,000 bits per seconds in either direction.
Bit	(Binary Digit) – A single digit number in base-2, in other words, either a one or a zero. The smallest unit of computerized data.
BRI	(Basic Rate Interface): The most common kind of ISDN interface available in the US. BRI contains two B channels, each with 64 kbps capacity, and a single D channel (16 kbps) which is used for signaling and call progress messages.
Byte	A set of bits that represent a single character. There are 8 bits in a Byte.

CDR	Call Detail Record. This is a name used by telephone companies for call-related information.
CHAP	Challenge Handshake Authentication Protocol is an alternative protocol that avoids sending passwords over the wire by using a challenge/response technique.
Cipher Text	Text that has been scrambled or encrypted so that it cannot be read without deciphering it. See Encryption
Client	A software program that is used to contact and obtain data from a Server software program on another computer. Each Client program is designed to work with one or more specific kinds of Server programs, and each Server requires a specific kind of Client. A Web Browser is a specific kind of Client.
CO	(Central Office): a facility that serves local telephone subscribers. In the CO, subscribers' lines are joined to switching equipment that allows them to connect to each other for both local and long distance calls.
Cookie	A string of characters saved by a web browser on the user's hard disk. Many web pages send cookies to track specific user information. Cookies can be used to retain information as the user browses a web site. For example, cookies are used to 'remember' the items a shopper may have in a shopping cart.
Crossover Ethernet Cable	A cable that wires a pin to its opposite pin, for example, RX+ is wired to TX+. This cable connects two similar devices, for example, two data terminal equipment (DTE) or data communications equipment (DCE) devices.
CSU/DSU	Channel Service Unit/Data Service Unit. CSUs (channel service units) and DSUs (data service units) are actually two separate devices, but they are used in conjunction and often combined into the same box. The devices are part of the hardware you need to connect computer equipment to digital transmission lines. The Channel Service Unit device connects with the digital communication line and provides a termination for the digital signal. The Data Service Unit device, sometimes called a digital service unit, is the hardware component you need to transmit digital data over the hardware channel. The device converts signals from bridges, routers, and multiplexors into the bipolar digital signals used by the digital lines. Multiplexors mix voice signals and data on the same line.
DCE	Data Communications Equipment is typically a modem or other type of communication device. The DCE sits between the DTE (data terminal equipment) and a transmission circuit such as a phone line.
D-Channel	This is an ISDN communication channel used for sending information between the ISDN equipment and the ISDN central office switch. The D-channel can also carry "user" packet data at rates up to 9.6 Kilobits.
Decryption	The act of restoring an encrypted file to its original state.
Denial of Service	Act of preventing customers, users, clients or other machines from accessing data on a computer. This is usually accomplished by interrupting or overwhelming the computer with bad or excessive information requests.
DHCP	Dynamic Host Configuration Protocol automatically assigns IP addresses to clients when they log on. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses for a period of time

	which means that addresses are made available to assign to other systems.
Digital	The use of a binary code to represent information, such as 0/1, or on/off.
Digital Signature	Digital code that authenticates whomever signed the document or software. Software, messages, Email, and other electronic documents can be signed electronically so that they cannot be altered by anyone else. If someone alters a signed document, the signature is no longer valid. Digital signatures are created when someone generates a hash from a message, then encrypts and sends both the hash and the message to the intended recipient. The recipient decrypts the hash and original message, makes a new hash on the message itself, and compares the new hash with the old one. If the hashes are the same, the recipient knows that the message has not been changed. Also see Public-key encryption.
DMS	The name of digital central office switches from Northern Telecom. Model numbers start with BCS.
DNS	Domain Name System. A database of domain names and their IP addresses. DNS is the primary naming system for many distributed networks, including the Internet.
Domain Name	The unique name that identifies an Internet site. Domain Names always have 2 or more parts, separated by dots. The part on the left is the most specific, and the part on the right is the most general.
DRAM	Dynamic RAM that stores information in capacitors that must be refreshed periodically.
DSL	Digital Subscriber Line technologies enhances the data capacity of the existing twisted-pair wire that runs between the local telephone company switching offices and most homes and offices. There are actually seven types of DSL service, ranging in speeds from 16 Kbits/sec to 52 Mbits/sec. The services are either symmetrical (traffic flows at the same speed in both directions), or asymmetrical (the downstream capacity is higher than the upstream capacity). DSL connections are point-to-point dedicated circuits, meaning that they are always connected. There is no dial-up. There is also no switching, which means that the line is a direct connection into the carrier's frame relay, ATM (Asynchronous Transfer Mode), or Internet-connect system.
DSLAM	A Digital Subscriber Line Access Multiplexer (DSLAM) is a network device, usually at a telephone company central office, that receives signals from multiple customer Digital Subscriber Line connections and puts the signals on a high-speed backbone line using multiplexing techniques. Depending on the product, DSLAM multiplexers connect DSL lines with some combination of asynchronous transfer mode ATM, frame relay, or IP networks.
DTE	Originally, the DTE (data terminal equipment) meant a dumb terminal or printer, but today it is a computer, or a bridge or router that interconnects local area networks.
EMI	ElectroMagnetic Interference. The interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.
Encryption	The act of substituting numbers and characters in a file so that the file is unreadable until it is decrypted. Encryption is usually done using a mathematical formula that determines how the file is decrypted.

Ethernet	A very common method of networking computers in a LAN. There are a number of adaptations to the IEEE 802.3 Ethernet standard, including adaptations with data rates of 10 Mbits/sec and 100 Mbits/sec over coaxial cable, twisted-pair cable, and fiber-optic cable. The latest version of Ethernet, Gigabit Ethernet, has a data rate of 1 Gbit/sec.
Events	These are network activities. Some activities are direct attacks on your system, while others might be depending on the circumstances. Therefore, any activity, regardless of severity is called an event. An event may or may not be a direct attack on your system.
FAQ	(Frequently Asked Questions) – FAQs are documents that list and answer the most common questions on a particular subject.
FCC	The FCC (Federal Communications Commission) is in charge of allocating the electromagnetic spectrum and thus the bandwidth of various communication systems.
Flash Memory	The nonvolatile storage that can be electrically erased and reprogrammed so that data can be stored, booted, and rewritten as necessary.
Foreign Exchange	If your local central office is not scheduled to have ISDN for a while, it may be possible to obtain ISDN service from a nearby central office. This is called Foreign Exchange. There are additional charges associated with this type of service.
FTP	File Transfer Protocol is an Internet file transfer service that operates on the Internet and over TCP/IP networks. FTP is basically a client/server protocol in which a system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. FTP is popular on the Internet because it allows for speedy transfer of large files between two systems.
Gateway	A gateway is a computer system or other device that acts as a translator between two systems that do not use the same communication protocols, data formatting structures, languages, and/or architecture.
HDLC	HDLC (High-level Data Link Control) is a bit-oriented (the data is monitored bit by bit), link layer protocol for the transmission of data over synchronous networks.
Host	Any computer on a network that is a repository for services available to other computers on the network. It is quite common to have one host machine provide several services, such as WWW and USENET.
HTTP	Hyper Text Transfer Protocol. The most common protocol used on the Internet. HTTP is the primary protocol used for web sites and web browsers. It is also prone to certain kinds of attacks.
IANA	Internet Assigned Number Authority acts as the clearinghouse to assign and coordinate the use of numerous Internet protocol parameters such as Internet addresses, domain names, protocol numbers, and more. The IANA Web site is at http://www.isi.edu/iana.
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol

	(IP) datagrams, but the messages are processed by the TCP/IP software and are not directly apparent to the application user.
IDSL	IDSL is a technical innovation from Ascend and the first of a series of DSL product offerings from Ascend. It stands for ISDN Digital Subscriber Line (IDSL). IDSL uses the 2B1Q line coding standard for ISDN BRI circuits. Used for data-only applications, IDSL operates at 128 Kbps for up to 18,000 feet.
Inside Wiring	Wiring that is done from the point of demarcation to the jack in the wall where the line terminates.
internet	(Lower case i) Any time you connect 2 or more networks together, you have an internet.
Internet	(Upper case I) The vast collection of inter-connected networks that all use the TCP/IP protocols and that evolved from the ARPANET of the late 60's and early 70's.
Intranet	A private network inside a company or organization that uses the same kinds of software that you would find on the public Internet, but that is only for internal use.
IP	Internet Protocol. The IP (currently IP version 4, or IPv4), is the underlying protocol for routing packets on the Internet and other TCP/IP-based networks.
IPCP (PPP)	IP Control Protocol allows changes to IP parameters such as the IP address.
IPX	Internetwork Packet eXchange The native NetWare internetworking protocol is IPX (Internetwork Packet Exchange). Like IP (Internet Protocol), IPX is an internetworking protocol that provides datagram services.
IRC	Internet Relay Chat. IRC was developed in the late 1980s as a way for multiple users on a system to "chat" over the network. Today IRC is a very popular way to "talk" in real time with other people on the Internet. However, IRC is also one avenue hackers use to get information from you about your system and your company. Moreover, IRC sessions are prone to numerous attacks that while not dangerous can cause your system to crash.
ISP	Internet Service Providers provide connections into the Internet for home users and businesses. There are local, regional, national, and global ISPs. You can think of local ISPs as the gatekeepers into the Internet.
Jack Type	Different types of jacks (RJ11, RJ45, or RJ48) can be used for an ISDN line. The RJ11 is the most common in the world and is most often used for analog phones, modems, and fax machines. RJ48 and RJ45 are essentially the same, as they both have the same 8-pin configuration. An RJ11 jack can fit into an RJ45/RJ48 connector, however, an RJ45/RJ48 cannot fit into an RJ11 connector.
LAN	Local Area Network is a shared communication system to which many computers are attached. A LAN, as its name implies, is limited to a local area. This has to do more with the electrical characteristics of the medium than the fact that many early LANs were designed for departments, although the latter accurately describes a LAN as well. LANs have different topologies, the most common being the linear bus and the star configuration.

LATA	(Local Access and Transport Area): A geographic territory used primarily by local telephone companies to determine charges for intrastate calls. As a result of the Bell divestiture, switched calls that both begin and end at points within the LATA (intraLATA) are generally the sole responsibility of the local telephone company, while calls that cross outside the LATA (interLATA) are passed on to an Inter eXchange Carrier (IXC).
LEC	(Local Exchange Carrier): The local phone companies - either a Regional Bell Operating Company (RBOC) or an independent phone company (e.g. GTE) - that provide local transmission services.
Linux	A version of the UNIX operating system designed to run on IBM Compatible computers.
Logic Bomb	A virus that only activates itself when certain conditions are met. Logic bombs usually damage files or cause other serious problems when they are activated.
Loop Qualification	This is a test done by the phone company to make sure the customer is within the maximum distance of 18,000 feet from the central office that services that customer. Note however that ISDN service "could" be available at a longer distance than that with a mid-span repeater.
MAC	On a local area network (LAN) or other network, the MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it is the same as your Ethernet address.) The MAC layer frames data for transmission over the network, then passes the frame to the physical layer interface where it is transmitted as a stream of bits.
Master/Slave	Refers to the architecture in which one device (the master) controls one or more other devices (the slaves).
Mid Span Repeater	A device that amplifies the signal coming or going to the central office. This device is necessary for ISDN service if you are outside the 18,000 feet distance requirement from the central office.
Name Resolution	The allocation of an IP address to a host name. See DNS.
NAT	Network Address Translation is the translation of an Internet Protocol address used within one network to a different IP address known within another network – see also SUA.
NDIS	Network Driver Interface Specification is a Windows specification for how communication protocol programs (such as TCP/IP) and network device drivers should communicate with each other.
NetBIOS	Network Basic Input / Output System. NetBIOS is an extension of the DOS BIOS that enables a PC to connect to and communicate with a LAN.
Network	Any time you connect 2 or more computers together so that they can share resources, you have a computer network. Connect 2 or more networks together and you have an internet.
NI1	(National ISDN 1): A specification for a "standard" ISDN phone line. The goal is for National ISDN 1 to become a set of standards that every manufacturer can conform to. For example, ISDN phones that conform to the National ISDN 1 standard works, regardless of the central office the customer is connected to. NOTE: Future

	standards, denoted as NI2 and NI3, are currently being developed.
NIC	Network Interface Card. A board that provides network communication capabilities to and from a computer system. Also called an adapter.
Node	Any single computer connected to a network.
NT-1	The NT-1 (Network Termination 1) is a device that is required to connect ISDN terminal equipment to an ISDN line. The NT-1 connects to the two-wire line (twisted pair copper wiring) that your telephone company has assigned for your ISDN service. Your ISDN service does not work if the NT-1's plug is not connected to a working electrical outlet.
Open Architecture	Allows the system to be connected easily to devices and programs made by other manufacturers. Open architectures use off-the-shelf components and conform to approved drafts. A system with a *closed architecture,* on the other hand, is one whose design is proprietary making it difficult to connect the system to other systems.
Packet Filter	A filter that scans packets and decides whether to let them through.
PAP	Password Authentication Protocol (PAP) is a security protocol that requires users to enter a password before accessing a secure system. The user's name and password are sent over the wire to a server, where they are compared with a database of user account names and passwords. This technique is vulnerable to wiretapping (eavesdropping) because the password can be captured and used by someone to log onto the system.
Password Cracker	A program that uses a dictionary of words, phrases, names, etc. to guess a password.
Password Encryption	A system of encrypting electronic files using a single key or password. Anyone who knows the password can decrypt the file.
Password Shadowing	The storage of a user's username and password in a network administrator database.
PBX	Private Branch eXchange is a small version of the phone company's larger central switching office. A PBX is a private telephone switch. It is connected to groups of lines from one or more central offices and to all of the telephones at the location served by the PBX.
Ping Attack	An attack that slows down the network until it is unusable. The attacker sends a "ping" command to the network repeatedly to slow it down. See also Denial of Service.
Pirate	Someone who steals or distributes software without paying the legitimate owner for it. This category of computer criminal includes several different types of illegal activities. Making copies of software for others to use. Distributing pirated software over the Internet or a Bulletin Board System. Receiving or downloading illegal copies of software in any form.
Pirated Software	Software that has been illegally copied, or that is being used in violation of the software's licensing agreement. Pirated software is often distributed through pirate bulletin boards or on the Internet. In the internet underground it is known as Warez.
Plain Text	The opposite of Cipher Text, Plain Text is readable by anyone.
Point of Demarcation	The physical point where the phone company ends its responsibility with the wiring of the phone line.

POP	Post Office Protocol. This is a common protocol used for sending, receiving, and delivering mail messages.
Port (H/W)	An interface on a computer for connecting peripherals or devices to the computer. A printer port, for example, is an interface that is designed to have a printer connected to it. Ports can be defined by specific hardware (such as a keyboard port) or through software.
Port	An Internet port refers to a number that is part of a URL, appearing after a colon (:) right after the domain name. Every service on an Internet server listens on a particular port number on that server. Most services have standard port numbers, e.g., Web servers normally listen on port 80.
POTS	Plain Old Telephone Service is the analog telephone service that runs over copper twisted-pair wires and is based on the original Bell telephone system. Twisted-pair wires connect homes and businesses to a neighborhood central office. This is called the local loop. The central office is connected to other central offices and long-distance facilities.
PPP	Point to Point Protocol. PPP encapsulates and transmits IP (Internet Protocol) datagrams over serial point-to-point links. PPP works with other protocols such as IPX (Internetwork Packet Exchange). The protocol is defined in IETF (Internet Engineering Task Force) RFC 1661 through 1663. PPP provides router-to-router, host-to-router, and host-to-host connections.
Promiscuous Packet Capture	Actively capturing packet information from a network. Most computers only collect packets specifically addressed to them. Promiscuous packet capture acquires all network traffic it can regardless of where the packets are addressed.
Protocol	A “language” for communicating on a network. Protocols are sets of standards or rules used to define, format, and transmit data across a network. There are many different protocols used on networks. For example, most web pages are transmitted using the HTTP protocol.
Proxy Server	A server that performs network operations in lieu of other systems on the network. Proxy Servers are most often used as part of a firewall to mask the identity of users inside a corporate network yet still provide access to the Internet. When a user connects to a proxy server, via a web browser or other networked application, he submits commands to the proxy server. The server then submits those same commands to the Internet, yet without revealing any information about the system that originally requested the information. Proxy servers are an ideal way to also have all users on a corporate network channel through one point for all external communications. Proxy servers can be configured to block certain kinds of connections and stop some hacks.
PSTN	Public Switched Telephone Network was put into place many years ago as a voice telephone call-switching system. The system transmits voice calls as analog signals across copper twisted cables from homes and businesses to neighborhood COs (central offices); this is often called the local loop. The PSTN is a circuit-switched system, meaning that an end-to-end private circuit is established between caller and callee.
Public Key Encryption	System of encrypting electronic files using a key pair. The key pair contains a public key used during encryption, and a corresponding private key used during decryption.

PVC	Permanent Virtual Circuit. A PVC is a logical point-to-point circuit between customer sites. PVCs are low-delay circuits because routing decisions do not need to be made along the way. Permanent means that the circuit is preprogrammed by the carrier as a path through the network. It does not need to be set up or torn down for each session.
RBOC	(Regional Bell Operating Company): There are currently seven regional telephone companies that were created by the AT& T divestiture.
RFC	An RFC (Request for Comments) is an Internet formal document or standard that is the result of committee drafting and subsequent review by interested parties. Some RFCs are informational in nature. Of those that are intended to become Internet standards, the final version of the RFC becomes the standard and no further comments or changes are permitted. Change can occur, however, through subsequent RFCs.
RIP	Routing Information Protocol is an interior or intra-domain routing protocol that uses the distance-vector routing algorithms. RIP is used on the Internet and is common in the NetWare environment as a method for exchanging routing information between routers.
Router	A device that connects two networks together. Routers monitor, direct, and filter information that passes between these networks. Because of their location, routers are a good place to install traffic or mail filters. Routers are also prone to attacks because they contain a great deal of information about a network.
SAP	In NetWare, the SAP (Service Advertising Protocol) broadcasts information about available services on the network that other network devices can listen to. A server sends out SAP messages every 60 seconds. A server also sends out SAP messages to inform other devices that it is closing down. Workstations use SAP to find services they need on the network.
Server	A computer, or a software package, that provides a specific kind of service to client software running on other computers.
Shoulder Surfing	Looking over someone's shoulder to see the numbers they dial on a phone, or the information they enter into a computer.
Slave	Any device that is controlled by another device called the master.
SNMP	System Network Management Protocol is a popular management protocol defined by the Internet community for TCP/IP networks. It is a communication protocol for collecting information from devices on the network.
SOCKS	A protocol that handles TCP traffic through proxy servers.
SON	(Service Order Number): The SON is the number issued by the local exchange carrier to confirm the order for the ISDN service. It provides a matching number for cross-referencing the order to the phone company.
SPAM	Unwanted e-mail, usually in the form of advertisements.
SPID	(Service Profile Identifier): The ISDN switch needs to have a unique identification number for each ISDN set to which it sends calls and signals.
Spoofing	To forge something, such as an IP address. IP Spoofing is a common way for hackers to hide their location and identity.

SSL (Secured Socket Layer)	Technology that allows you to send information that only the server can read. SSL allows servers and browsers to encrypt data as they communicate with each other. This makes it very difficult for third parties to understand the communications.
S/T-interface	A 4-wire ISDN circuit. The S/T interface is the part of a ISDN line that connects to the terminal equipment.
STP	Twisted-pair cable consists of copper-core wires surrounded by an insulator. Two wires are twisted together to form a pair, and the pair form a balanced circuit. The twisting prevents interference problems. STP (shielded twisted-pair) provides protection against external crosstalk.
Straight Through Ethernet Cable	A cable that wires a pin to its equivalent pin. This cable connects two dissimilar devices, for example, a data terminal equipment (DTE) device and a data communications equipment (DCE) device. A straight through Ethernet cable is the most common cable used.
SUA	Single User Account – The Prestige's SUA (Single User Account) feature allows multiple user Internet access for the cost of a single ISP account – see also NAT.
SVN	(Subscriber Verification Number): The SVN is the number issued by the long distance carrier to confirm the order for long distance service.
Switched 56	Digital service at 56 Kbps provided by local telephone companies and long distance carriers. Similar to ISDN, Switched 56 traffic can travel over the same physical infrastructure that supports ISDN. Switched 56, however, is an older technology with decreasing significance.
TCP	Transmission Control Protocol handles flow control and packet recovery and IP providing basic addressing and packet-forwarding services.
Telnet	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.
Tempest	Illegal interception of data from computers and video signals.
Terminal	A device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard and a display screen and some simple circuitry.
Terminal Software	Software that pretends to be (emulates) a physical terminal and allows you to type commands to a computer somewhere else.
TFTP	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP (File Transfer Protocol), but it is scaled back in functionality so that it requires fewer resources to run. TFTP uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
Twisted Pair	Two insulated wires, usually copper, twisted together and often bound into a common sheath to form multi-pair cables. In ISDN, the cables are the basic path between a subscriber's terminal or telephone and the PBX or the central office.
UDP	UDP is a connectionless transport service that dispenses with the reliability services provided by TCP. UDP gives applications a direct interface with IP and the ability to address a particular application process running on a host via a port number without

	setting up a connection session.
U-interface	A 2-wire ISDN circuit - essentially today's standard one pair telephone company local loop made of twisted-wire. The U interface is the most common ISDN interface and extends from the central office.
UNIX	A widely used operating system in large networks.
URL	(Uniform Resource Locator) URL is an object on the Internet or an intranet that resides on a host system. Objects include directories and an assortment of file types, including text files, graphics, video, and audio. A URL is the address of an object that is normally typed in the Address field of a Web browser. The URL is basically a pointer to the location of an object.
Virtual ISDN	This is an alternative way for a customer to get ISDN service. A customer can be serviced out of a nearby central office which has ISDN capabilities but not charged the extra mileage charges as they would with a foreign exchange. The phone company does not add on charges because the costs are recouped from the large volume of customers serviced out of the CO. A customer usually has to change phone numbers if the CO where they receive their POTS service becomes ISDN capable.
WAN	Wide Area Networks link geographically dispersed offices in other cities or around the globe. Just about any long-distance communication medium can serve as a WAN link, including switched and permanent telephone circuits, terrestrial radio systems, and satellite systems.
Warez	A term that describes Pirated Software on the Internet. Warez include cracked games or other programs that software pirates distribute on the Internet.
WWW	(World Wide Web) – Frequently used when referring to "The Internet", WWW has two major meanings – First, loosely used: the whole constellation of resources that can be accessed using Gopher, FTP, HTTP, telnet, USENET, WAIS and some other tools. Secondly, the universe of hypertext servers (HTTP servers).

Appendix A
Important Safety Instructions

The following safety instructions apply to the Prestige:

1. Be sure to read and follow all warning notices and instructions.
2. The maximum recommended ambient temperature for the Prestige is 40ºC (104ºF). Care must be taken to allow sufficient air circulation or space between units when the Prestige is installed inside a closed rack assembly. The operating ambient temperature of the rack environment might be greater than room temperature.
3. Installation in a rack without sufficient airflow can be unsafe.
4. Racks should safely support the combined weight of all equipment.
5. The connections and equipment that supply power to the Prestige should be capable of operating safely with the maximum power requirements of the Prestige. In case of a power overload, the supply circuits and supply wiring should not become hazardous. The input rating of the Prestige is printed on the nameplate.
6. The AC adapter must plug in to the right supply voltage, i.e., 120VAC adapter for North America and 230VAC adapter for Europe. Make sure that the supplied AC voltage is correct and stable. If the input AC voltage is over 10% or lower than the standard may cause the Prestige to malfunction.
7. Installation in restricted access areas must comply with Articles 110-16, 110-17, and 110-18 of the National Electrical Code, ANSI/NFPA 70.
8. Do not allow anything to rest on the power cord of the AC adapter, and do not locate the product where anyone can walk on the power cord.
9. Do not service the product by yourself. Opening or removing covers can expose you to dangerous high voltage points or other risks. Refer all servicing to qualified service personnel.
10. Generally, when installed after the final configuration, the product must comply with the applicable safety standards and regulatory requirements of the country in which it is installed. If necessary, consult the appropriate regulatory agencies and inspection authorities to ensure compliance.
11. A rare condition can create a voltage potential between the earth grounds of two or more buildings. If products installed in separate building are interconnected, the voltage potential can cause a hazardous condition. Consult a qualified electrical consultant to determine whether or not this phenomenon exists and, if necessary, implement corrective action before interconnecting the products. If the equipment is to be used with telecommunications circuit, take the following precautions:
    - Never install telephone wiring during a lightning storm.
    - Never install telephone jacks in wet location unless the jack is specially designed for wet location.
    - Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
    - Use caution when installing or modifying telephone lines (other than a cordless telephone) during an electrical storm. There is a remote risk of electric shock from lightning.
    - Do not use a telephone or other equipment connected to telephone lines to report a gas leak near the leak.

Appendix B
Power Adapter Specifications

AC POWER ADAPTER SPECIFICATIONS
North America
AC Power Adapter model: MW48-1601000A
Input power: AC 120Volts/60Hz/22W
Output power: DC 16Volts/1.0A
Power consumption: 4 to 9W
Plug: North American standards
Safety standards: UL; CUL (UL 1310, CSA C22.2 No.233-M91)
European Union
AC Power Adapter model: MW48-1801000UA
Input power: AC 230Volts/50Hz
Output power: DC 18Volts/1.0A
Power consumption: 4 to 9W
Plug: European Union standards
Safety standards: TUV, SEV, CE (EN 60950)
AC Power Adapter model: SLA81610-3
Input power: AC 230Volts/50Hz
Output power: DC 16Volts/1.0A
Power consumption: 4 to 9W
Plug: European Union standards
Safety standards: TUV, CE (EN 60950)
United Kingdom
AC Power Adapter model: JAA-161000F
Input power: AC 230Volts/50Hz
Output power: DC 16Volts/1.0A
Power consumption: 4 to 9 W
Plug: United Kingdom standards
Safety standards: TUV, CE (EN 60950, BS7002)

Index

1

10Base-T hub, 2-3
10Base-T network, 2-3

A

Acronyms and Abbreviations, M
Action Matched, 6-9, 6-12
Action Not Matched, 6-9, 6-12
Active, 6-8, 6-12
Ambient temperature, L
Ascend, 1-2
AT command, 11-1
Authentication protocol, 4-2
Average Line Utilization, 10-3

B

Backup, 11-2
Binary mode, 11-7
Bit-wise ANDing, 6-11

C

Call Detail Record, 10-7
Call Direction, 4-2
Call filtering, 6-1
CHAP, 1-1, 4-2, 8-1
CISCO PPP, 4-3
Client, 2-9
Client IP, 3-5
Client router, 2-9
COM port, 2-3
Command interpreter (CI), 11-5
Command Interpreter Mode, 11-8
Command Mode, 10-8
Compression, 4-3
Computer, 2-2
Connection diagram, 2-1
Console Port, 10-4, 10-5, 12-1
Contact Person's Name, 2-8
Corrective Action, 12-1
Country Code, 10-5
CPU Load, 10-3
Crossover cable, 2-3
Current Line Utilization, 10-3
Customer Support, vii

D

Data bits, 12-1
Data Compression, 1-1
Data filtering, 6-1
Destination
  IP Mask, 6-8
  Port #, 6-8
  Port # Comp, 6-9
Destination Address, 6-7
Destination IP Address, 6-8
Destination Port number, 6-7
DHCP (Dynamic Host Configuration Protocol), 1-1, 3-1, 3-3
Diagnostic, 10-8
DNS, 3-3, 3-5
Domain Name, 3-3, C
Download, 11-2

E

Echo, 3-7
Encapsulation, 4-3
Error Log, 10-6
Error packets, 10-3
Ethernet Address, 10-5
Ethernet cable, 2-2, 12-2
Ethernet Hub, 1-2
Ethernet LAN, 2-1
Ethernet Setup, 2-10, 3-4
Ethernet traffic, 2-10, 6-16
Examples of Error and Information Messages, 10-6

F

Filename Conventions, 11-1, 11-7
Filter, 4-7, 6-1
  About, 6-1
  Applying, 6-16
  Configuring, 6-4
  Example, 6-13
  Generic Filter Rule, 6-11
  Structure, 6-2
Filter #, 6-12
Filter applications, 6-1
Filter Rule Process, 6-3
Filter Rules Summary, 6-5
Filter Set, 2-10
Filter Set Configuration, 2-6
Filter Type, 6-7, 6-12
Filters
  Executing a Filter Rule, 6-2
  Logic Flow of an IP Filter, 6-9
Firmware, 1-2
Flow Control, 2-8, 12-1
Framing Rate, 2-9
Front Panel LEDs, 2-1
FTP command, 11-6

G

Gateway, 5-3
General Setup, 2-8, 2-10
Get Community, 7-2

H

Hidden Menus, 2-5
Host IP Address, 10-8
Housing, 2-3
HTTP, D, H, K

I

IANA, 3-1, 3-2
IDSL Client, 1-1
IDSL firmware, 10-5
IDSL Line, 2-1
IDSL Router, 1, ii, xvii, 1-1
IDSL Setup, 2-9
IDSL wall jack, 2-2
Initial configuration, 2-2
Initial Screen, 2-4
Initialization, 2-3
Input filter sets, 6-16
Internet access, 1-1, 1-2, 3-1
Internet Access Setup, 2-6, 3-6, 3-7, 12-2
Internet Assigned Numbers Authority. *See* IANA
IP address, 3-1, 3-6, 3-7, 4-2, 4-5, 5-3, 10-5, 11-7, 12-2
IP Network Number, 3-1
IP packets, 6-8
IP Pool, 3-3
IP Protocol, 6-8
IP Source Route, 6-8
IP Spoofing, I
IP Static Route, 5-1, 5-2, 5-3
IPX packet, 6-11

L

LAN Defaults, 3-1
LAN Setup, 2-5
LAN-to-LAN Application, 4-4
LAN-to-LAN connections, xvii, 1-1
LED functions, 2-1
Length, 6-12
Line status, 12-2
Local directory, 11-7
Location, 2-8
Log, 6-9, 6-12, 10-6
Log Facility, 10-7
Logical channels, 10-3
Login name, 3-7, 4-2
Login Type, 11-7

M

Main Menu, 2-6
Main Menu Commands, 2-4
Mask, 6-11, 6-12
Media Access Control, 10-5
Message logging, 10-6
Metric, 4-5, 5-3
Multicasting, 3-2

Multiple Server Configuration, 3-10

N

NAT, 3-7
National Electrical Code, L
NetBIOS, 6-2, 6-16
NetBIOS_LAN, 6-16
Network Address Translation, 3-1
Network Management, 1-1

O

Offset, 6-7, 6-11, 6-12
Output filter sets, 6-16

P

Packet Filtering, 6-1
Packing List Card, xviii
PAP, 1-1, 4-2, 8-1
Parity, 12-1
Password, 2-4, 2-7, 3-7, 4-2, 12-2
Phone line, 2-2
Ping, 10-8, 12-2
Port Number, 3-10
Power Adapter, 2-3
Power Adapter Specifications, M
Powering On, 2-3
PPP, 1-1, 4-2
PPP Options, 4-3
Private, 3-2, 4-5, 5-3
Private IP Addresses, 3-2
Protocol, 6-7
Protocol filters, 6-16
Protocol-dependent Parameters, 4-4

R

Racks, L
RAS F/W Version, 11-1
RAS software, 10-5
Rear Panel, 2-1, 2-2
Received packets, 10-3
Related Documentation, xviii
Relay, 3-5
Remote Access, 1-1
Remote directory, 11-7
Remote File, 11-7
Remote Node, 4-1, 8-1
Remote Node Filter, 4-7, 6-16
Remote Node Profile, 4-1
Remote Node Setup, 2-6, 4-4
Remote Nodes, xvii
Required fields, 2-5
Resetting the Prestige, 2-8
Restore Configuration, 11-2
RFC 1466, Guidelines for Management of IP Address Space, 3-2
RFC 1597, Address Allocation for Private Internets, 3-2
RFC 1631, The IP Network Address Translator, 3-7
RFC 1700, 3-10
RIP, 3-2, 3-6
RIP broadcasts, 4-5
RIP Direction, 4-5
RIP packets, 3-2
RIP-1, 3-2, 4-6
RIP-2, 3-2
RIP-2B, 3-2, 4-6
RIP-2M, 3-2, 4-6
RJ-45 connectors, 2-3
ROM File, 11-4
Router Firmware, 11-3
Routing protocol, 10-5
RS-232 Cable, 2-2

S

Safety Instructions, L
Serial port, 2-2, 12-1
Server, 3-3, 3-5, B, H, I
Service Type, 2-9
Set Community, 7-2
Setup, 2-1
Single Administrator, 9-1
Single User Account, 1-2, 4-5
SMT, 2-4
SMT timeout, 11-5
SNMP, 1-1, 2-6

SNMP Configuration, 7-1
Source
  IP Mask, 6-9
Source Address, 6-7
Source IP Address, 6-9
Source port, 6-9
Source Port number, 6-7
Standard PPP, 4-3
Static Routing Setup, 2-6
Stop bit, 12-1
Straight through cable, 2-3
Structure of this Manual, xvii
SUA, 3-7
  Multiple Servers, 3-8
SUA Server Setup, 2-6
SUA Topology, 3-9
Subnet mask, 3-1, 3-2, 3-3, 3-6, 4-5, 5-3, 10-5, 12-2
Syslog IP Address, 10-7
System Diagnosis, 10-1
System Information, 10-1, 10-4
System Maintenance, 2-6, 10-1, 10-2, 10-3, 10-4, 10-5, 10-6, 10-7, 10-8, 11-1, 11-3, 11-8
System Management Terminal, 1-1
System Name, 2-8, 2-9, 10-5
System Password, 8-1
System Security, 2-6, 8-1
System Status, 10-2
System Timeout, 9-1

T

TCP/IP, xvii, 3-1, 3-3, 3-4, 3-6, 4-3, 6-6, 6-7, 6-8, 6-9, 6-12, 9-1, 11-1, D, E, F, I, J
TCP/IP filter rule, 6-7
Telnet, 9-1
Telnet Configuration and Capabilities, 9-1
TELNET_WAN, 6-13
Terminal emulation, 12-1
TFTP, 11-2
TFTP File Transfer, 11-5
Third Party TFTP Clients, 11-7
Trace, 10-6
Traceroute, 3-7
Transfer Type, 11-7
Transmitted packets, 10-3
Trap
  Community, 7-2
  Destination, 7-2
Trivial File Transfer Protocol, 11-5
Troubleshooting, 12-1
  LAN Interface, 12-2
  WAN Interface, 12-2
Trusted Host, 7-2

U

UNIX, 4-5
UNIX Syslog, 10-6, 10-7
Unshielded Twisted Pair, 2-3
Up Time, 10-3
Upload, 11-2
Upload Firmware, 11-3
User ID, 12-2
User Name, 12-2

V

Value, 6-12
Version, 3-2, 4-6

W

WAN Addr, 4-5
WAN IP, 12-2
WAN Setup, 2-5
Warning notices, L
Workstations, 12-2

X

XMODEM protocol, 11-2

Z

ZyNOS, 11-1
ZyNOS F/W Version, 10-5