

Prestige 128^{Plus}

User's Guide

Version 2.20

ZyXEL

TOTAL INTERNET ACCESS SOLUTION

Prestige 128^{Plus}

ISDN Router

Copyright

Copyright © 02.08.1999 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

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

Trademarks

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

The declarations of CE marking:



The Prestige 128^{Plus} (Prestige 128+) has been approved for connection to the Public Switched Telecommunication Network using interfaces compatible with ITU-TSS recommendation I.420 (Basic Rate ISDN user access). The Prestige 128+ complies with the following directives:

1. The Council Directive 89/336/EEC of 3 May 1992 on the approximation of the laws of the member states relation to Electro Magnetic Compatibility. (EMC Directive).
2. Council Directive 91/263/EEC of 29 April 1991 on the approximation of the laws of the Member States concerning telecommunication terminal equipment. (The Telecom Terminal Equipment Directive).
3. 93/68/EEC of 22 July 1993 amending the Directives 89/336/EEC, 91/263 /EEC and 92/31/EEC. (Marking Directive).
4. The Council Directive 92/31/EEC of 28 April 1992 amending directive on the approximation of the laws of the member states relating to Electro Magnetic Compatibility

ZyXEL Limited Warranty

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

Note

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

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

Customer Support

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

METHOD	NORTH AMERICA	OUTSIDE NORTH AMERICA
E-Mail-Tech Support	support@zyxel.com	See your local distributor (check http://www.zyxel.com for a listing)
E-Mail-Sales	sales@zyxel.com	sales@zyxel.com.tw
Web Site	www.zyxel.com	www.zyxel.com
Phone	(714) 632-0882 (8:00 to 5:00 PM PST).	+886-3-5783942 Ext.266 (8:00 to 5:00 PM Taiwan local time)
Fax	(714) 632-0858	+886-3-5782439
FTP File Downloads	ftp.zyxel.com (software and ROM upgrades)	ftp.zyxel.co.at (software and ROM upgrades)
Regular Mail	ZyXEL Communications Inc., 1650 Miraloma Avenue, Placentia, CA 92807, U.S.A.	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, Taiwan 300, R.O.C.

Table of Contents

Prestige 128+	1
Table of Contents	vii
List of Figures	xiii
List of Tables	xvii
Preface	xxi
Chapter 1	1-1
Getting to Know Your Router	1-1
1.1 Prestige 128+ ISDN Bridge Router	1-1
1.2 Features of Prestige 128+	1-1
1.3 Applications for Prestige 128+	1-5
Chapter 2	2-1
Hardware Installation & Initial Setup	2-1
2.2 Prestige 128+ Rear Panel and Connections.....	2-3
2.3 Additional Installation Requirements	2-5
2.4 Power On Your Prestige	2-6
2.5 Navigating the SMT Interface.....	2-7
2.6 Changing the System Password	2-10
2.7 General Setup	2-13
2.8 European ISDN Setup Menus.....	2-15
2.9 Ethernet Setup	2-19
2.10 Protocol Dependent Ethernet Setup	2-20

Chapter 3	3-1
Internet Access	3-1
3.1 Route IP Setup	3-1
3.2 TCP/IP Parameters	3-2
3.3 TCP/IP Ethernet Setup and DHCP	3-6
3.4 Internet Access Configuration	3-9
3.5 Single User Account	3-12
3.6 Configuring Backup ISP Accounts	3-16
Chapter 4	4-1
Remote Node Configuration	4-1
4.1 Remote Node Setup	4-1
Chapter 5	5-1
Remote Node TCP/IP Configuration	5-1
5.1 LAN-to-LAN Application	5-1
Chapter 6	6-1
IPX Configuration	6-1
6.1 IPX Network Environment	6-1
6.2 Prestige in an IPX Environment	6-3
6.3 IPX Spoofing	6-4
6.4 IPX Ethernet Setup	6-5
6.5 LAN-to-LAN Application with Novell IPX	6-6
Chapter 7	7-1
Bridging Setup	7-1

7.1 Bridging in General.....	7-1
7.2 Bridge Ethernet Setup.....	7-1
7.3 Bridge Static Route Setup	7-5
Chapter 8.....	8-1
Dial-in Server Configuration	8-1
8.1 Remote Access Server.....	8-2
8.2 LAN-to-LAN Server Application.....	8-3
8.3 Default Dial-In Setup	8-4
8.4 Dial-In Users Setup	8-8
8.5 Multiple Servers behind SUA.....	8-12
Chapter 9.....	9-1
Advanced Phone Services	9-1
9.1 Getting Started	9-1
9.2 Setting Up Supplemental Phone Service.....	9-2
9.3 The Flash Key	9-2
9.4 Call Waiting	9-2
9.5 Three way calling	9-3
9.6 Call Transfer.....	9-4
9.7 Call Forwarding	9-5
Chapter 10.....	10-1
L2TP Support.....	10-1
10.1 What is L2TP?.....	10-1
10.2 Advantages of L2TP:.....	10-2

10.3	How L2TP Works.....	10-2
10.4	The Prestige and L2TP	10-4
Chapter 11	11-1
Filter Configuration	11-1
11.1	About Filtering	11-1
11.2	Configuring a Filter Set.....	11-3
11.3	Configuring a Filter Rule.....	11-7
11.4	Novell IPX Filter Rule	11-13
Chapter 12	12-1
SNMP Configuration	12-1
12.1	About SNMP	12-1
12.2	Configuring SNMP.....	12-1
Chapter 13	13-1
System Security	13-1
13.1	Changing the System Password	13-1
13.2	Using RADIUS Authentication	13-3
Chapter 14	14-1
Telnet Configuration and Capabilities	14-1
14.1	About Telnet Configuration	14-1
14.2	Telnet Under SUA.....	14-2
14.3	Telnet Capabilities	14-2
Chapter 15	15-1
System Maintenance	15-1

15.1	System Status	15-2
15.2	Log and Trace	15-6
15.3	Diagnostic.....	15-10
15.4	Backup Configuration	15-13
15.5	Restore Configuration	15-13
15.6	Software Update.....	15-13
15.7	Command Interpreter Mode	15-16
15.8	Call Control.....	15-16
Chapter 16	16-1
Troubleshooting	16-1
16.1	Problems Starting Up the Prestige	16-1
16.2	Problems With the ISDN Line	16-2
16.3	Problems with the Ethernet Connection.....	16-3
16.4	Problems Connecting to a Remote Node or ISP	16-3
16.5	Problems for Remote User to Dial-in	16-3
Setup Information Worksheet	A-1
Acronyms and Abbreviations	B-1
Index	C-1

List of Figures

Figure 1-1 Internet Access Application.....	1-5
Figure 1-2 LAN-to-LAN Connection Application.....	1-6
Figure 1-3 Telecommuting/Remote Access Server Application	1-7
Figure 2-1 Front Panel.....	2-1
Figure 2-2 Prestige 128+ Rear Panel and Connections.....	2-3
Figure 2-3 Power-On Display.....	2-6
Figure 2-4 Login Screen	2-6
Figure 2-5 SMT Main Menu.....	2-9
Figure 2-6 Menu 23 - System Security	2-10
Figure 2-7 Menu 23.1 - System Security - Change Password	2-12
Figure 2-8 Menu 1 – General Setup.....	2-13
Figure 2-9 Menu 2 – ISDN Setup.....	2-17
Figure 2-11 Loopback test	2-19
Figure 2-12 Menu 3 - Ethernet Setup	2-19
Figure 2-13 Menu 3.1 - General Ethernet Setup.....	2-20
Figure 3-1 Menu 1 – General Setup.....	3-1
Figure 3-2 Menu 3.2 – TCP/IP and DHCP Ethernet Setup.....	3-6
Figure 3-3 Menu 4 – Internet Access Setup.....	3-10
Figure 3-4 Single User Account Topology	3-12
Figure 3-5 Menu 4 – Internet Access Setup for Single User Account	3-15
Figure 4-1 Menu 11 – Remote Node Setup	4-2

Figure 4-2 Menu 11.1 Remote Node Profile	4-3
Figure 4-3 Menu 11.2 - Remote Node PPP Options.....	4-9
Figure 4-4 Menu 11.5 – Remote Node Filter	4-12
Figure 5-1 TCP/IP LAN-to-LAN Application.....	5-1
Figure 5-2 Menu 11.3- Remote Node TCP/IP Options	5-3
Figure 5-3 Sample IP Addresses for a TCPI/IP LAN-to-LAN Connection	5-4
Figure 5-4 Example of Static Routing Topology.....	5-7
Figure 5-5 Menu 12 - Static Route Setup.....	5-7
Figure 5-6 Menu 12.1 - IP Static Route Setup.....	5-8
Figure 5-7Edit IP Static Route.....	5-8
Figure 6-1 NetWare Server.....	6-2
Figure 6-2 Prestige in an IPX Environment	6-3
Figure 6-3 Menu 3.3 - Novell IPX Ethernet Setup.....	6-5
Figure 6-4 LAN-to-LAN Application with Novell IPX	6-6
Figure 6-5 Menu 11.3 - Remote Node Novell IPX Options.....	6-7
Figure 6-6 Menu 12.2 - Edit IPX Static Route	6-9
Figure 7-1 Menu 3.5 - Bridge Ethernet Setup	7-2
Figure 7-2 Menu 11.3 - Remote Node Bridging Options	7-3
Figure 7-3 Menu 12.3 - Bridge Static Route Setup	7-5
Figure 7-4 Menu 12.3.1 - Edit Bridge Static Route.....	7-5
Figure 8-1 Example of Telecommuting	8-2
Figure 8-2 Example of a LAN-to-LAN Server Application.....	8-3
Figure 8-3 Menu 13 – Default Dial-in Setup.....	8-4

Figure 8-4 Default Dial-in Filter.....	8-8
Figure 8-5 Menu 14 - Dial-in User Setup.....	8-9
Figure 8-6 Edit Dial-in User.....	8-9
Figure 8-7 Multiple Server Configuration.....	8-13
Figure 10-1 How L2TP works.....	10-2
Figure 10-2 Prestige as LNS.....	10-5
Figure 10-3 SMT Menu 11.1.....	10-6
Figure 10-4 Prestiges in Direct mode.....	10-7
Figure 10-5 Menu 10 – Tunnel Endpoint Setup.....	10-8
Figure 10-6 Menu 10.1 Tunnel Endpoint Profile.....	10-8
Figure 10-7 Prestige in Proxy mode.....	10-9
Figure 11-1 Outgoing Packet Filtering Process.....	11-2
Figure 11-2 Menu 21 - Filter Set Configuration.....	11-3
Figure 11-3 Menu 21.1 - Filter Rules Summary.....	11-4
Figure 11-4 Menu 21.1.1 - TCP/IP Filter Rule.....	11-8
Figure 11-5 Menu 21.1.2 - Generic Filter Rule.....	11-11
Figure 11-6 Menu 21.1.3 - IPX Filter Rule.....	11-13
Figure 12-1 Menu 22 - SNMP Configuration.....	12-1
Figure 13-1 Menu 23 - System Security.....	13-1
Figure 13-2 Menu 23.1 - System Security - Change Password.....	13-2
Figure 13-3 Menu 23.2 - System Security - External Server.....	13-5
Figure 14-1 Telnet Configuration on a TCP/IP Network.....	14-1
Figure 15-1 Menu 24 - System Maintenance.....	15-1

Figure 15-2 Menu 24.1 - System Maintenance – Status	15-3
Figure 15-3 LAN Packet That Triggered Last Call	15-4
Figure 15-4 System Maintenance - Information.....	15-5
Figure 15-5 Menu 24.2.2 – System Maintenance – Change Console Port Speed.....	15-6
Figure 15-6 Examples of Error and Information Messages.....	15-7
Figure 15-7 Menu 24.3.2 - System Maintenance - Syslog and Accounting	15-8
Figure 15-8 Menu 24.4 - System Maintenance - Diagnostic.....	15-10
Figure 15-9 Trace Display for a Successful Manual Call.....	15-12
Figure 15-10 Trace Display for a Failed Authentication	15-12
Figure 15-11 Menu 24.7 - System Maintenance - Upload Firmware	15-14
Figure 15-12 Boot module commands	15-15
Figure 15-13 Command mode.....	15-16
Figure 15-14 Menu 24.9 - System Maintenance - Call Control	15-17
Figure 15-15 Call Control Parameters.....	15-17
Figure 15-16 Menu 24.9.2 - Blacklist	15-19
Figure 15-17 Menu 24.9.3 - Budget Management	15-20
Figure 15-18 Call History.....	15-21

List of Tables

Table 1-1 IP subnet masks and the number of hosts allowed.....	xxv
Table 2-1 LED functions.....	2-2
Table 2-2 Main Menu Commands	2-7
Table 2-3 Main Menu Summary	2-9
Table 2-4 General Setup Menu Fields	2-14
Table 2-5 Menu 2 – ISDN Setup	2-17
Table 3-1 DHCP Ethernet Setup Menu Fields	3-7
Table 3-2 TCP/IP Ethernet Setup Menu Fields.....	3-8
Table 3-3 Internet Account Information	3-9
Table 3-4 Internet Access Setup Menu Fields.....	3-11
Table 3-5 Single User Account Menu Fields	3-15
Table 4-1 Remote Node Profile Menu Fields	4-3
Table 4-2 BTR v MTR for BOD.....	4-8
Table 4-3 Remote Node PPP Options Menu Fields	4-11
Table 5-1 TCP/IP related fields in Remote Node Profile.....	5-4
Table 5-2 TCP/IP Remote Node Configuration	5-5
Table 5-3 Edit IP Static Route Menu Fields.....	5-9
Table 6-1 Novell IPX Ethernet Setup Fields.....	6-5
Table 6-2 Remote Node Novell IPX Options	6-8
Table 6-3 Edit IPX Static Route Menu Fields.....	6-10
Table 7-1 Bridge Ethernet Setup Menu - Handle IPX Field Configuration.....	7-2

Table 7-2 Remote Node Network Layers Menu Bridge Options	7-4
Table 7-3 Bridge Static Route Menu Fields	7-6
Table 8-1 Remote Dial-in Users/Remote Nodes Comparison Chart	8-1
Table 8-2 Default Dial-in Setup Fields.....	8-5
Table 8-3 Edit Dial-in User Menu Fields	8-10
Table 8-4 Edit Dial-in User Menu Fields (continued).....	8-11
Table 8-5 Services vs. Port number.....	8-13
Table 9-1 Phone Flash Commands	9-5
Table 10-1 SMT Menu 11.1- Remote Profile L2TP fields	10-7
Table 10-2 Tunnel Endpoint Profile Fields.....	10-8
Table 11-1 Abbreviations Used in the Filter Rules Summary Menu	11-4
Table 11-2 Abbreviations Used in the Filter Rules Summary Menu (continued).....	11-5
Table 11-3 Abbreviations Used If Filter Type Is IP	11-5
Table 11-4 Abbreviations Used If Filter Type Is IPX	11-6
Table 11-5 Abbreviations Used If Filter Type Is GEN	11-6
Table 11-6 TCP/IP Filter Rule Menu Fields	11-9
Table 11-7 Generic Filter Rule Menu Fields	11-12
Table 11-8 IPX Filter Rule Menu Fields	11-14
Table 12-1 SNMP Configuration Menu Fields.....	12-2
Table 13-1 System Security - External Server Menu Fields.....	13-6
Table 15-1 System Maintenance - Status Menu Fields.....	15-3
Table 15-2 Fields in System Maintenance.....	15-5
Table 15-3 System Maintenance Menu Syslog Parameters.....	15-8

Table 15-4 System Maintenance Menu Diagnostic	15-11
Table 15-5 Call Control Parameters Fields	15-18
Table 15-6 Call History Fields	15-21
Table 16-1 Troubleshooting the Start-Up of your Prestige	16-1
Table 16-2 Troubleshooting the ISDN Line.....	16-2
Table 16-3 Troubleshooting the Ethernet Connection	16-3
Table 16-4 Troubleshooting a Connection to a Remote Node or ISP	16-3
Table 16-5 Troubleshooting for Remote Users to Dial-in.....	16-3

Preface

About Your Router

Congratulations on your purchase of the Prestige 128^{Plus} (Prestige 128+) ISDN Router.

The Prestige 128+ is a high-performance bridge/router that offers a complete solution for your WAN (Wide Area Network) applications such as Internet access, multi-protocol LAN-to-LAN connections, telecommuting and remote access over ISDN (Integrated Service Digital Network).

The Prestige 128+ supports multi-protocol routing for TCP/IP and Novell IPX, as well as transparent bridging for other protocols. Your Prestige 128+ is easy to install and to configure since you do not need to set any switches.

The Prestige Web Configurator (PWC) is a JAVA based utility designed that allows users to manage the Prestige via a Worldwide Web browser. Moreover, all functions of the Prestige 128+ are software configurable via the SMT (System Management Terminal) Interface. The SMT is a menu-driven interface that you can access from either a VT100 compatible terminal or a terminal emulation program on a PC.

About This User's Manual

This user's guide shows you how to configure and manage your router.

It is designed to guide you through the configuration of your Prestige 128+ for its various applications.

Ordering an ISDN Line

If you do not have the ISDN line installed already, we suggest that you order it from your telephone company as soon as possible to avoid the long wait commonly encountered when ordering a new line.

To order a new ISDN line, do the following:

1. Contact your local telephone company's ISDN Ordering Center to find out what type of ISDN service is available and the switch type.
2. Provide your telephone company with the line provisioning information for that switch type, which can be found in the Appendix of this manual. This insures proper operation of all of the Prestige's features with the ISDN line.
3. When the telephone company installs your ISDN line, please be sure to obtain and write down the following information for future use:
 - ISDN switch type
 - ISDN telephone number(s)

Completing the Setup Information Worksheet

Before you continue, locate the worksheet in the Appendix . This information worksheet has been provided to help you collect the necessary information needed for setup and installation in the following chapters.

Collecting General Setup Information

The Prestige requires certain system information. You can obtain all the pertinent information from your network administrator. Record this information into the worksheet as it becomes available. This worksheet will later be referred to as you configure your Prestige.

System Name - This is the name given to the Prestige for identification purposes. This name should be no more than eight alphanumeric characters. Spaces are not allowed, but '-' and '_' are accepted.

You have now collected all of the general setup information you need. Please make sure that you have entered all the values onto the worksheet before proceeding to the next section.

Collecting ISDN Phone Line Information

Once your ISDN line is installed by the telephone company, you need to use the following information to complete the worksheet and configure your Prestige. Much of this information is provided by your telephone company upon installation of the ISDN line.

Switch Type - This is the type of switch used by your telephone company. Check with your telephone company and choose the appropriate option on the worksheet.

B Channel Usage - Determine which connection is appropriate for your B channel and check the corresponding option on the worksheet. If your Prestige is the only device using the ISDN line, then configure **B Channel Usage** to **Switch/Switch** so that your Prestige will use both B channels to communicate. If your Prestige is sharing the ISDN line with other devices, then configure B Channel to **Switch/Unused**.

Telephone Number(s) - Record on the worksheet the telephone number(s) given to you by your telephone company. Some switch types only have one telephone number. The Prestige only accept digits; '-' and spaces are not allowed.

Analog Call - Check the appropriate **Analog Call** option on the worksheet for each telephone number. This information is later used to configure the Prestige in routing an incoming analog call. Set to **Phone1** or **Phone2** if you wish to route the incoming analog call for this telephone number to PHONE port number 1 or 2.

Supplemental Service Activation Keys – Sometimes called ‘buttons,’ most of the supplemental services supported by the Prestige require that an activation key be set before a feature can be used.

You have now collected all of the necessary information about your ISDN telephone line. Make sure that these values are entered into your ‘Setup Information Worksheet’ before you continue to the next section.

Collecting Ethernet Setup Information

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

Record the IP Address into the worksheet as assigned by your network administrator. Please note that every machine on an internet must have a unique IP address - do not assign an arbitrary address to any machine. If you are not sure as to which IP address to assign to the Prestige, contact your LAN administrator or refer to Chapter 4 of this guide for more details.

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

The table below lists some examples of IP subnet masks and the number of hosts that are allowed. Consult your network administrator if you are unsure of this value.

Table 1-1 IP subnet masks and the number of hosts allowed

IP Subnet Mask	Number of Host ID's	Number of Bits
255.255.255.0	254	24
255.255.255.128	126	25
255.255.255.192	62	26
255.255.255.224	30	27
255.255.255.255	1	32

Structure of this Manual

This manual is divided into five parts:

1. *Getting Started* (Chapters 1-2) is structured as a step-by-step guide to help you connect, install and setup your Prestige to operate on your network.
2. *The Internet* (Chapter 3) describes how to configure your Prestige for Internet access.
3. *Setting Up Advanced Applications* (Chapters 4-10) describes how to use your Prestige for more advanced applications such as LAN-to-LAN connectivity for TCP/IP and Novell IPX, and transparent bridging for other protocols.
4. *Management & Maintenance* (Chapters 11-15) provides information on management and maintenance facilities.
5. *Troubleshooting* (Chapter 16), provides information about solving common problems.

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

Syntax Conventions

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.

Chapter 1

Getting to Know Your Router

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

1.1 Prestige 128+ ISDN Bridge Router

The Prestige 128+ is an ISDN bridge/router. The Prestige is ideal for everything from Internet browsing to receiving calls from remote dial-in users to making LAN-to-LAN connections to remote networks.

1.2 Features of Prestige 128+

The following are the key features of the Prestige 128+.

L2TP Support

The L2TP protocol allows users to build their own private “tunnel” through the Internet to enable transport of non-IP traffic (e.g., IPX). Rather than making a long-distance call to the corporate server, a telecommuter or branch office can use a local ISP and the Internet to connect to a corporate network.

ISDN Basic Rate Interface (BRI) Support

The P128+ supports a single BRI. A BRI offers two 64Kbps channels, which can be used independently for two destinations or be bundled to speed up data transfer.

Extensive Analog Phone Support

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

Ethernet Port

The P128+ offers a choice of 10Base-T or AUI Ethernet port connections.

Single User Account (SUA)

The SUA™ (Single User Account) features allows multiple users to share a single user account.

Incoming Call Support

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

Multiple Protocol Support

- ◆ TCP/IP (Transmission Control Protocol/Internet Protocol) network layer protocol.
- ◆ Novel IPX (Internetwork Packet eXchange) network layer protocol.
- ◆ Transparently bridging for unsupported network layer protocols.
- ◆ PPP/MP (Point-to-Point Protocol/Multilink Protocol) link layer protocol.

Dial-On-Demand

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

PPP Multilink

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

Bandwidth-On-Demand

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

Full Network Management

- ◆ SNMP (Simple Network Management Protocol) support.
- ◆ Accessing SMT (System Management Terminal) through telnet connection.
- ◆ Web-based PWC (Prestige Web Configurator).

Logging and Tracing

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

RADIUS Support

RADIUS (Remote Authentication Dial-In User Service) is the most popular protocol for user authentication on dial-up lines. RADIUS support allows you to use an external server for unlimited number of users and the ease of centralized management.

PAP and CHAP Security

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

DHCP Support

DHCP (Dynamic Host Configuration Protocol) allows the workstations on your LAN to obtain the configuration from the Prestige.

Call Control

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

Data Compression

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

Networking Compatibility

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

Prestige Web Configurator

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

Backup and Restore Configuration File via LAN or WAN

PCT (Prestige Configuration Transfer), the stand-alone Java-based utility, allows backup and restoration of the configuration file via LAN or WAN.

Supplementary Voice Features

The Prestige supports the following Supplementary Voice Features on both of its Analog (POTS) Phone Ports:

- ◆ Call Waiting
- ◆ Three Way Calling (conference)

- ◆ Call Transfer
- ◆ Call Forwarding

1.3 Applications for Prestige 128+

The following sections show you the possible applications for your Prestige.

1.3.1 Internet Access

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

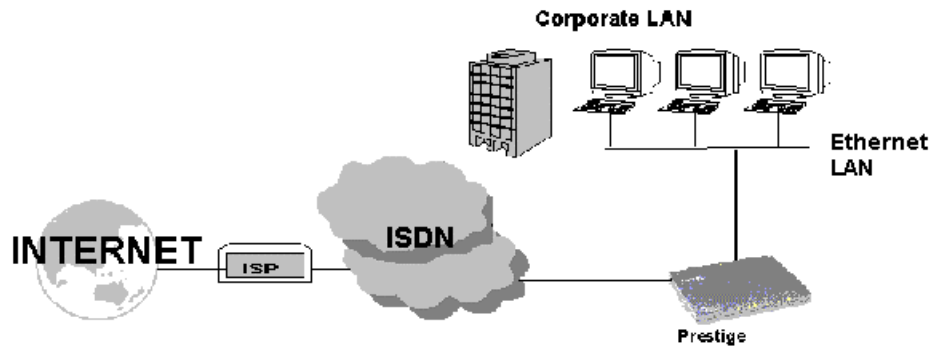


Figure 1-1 Internet Access Application

Internet Single User Account

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

1.3.2 Multi-Protocol/Multilink LAN-to-LAN Connection

You can use the Prestige to connect two geographically dispersed networks over up to 128Kbps over a single ISDN BRI line. It incorporates PPP/MP (Point-to-Point Protocol/Multilink Protocol) to bundle two B channels in a BRI line. The Prestige supports TCP/IP and Novell IPX routing, as well as transparent bridging for other network layer protocols. Your Prestige can also bundle multiple links in a single connection for greater bandwidth. A typical LAN-to-LAN application for your Prestige is shown below.

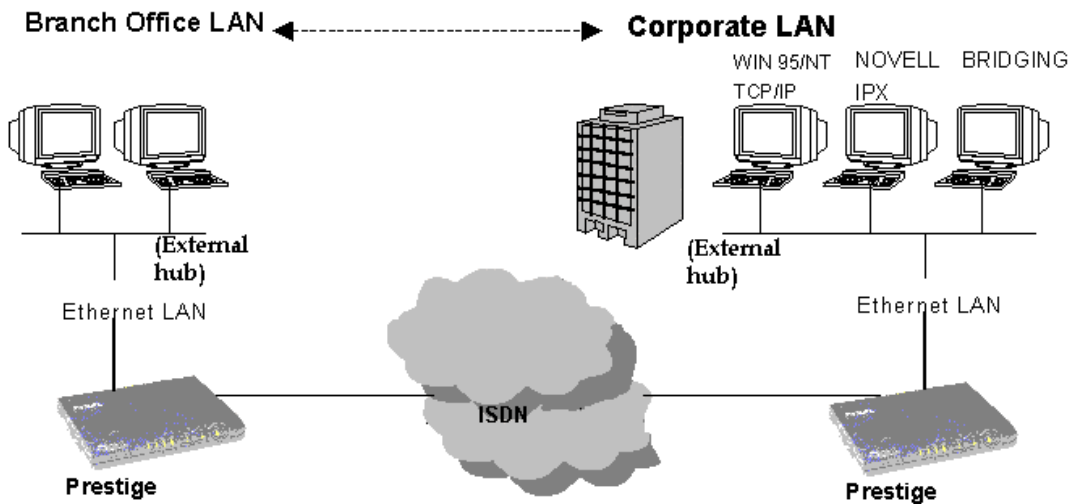


Figure 1-2 LAN-to-LAN Connection Application

1.3.3 Remote Access Server

Your Prestige allows remote users to dial-in and gain access to your LAN. This feature enables users that have workstations with remote access capabilities, e.g., Windows 95, to dial in to access the network resources without physically being

in the office. Either PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) authentication can be used to control the access from the remote users. You can also use callback for security and/or accounting purposes.

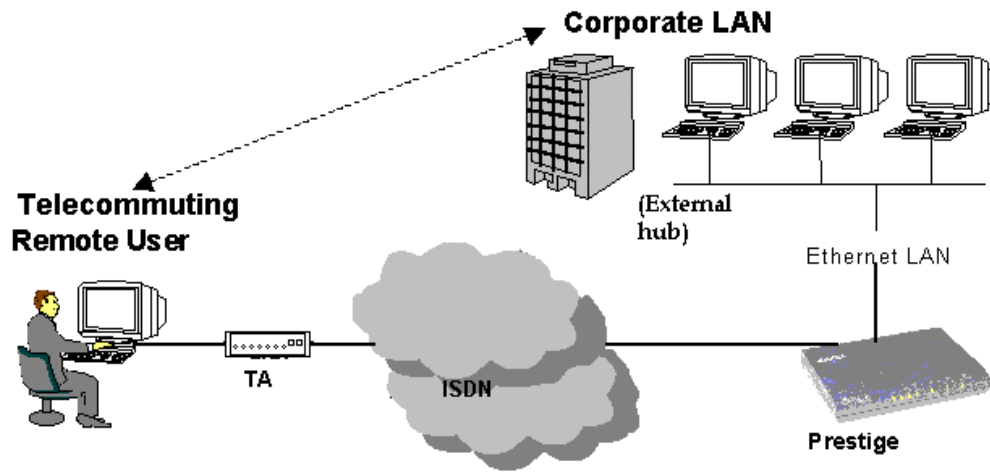


Figure 1-3 Telecommuting/Remote Access Server Application

Chapter 2

Hardware Installation & Initial Setup

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

2.1.1 Front Panel LEDs

The LED indicators on the front panel indicate the router functional status of the Prestige. The following table describes the LED functions:

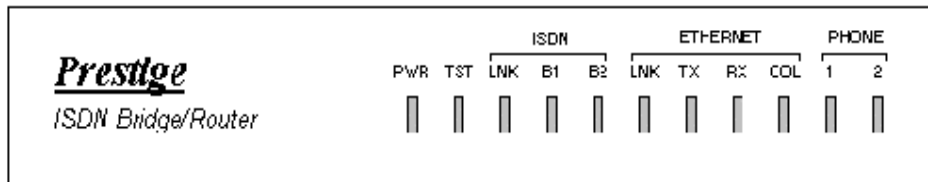


Figure 2-1 Front Panel

PWR	The PWR (power) LED is on when power is applied to the Prestige.
TST	A blinking TST (test) LED indicates the Prestige is functioning properly. A steady or an off TST indicates malfunction.
ISDN: LNK	The LNK (Link) LED is on when the Prestige is connected to an ISDN switch and the line has been successfully initialized.
ISDN: B1/B2	The B1/B2 LED is on when the corresponding B channel is in use.
ETHERNET	
LNK	This LED lights when the Prestige has made a successful Ethernet connection.
TX	This LED lights when the Prestige is transmitting via Ethernet connection.
RX	This LED lights when the Prestige is receiving via Ethernet connection.
COL	This LED blinks when collisions occur.
PHONE: 1/2	The LED is on when the device on the corresponding POTS port is in

	use.
--	------

Table 2-1 LED functions

2.2 Prestige 128+ Rear Panel and Connections

The figure below shows the rear panel of your Prestige 128MH and the connection diagram.

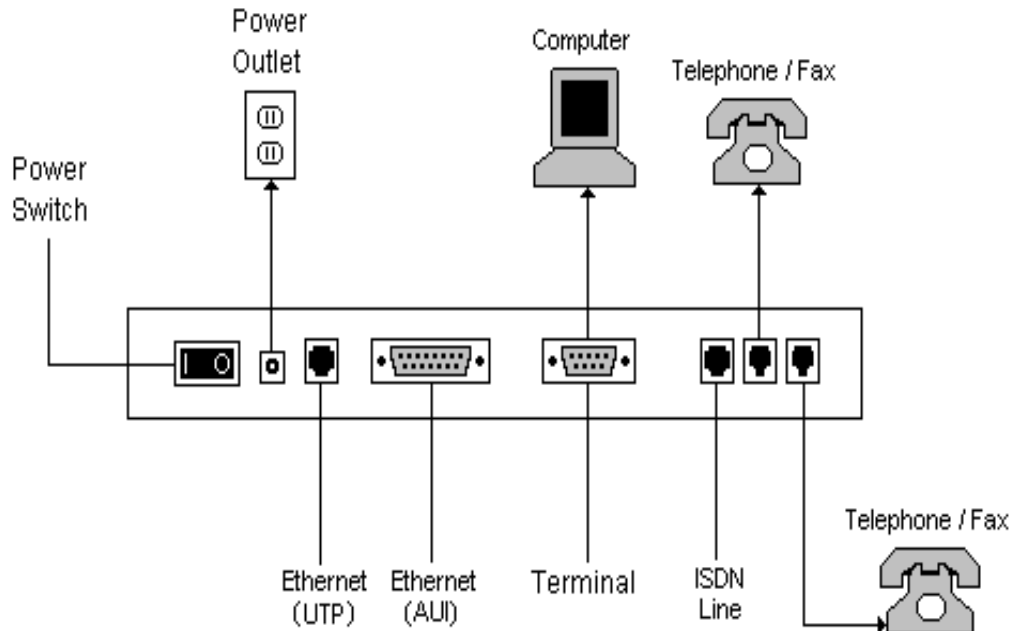


Figure 2-2 Prestige 128+ Rear Panel and Connections

This section outlines how to connect your Prestige 128MH to the LAN and to the ISDN network..

Step 1. Connecting the ISDN Line

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

Step 2. Connecting Ethernet to your Prestige

The Prestige supports two types of Ethernet connections. The connection procedure differs for each one; follow the one that is appropriate for your installation.

◆ UTP

The UTP port is used to connect to a 10Base-T network. 10Base-T networks use Unshielded Twisted Pair (UTP) cable and RJ-45 connectors that look like a bigger telephone plug with eight pins.

◆ AUI

The AUI port (the connector with 15 pins) is used to connect the Prestige to a 10Base5 (thicknet) network. If you have a 10Base2 network using BNC connectors and thin coaxial cables, you will need a transceiver between the AUI port and the 10Base2 cabling.

Warning *If one of these cables is accidentally used to connect your Prestige to the ISDN line, it may damage your Prestige. Please verify the correct cable before connecting.*

Step 2. Connecting a Telephone/Fax to the Prestige

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

Step 3. Connecting the Power Adapter to your Prestige

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

Step 4. Connecting the Console Port

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

After the initial setup, you can modify the configuration remotely through telnet connections. See *Chapter 14 - Telnet Configuration and Capabilities* for detailed instructions on using telnet to configure your Prestige.

2.3 Additional Installation Requirements

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

1. A computer with Ethernet 10Base-T NIC (Network Interface Card).
2. A computer equipped with communications software configured to the following parameters:
 - ◆ VT100 terminal emulation.
 - ◆ 9600 Baud.
 - ◆ No parity, 8 Data bits, 1 Stop bit.

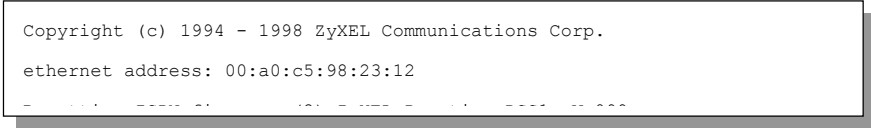
After the Prestige is properly set up, you can make future changes to the configuration through telnet connections.

2.4 Power On Your Prestige

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

Step 1. *Initial Screen*

When you power on your Prestige, it performs several internal tests as well as line initialization. After the initialization, the Prestige asks you to press **Enter** to



```
Copyright (c) 1994 - 1998 ZyXEL Communications Corp.  
ethernet address: 00:a0:c5:98:23:12  
-----
```

continue, as shown.

Figure 2-3 Power-On Display

Step 2. *Entering Password*

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

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

Please note that if there is no activity for longer than 5 minutes after you log in, your Prestige will automatically log you out and will display a blank screen. If



you see a blank screen, press [Enter] to bring up the login screen again.

Figure 2-4 Login Screen

2.5 Navigating the SMT Interface

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

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

Table 2-2 Main Menu Commands

Operation	Press/<read>	Description
Move forward to another menu	[Enter]	To move forward to a sub-menu, type in the number of the desired sub-menu and press [Enter].
Move backward to a previous menu	[Esc]	Press the [Esc] key to move back to the previous menu.
Move the cursor	[Enter] or [Up]/[Down] arrow keys	Within a menu, press [Enter] to move to the next field. You can also use the [Up]/[Down] arrow keys to move to the previous and the next field, respectively.
Enter information	Fill in, or Press the [Space bar] to toggle	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing the [Space] bar.
Required fields	<?>	All fields with the symbol <?> must be filled in order be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[Enter]	Save your configuration by pressing [Enter] at the message [Press ENTER to confirm or ESC to cancel]. Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [Enter].	Type 99 at the Main Menu prompt and press [Enter] to exit the SMT interface.

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

```

Copyright (c) 1994 - 1998 ZyXEL Communications Corp.
Prestige 128+ Main Menu

Getting Started
1. General Setup
2. ISDN Setup
3. Ethernet Setup
4. Internet Access Setup

Advanced Applications
10. Tunnel Endpoint Setup
11. Remote Node Setup
12. Static Routing Setup
13. Default Dial-in Setup
14. Dial-in User Setup
15. SUA Server Setup

Advanced Management
21. Filter Set Configuration
22. SNMP Configuration
23. System Security
24. System Maintenance

99. Exit

Enter Menu Selection Number:

```

Figure 2-5 SMT Main Menu

2.5.1 System Management Terminal Interface Summary

Table 2-3 Main Menu Summary

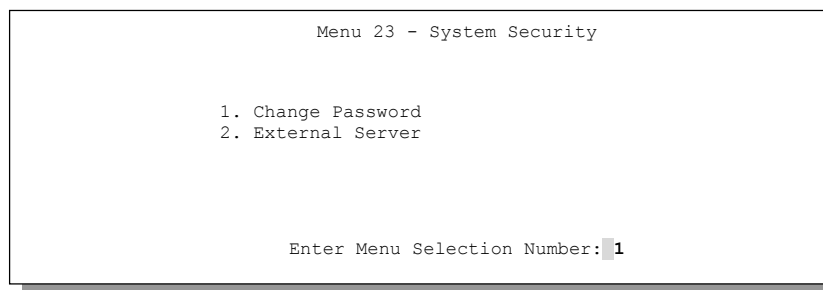
#	Menu Title	Description
1	General Setup	Use this menu to setup general information and to enable routing for specific protocols and bridging.
2	ISDN Setup	Use this menu to setup the ISDN.
3	Ethernet Setup	Use this menu to setup Ethernet.
4	Internet Access Setup	A quick and easy way to setup Internet connection.
10	Tunnel Endpoint Setup	Use this menu to configure L2TP support to route/bridge protocols over the Internet.
11	Remote Node Setup	Use this menu to setup the Remote Node for LAN-to-LAN connection, including Internet connection.
12	Static Routing Setup	Use this menu to setup static route for different protocols.

13	Default Dial-in Setup	Use this menu to setup default dial-in parameters so that your Prestige can be used as a dial-in server.
14	Dial-in User Setup	Use this menu to setup dial-in users.
15	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, call control, etc.
22	SNMP Configuration	Use this menu to setup SNMP related parameters
23	System Security	Use this menu to setup security related parameters.
24	System Maintenance	This menu provides system status, diagnostics, firmware upload, etc.
99	Exit	To exit from SMT and return to the blank screen.

2.6 Changing the System Password

The first thing you 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 Security** as



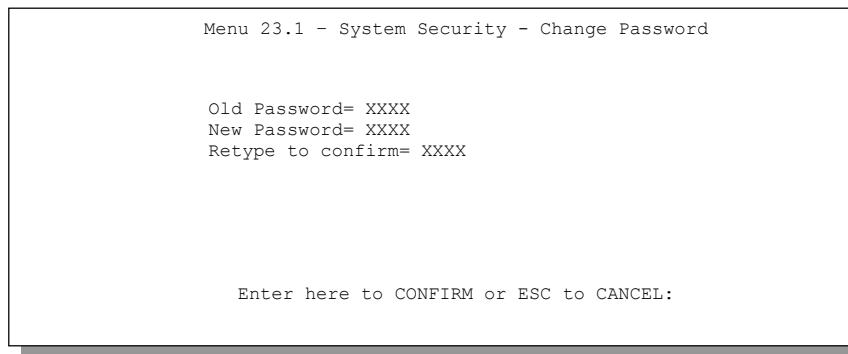
shown below.

Figure 2-6 Menu 23 - System Security

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

Password.

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



[Enter].

Figure 2-7 Menu 23.1 - System Security - Change Password

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

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

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

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 marked [?] and turn on the individual protocols for your applications, as explained in the following table.

```
Menu 1 - General Setup

System Name= P128plus
Location= branch
Contact Person's Name= JohnDoe

Route IP= Yes
Route IPX= No
Bridge= No

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

Figure 2-8 Menu 1 – General Setup

Table 2-4 General Setup Menu Fields

Field	Description	Example
System Name	Choose a descriptive name for identification purposes. This name can be up to 8 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted. This name can be retrieved remotely via SNMP, used for CHAP authentication, and will be displayed at the prompt in the Command Mode.	P128plus
Location (optional)	Enter the geographic location (up to 31 characters) of your Prestige.	MyHouse
Contact Person's Name (optional)	Enter the name (up to 8 characters) of the person in charge of this Prestige.	JohnDoe
Protocols:	Turn on or off routing for the individual protocols.	Press space-bar to toggle
Route IP	Set this field to Yes to enable IP routing. You must enable IP routing for Internet access.	Yes/No
Route IPX	Set this field Yes to enable IPX routing.	Yes/No
Bridge	Turn on/off bridging for protocols not supported (e.g., SNA) or not turned on in the previous Route fields.	Yes/No

Note on Bridging

When bridging is enabled, your Prestige forwards any packet that it does not route. Without bridging, the packets that the Prestige does not route are simply discarded. Compared to routing, bridging generates far more traffic for the same network protocol and consumes more CPU cycles and memory.

2.8 European ISDN Setup Menus

Menu 2 is for you to enter the information about your ISDN line. Please note that the Prestige only accepts digits in phone number fields; please do not include '-' or spaces in these fields.

2.8.1 Switch Type

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

2.8.2 MSN and Subaddress

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

2.8.3 Incoming Call Routing

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

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

2.8.4 Global Calls

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

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

2.8.5 Dial Prefix to Access Outside Line

Fill this field in if you need to dial a number (a single digit in most cases) to access an outside line; otherwise, leave it blank.

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

2.8.6 PABX Number (with S/T Bus Number)=

Enter the S/T bus number if the Prestige is connected to an ISDN PABX and a local loopback test is not possible. If this field is left blank then the loopback test

```

Menu 2 - ISDN Setup

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

ISDN Data      =                               Subaddress=
A/B Adapter 1 =                               Subaddress=
A/B Adapter 2 =                               Subaddress=

Dial Prefix to Access Outside Line =
PABX Number (with S/T Bus Number)=
Incoming Phone Number Matching= Multiple Subscriber Number (MSN)
  Analog Call Routing= N/A
  Global Analog Call= N/A
Edit Advanced Setup = No

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

is skipped.

Figure 2-9 Menu 2 – ISDN Setup

Table 2-5 Menu 2 – ISDN Setup

Switch Type	This field is fixed as DSS1.
B Channel Usage	In general, this is Switch/Switch . If you are only using one B channel (e.g., your Prestige is sharing the ISDN BRI line with another device on the S/T bus), then select Switch/Unused . The default is Switch/Switch .
ISDN Data & Subaddress	Enter the telephone number and the subaddress assigned to ISDN data calls for the Prestige. The maximum number of digits is 19 for the telephone number and 5 for the subaddress.
A/B Adapter 1 & Subaddress	Enter the telephone number and the subaddress assigned to A/B Adapter 1 (PHONE1).
A/B Adapter 2 & Subaddress	Same as above for A/B Adapter 2 (PHONE2).
Dial Prefix to Access Outside Line	Enter the prefix number if the Prestige is connected to an ISDN PABX. This number should be no longer than 3 digits. Otherwise, leave this field blank.
PABX Number (with S/T Bus Number)	Enter the S/T bus number if the Prestige is connected to an ISDN PABX. If this field is left as blank then the loopback test is skipped
Incoming Phone Number Matching	Determines how incoming calls are routed. The choices for this field are Multiple Subscriber Number (MSN) , Called Party Subaddress and Don't Care .
Analog Call Routing	Select the destination for analog calls. The choices are A/B Adapter 1 , A/B Adapter 2 and Ignore . This field is only applicable when Incoming Phone Number Matching is Don't Care .
Global Analog Call	Select how to handle global analog calls. The choices are Accept and Ignore . This field is not applicable when the Analog Call Routing is Ignore .
Advanced Setup	Select Yes and press Enter to go to the advanced setup submenu.

2.8.7 Advanced Setup

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

ISDN Call Waiting

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

How to use call waiting

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

Calling Line Indication

```

Menu 2.1 - ISDN Advanced Setup

Phone 1 Call Waiting= Disable
Phone 2 Call Waiting= Disable
Calling Line Indication= Presented (CLIP)

```

Figure 2-10 ISDN Advanced Setup

The **Calling Line Indication**, or Caller ID, governs whether the other party can see your number when you call. If set to **Presented (CLIP)**, the Prestige sends the caller ID and the party you call can see your number, otherwise, if set to **Restricted (CLIR)** the caller ID is blocked.

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

At this point, the Prestige asks if you wish to test your ISDN. If you select **Yes**, the Prestige will perform a loop-back test to check the ISDN line. If the loop-

```

2-18 Setup LoopBack Test...
      Dialing to 40000// ...
      Sending and Receiving Data ...

```

and Setup

back test fails, please note the error message that you receive and take the appropriate troubleshooting action.

Figure 2-11 Loopback test

2.9 Ethernet Setup

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

```
Menu 3 - Ethernet Setup

1. General Setup
2. TCP/IP and DHCP Setup
3. Novell IPX Setup
4. Bridge Setup

Enter Menu Selection Number:
```

Figure 2-12 Menu 3 - Ethernet Setup

2.9.1 General Ethernet Setup

This menu allows you to specify the filter sets that you wish to apply to the Ethernet traffic. You seldom need to filter Ethernet traffic, however, the filter

```
Menu 3.1 - General Ethernet Setup

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

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

sets may be useful to block certain packets, reduce traffic and prevent security breaches.

Figure 2-13 Menu 3.1 - General Ethernet Setup

If you need to define filters, please read *Chapter 9- Filter Set Configuration*, then return to this menu to define the filter sets.

2.10 Protocol Dependent Ethernet Setup

Depending on the protocols for your applications, you need to configure the respective Ethernet Setup, as outlined below.

- For TCP/IP Ethernet setup refer to *Chapter 3 - Internet Access Application*.
- For Novell IPX Ethernet setup refer to Section 7.4 - IPX Ethernet Setup in *Chapter 7 - Novell IPX Configuration for LAN-to-LAN*.
- For bridging Ethernet setup refer to *Chapter 8 - Bridge Configuration for LAN-to-LAN*.

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 Route IP Setup

The first step is to enable the IP routing in Menu 1 - General Setup.

To edit Menu 1, enter 1 in the Main Menu to select **General Setup** and press [Enter]. Set the **Route IP** field to **Yes** by pressing the space bar.

```
Menu 1 - General Setup

System Name= p128plus
Location= location
Contact Person's Name= name
Route IP= Yes
Route IPX= No
Bridge= No

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

Figure 3-1 Menu 1 – General Setup

3.2 TCP/IP Parameters

3.2.1 IP Address and Subnet Mask

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

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 (ignoring the trailing zero) and you must enable the Single User Account feature of the Prestige. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do *not* use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first 3 numbers specify the network number while the last number identifies an individual workstation on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, e.g., 192.168.1.1, for your Prestige.

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

3.2.2 RIP Setup

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

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

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

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

3.2.3 DHCP Configuration

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (workstations) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The Prestige has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client.

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 Server Address

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

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

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

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

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make

sure that you enter their IP addresses in the **DHCP Setup** menu. This way, the Prestige can pass the DNS servers to the workstations and the workstations can query the DNS server directly without the Prestige's intervention.

3.3 TCP/IP Ethernet Setup and DHCP

You will now use Menu 3.2 to configure your Prestige for TCP/IP.

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

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

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

TCP/IP Setup:
IP Address= 192.68.1.1
IP Subnet Mask= 255.255.255.0
RIP Direction= Both
Version= RIP-2B

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

Ethernet Setup, as shown below.

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

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

Table 3-1 DHCP Ethernet Setup Menu Fields

Field	Description	Example
DHCP Setup		
DHCP=	This field enables/disabled the DHCP server. If it is set to Server , your Prestige will act as a DHCP server. If set to None , DHCP server will be disabled. When DHCP is used, the following four items need to be set:	None 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	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.	
Secondary DNS Server		

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

Table 3-2 TCP/IP Ethernet Setup Menu Fields

Field	Description	Example
TCP/IP Setup		
IP Address	Enter the IP address of your Prestige in dotted decimal notation	192.168.1.1 (default)
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige	255.255.255.0
RIP Direction	Press the space bar to select the RIP direction from Both/In Only/Out Only .	Both (default)
Version	Press the space bar to select the RIP version from RIP-1/RIP-2B/RIP-2M .	RIP-1 (default)
When you have completed this menu, press [Enter] at the prompt [Press ENTER to Confirm...] to save your configuration, or press [Esc] at any time to cancel.		

3.4 Internet Access Configuration

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

Use the table below to record your Internet Account Information.

Table 3-3 Internet Account Information

Internet Account Information	Write your account information here
IP Address of the ISP's Gateway (Optional)	<input type="text"/>
Telephone Number(s) of your ISP	<input type="text"/>
Login Name	<input type="text"/>
Password for ISP authentication	<input type="text"/>
DNS server address(es) for your workstation	<input type="text"/>

From the Main Menu, enter option **Internet Access Setup** to go to Menu 4 - Internet Access Setup, as displayed below. The following table contains

```
Menu 4 - Internet Access Setup

ISP's Name= myISP
Pri Phone #= 1234
Sec Phone #=
My Login= JohnDoe
My Password= *****
Single User Account= Yes
IP Addr= 0.0.0.0

Telco Options:
Transfer Type= 64K

Multilink= Off
Idle Timeout= 100

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

instructions on how to configure your Prestige for Internet access.

Figure 3-3 Menu 4 – Internet Access Setup

Table 3-4 Internet Access Setup Menu Fields

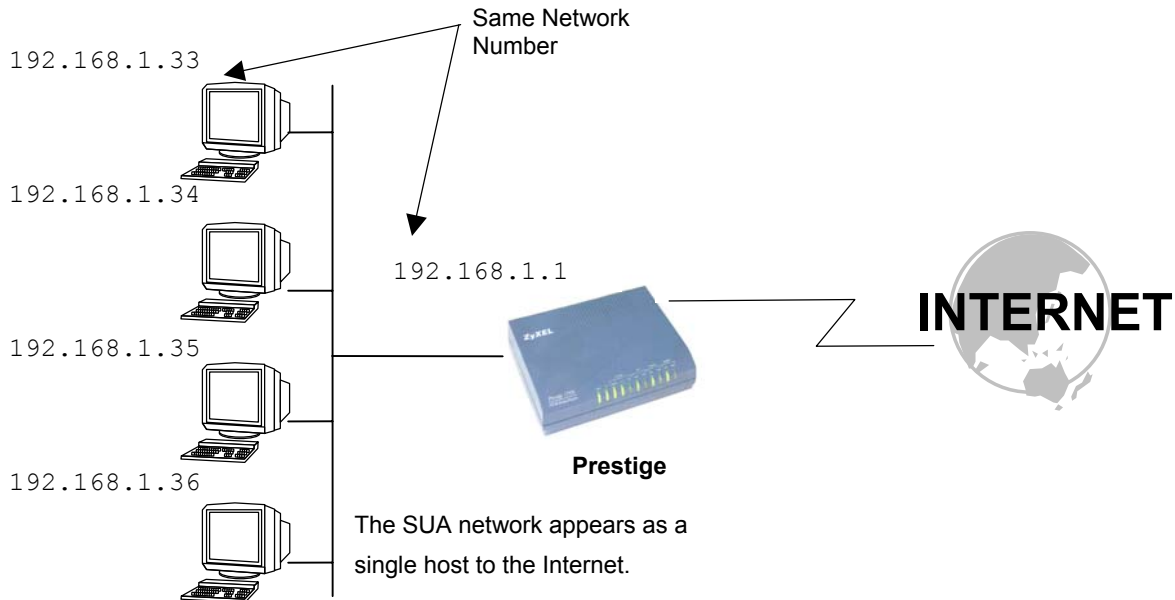
Field	Description
ISP's Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.
ISP IP Addr	Enter the IP Address of the remote gateway at the ISP's site. If you don't have this data, just leave it blank.
Pri Phone and Sec Phone Number	Both the Primary and the Secondary Phone number refer to the number that the Prestige dials to connect to the ISP.
My Login Name	Enter the login name given to you by your ISP.
My Password	Enter the password associated with the login name above.
Single User Account	Please see the following section for a more detailed discussion on the Single User Account feature. The default is Yes .
Telco options: Transfer Type	This field specifies the type of connection between the Prestige and this remote node. Select 64K , or Leased .
Multilink	The Prestige uses the PPP Multilink Protocol (PPP/MP) to bundle multiple links in a single connection to boost the effective throughput between two nodes. This option is only available if the transfer type is 64K . See menu 11.2 for more details.
Idle Timeout	This value specifies the number of idle seconds that elapses before the remote node is automatically disconnected. Idle seconds is the period of time when no data is transmitted from your Prestige. Administrative packets such as RIP are not counted as data. The default is 100 seconds. <i>This option only applies when the Prestige initiates the call.</i>

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

3.5 Single User Account

Typically, if there are multiple users on the LAN wanting to concurrently access the Internet, you will 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).

Figure 3-4 Single User Account Topology

The Single User Account feature may also be used on connections to remote networks other than the ISP. For example, this feature can be used to simplify

the allocation of IP addresses when connecting branch offices to the corporate network.

The IP address for the SUA can be either fixed or dynamically assigned when a call is connected. 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 will be filtered out by your Prestige and 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)*.

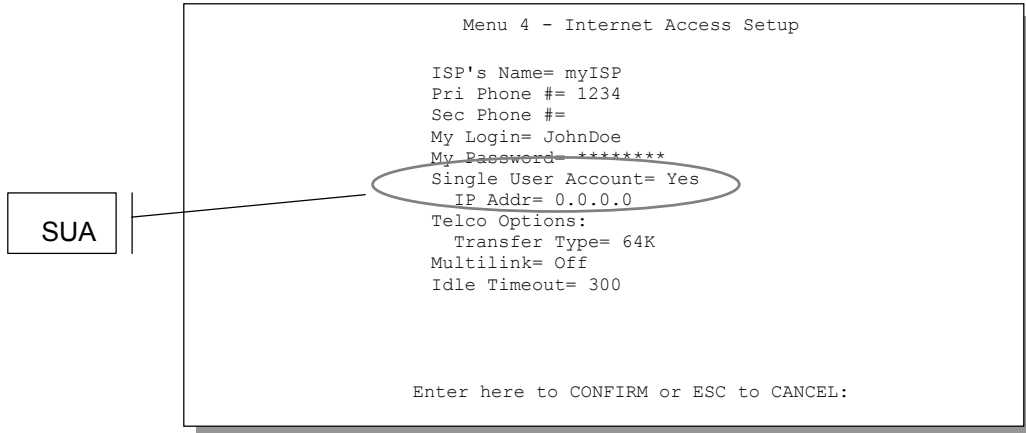
3.5.1 Advantages of SUA

In summary:

- SUA is a cost-effective solution for small offices with less than 20 hosts 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 will be filtered out by your Prestige.
- UDP and TCP packets can be routed. In addition, partial ICMP, including echo and trace route, is supported.

3.5.2 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, as shown below.

Figure 3-5 Menu 4 – Internet Access Setup for Single User Account

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 3-5 Single User Account Menu Fields

Field	Description
Single User Account	Select Yes to enable SUA.
IP Addr.	If your ISP did <i>not</i> assign you a static IP address, enter [0.0.0.0] here; otherwise, enter that IP address here.
Press [Enter] at the message [Press ENTER to Confirm ...] to save your configuration, or press [Esc] at any time to cancel.	

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

3.6 Configuring Backup ISP Accounts

If you have more than one ISP account, you can configure the secondary ISP as a backup. You can switch to the backup ISP in the event that the primary ISP is out of service. The SUA feature can be enabled for all these accounts.

3.6.1 Configure a Backup ISP

To configure a backup ISP Account, follow these steps:

- Step 1.** Configure your primary ISP using Menu 4, as described earlier in this chapter.
- Step 2.** Enter Menu 11, then select an unused remote node.
- Step 3.** In Menu 11.1, choose a name for your backup ISP account, then set the **Active** field to **No**, and enter your outgoing login name, password, and phone number(s). The Remote IP Address field should be set to **1.1.1.1**.
- Step 4.** In Menu 11.3, set the remote node's subnet mask to **0.0.0.0**, and set RIP to **None**.
- Step 5.** Save the new configuration.

Please note that the remote IP address of **1.1.1.1** is only a placeholder to avoid conflicting with that of the primary ISP, which is implicitly set at **0.0.0.0**. When the backup ISP is activated, the remote IP address of **1.1.1.1** combined with the subnet mask of **0.0.0.0** creates a default route that is equivalent to the one derived from the primary ISP.

3.6.2 To Switch ISP

Follow these steps when you need to switch from your primary ISP to a backup ISP:

- Step 1.** Enter Menu 11 and select your Primary ISP.
- Step 2.** In Menu 11.1, set the **Active** field to **No**.
- Step 3.** Enter Menu 11 again and select your Backup ISP.
- Step 4.** In Menu 11.1, set the **Active** field to **Yes**.

You will now be able to access the Internet through the backup ISP Remote Node.

Chapter 4

Remote Node Configuration

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

In this chapter, we will discuss the parameters that are protocol independent. The protocol-dependent configuration will be covered in subsequent chapters. For TCP/IP, see *Chapter 5*, for IPX, see *Chapter 6* and for Bridging, see *Chapter 7*.

4.1 Remote Node Setup

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

4.1.1 Remote Node Profile

To configure a remote node, follow these steps:

- Step 1.** From the Main Menu, select menu option **1. Remote Node Setup**
- Step 2.** When Menu 11 appears, as shown below, enter the number of the remote node that you wish to configure.

```

Menu 11 - Remote Node Setup

Menu 11 - Remote Node Setup

1. nodename
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____
12. _____

Enter Node # to Edit:
    
```

Figure 4-1 Menu 11 – Remote Node Setup

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

```

Menu 11.1 - Remote Node Profile

Rem Node Name= nodename          Route= IP
Active= Yes                       Bridge= No

Call Direction= Outgoing          Edit PPP Options= No
Tunneling Mode= Direct            Rem IP Addr= 0.0.0.0
Endpoint Index= 1                Edit IP/IPX/Bridge= No
Incoming:                          Telco Option:
  Rem Login= N/A                  Allocated Budget(min)= 0
  Rem Password= N/A              Period(hr)= 0
  Rem CLID= N/A                  Transfer Type= 64K
  Call Back= N/A                 Nailed-Up Connection= No
Outgoing:                          Session Options:
  My Login= ChangeMe             Edit Filter Sets= No
  My Password= *****          Idle Timeout(sec)= 100
  Authen= CHAP/PAP
  Pri Phone #= 1234
  Sec Phone #=

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

Profile Menu Fields table shows how to configure the Remote Node Menu.

Figure 4-2 Menu 11.1 Remote Node Profile

Table 4-1 Remote Node Profile Menu Fields

Field	Description	Options
Rem Node Name	This is a required field [?]. Enter a descriptive name for the remote node, for example, Corp. This field can be up to eight characters. This name must be unique from any other remote node name or remote dial-in user name.	
Active	Press the space bar to toggle between Yes and No . Inactive nodes are displayed with a minus sign (-) at the beginning of the name in Menu 11.	Press space bar to toggle Yes/No
Call Direction	<ul style="list-style-type: none"> ● If this parameter is set to Both, your Prestige can both place and receive calls to/from this remote node. ● If set to Incoming, your Prestige will not place a call to this remote node. ● If set to Outgoing, your Prestige will drop any incoming calls from this remote node. <p>Several other fields in this menu depend on this parameter. For example, in order to enable Callback, the Call Direction must be Both.</p>	Both Incoming Outgoing
Incoming: Rem Node Login Name	Enter the login name that this remote node will use when it calls your Prestige. The login name in this field combined with the Rem Node Password will be used to authenticate this node.	
Incoming: Rem	Enter the password used when this remote node	

	Node Password	calls your Prestige.	
Incoming:	Rem CLID	<p>This field is applicable only if Call Direction is either Both or Incoming. Otherwise, a N/A appears in the field.</p> <p>This is the Calling Line ID (the telephone number of the calling party) of this remote node.</p> <p>If you enable the CLID Authen field in Menu 13 – Default Dial In, your Prestige will check the CLID in the incoming call against the CLIDs in the database. If no match is found and CLID Authen is Required, the call will be dropped.</p>	
Incoming:	Callback	<p>This field is applicable only if Call Direction is Both. Otherwise, a N/A appears in the field.</p> <p>This field determines whether or not your Prestige will call back after receiving a call from this remote node.</p> <p>If this option is enabled, your Prestige will disconnect the initial call from this node and call it back at the Outgoing Primary Phone Number (see below).</p>	<p>Enable</p> <p>Disable</p>
Outgoing:	My Login Name	This is a required field [?] if Call Direction is either Both or Outgoing . Enter the login name for your Prestige when it calls this remote node.	
Outgoing:	My Password	This is a required field [?] if Call Direction is either Both or Outgoing . Enter the password for your Prestige when it calls this remote node.	
Outgoing:	Authen	<p>This field sets the authentication protocol used for outgoing calls.</p> <p>Options for this field are:</p> <ul style="list-style-type: none"> ● CHAP/PAP - Your Prestige will accept either CHAP or PAP when requested by this remote node. ● CHAP - accept CHAP only. ● PAP - accept PAP only. 	<p>CHAP/PAP</p> <p>CHAP</p> <p>PAP</p>
Outgoing:	Pri(mary) Sec(ondar)	Your Prestige always calls this remote node using the Primary Phone number first for a dial-	

y) Phone Numbers	<p>up line.</p> <p>If the Primary Phone number is busy or does not answer, your Prestige will dial the Secondary Phone number if available.</p> <p>Some areas require dialing the pound sign # before the phone number for local calls. A # symbol may be included at the beginning of the phone numbers as required.</p>	
Route	This field determines the protocols that your Prestige will route.	
Bridge	Bridging is used for protocols that the Prestige does not support, e.g., SNA, or not turned on in the previous Route field. When bridging is enabled, your Prestige will forward any packet that it does not route to this remote node; otherwise, the packets are discarded.	<p>Press space bar to toggle</p> <p>Yes/No</p>
Edit PPP Options	To edit the PPP options for this remote node, move the cursor to this field, use the space bar to select Yes and press [Enter]. This will bring you to Menu 11.2 - Remote Node PPP Options. For more information on configuring PPP options, see the section <i>Editing PPP Options</i> .	<p>Press space bar to toggle</p> <p>Yes then press [Enter]</p>
Rem IP Addr	This is a required field [?] if Route is set to IP . Enter the IP address of the remote gateway.	
Edit IP/IPX/Bridge Options	To edit the parameters, select Yes and press [Enter]. This will bring you to Menu 11.3 - Remote Node Network Layer Options. For more information on this screen, refer to the chapter pertaining to your specific protocol.	<p>Press space bar to toggle</p> <p>Yes then press [Enter]</p>
<p>Telco Options:</p> <p>Allocated Budget (min)</p> <p>Period (hr)</p>	<p>This field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 for no budget control.</p> <p>This field sets the time interval to reset the above outgoing call budget control.</p>	<p>Default = 0</p>
Transfer Type	This field specifies the type of connection between the Prestige and this remote node. When set to Leased , the Allocated Budget and Period do not apply.	<p>64k/</p> <p>Leased</p>

Nailed-up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. See below for more details.	Yes/No
Session Option: Edit Filter Sets	Use the space bar to toggle this field to Yes and press [Enter] to open Menu 11.5 to edit the filter sets. See the Remote Node Filter section for more details.	Default= Blank
Session Option: Idle Timeout (sec)	This value specifies the number of idle seconds that elapses before the remote node is automatically disconnected. Idle seconds is the period of time when no data is transmitted from your Prestige. Administrative packets such as RIP are not counted as data. <i><u>This option only applies when the Prestige initiates the call.</u></i>	Default= 100 secs for the first remote node and 300 secs for the others.
Once you have completed filling in Menu 11.1.1 – Remote Node Profile, press [Enter] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] at any time to cancel.		

4.1.2 Nailed-up Connection

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The Prestige does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the Prestige will try to bring up the connection at power-on and whenever the connection is down.

A nailed-up connection can be very expensive for obvious reasons. Please do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

4.1.3 Outgoing Authentication Protocol

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

4.1.4 PPP Multilink

The Prestige uses the PPP Multilink Protocol (PPP/MP) to bundle multiple links in a single connection to boost the effective throughput between two nodes. The bundle works best when the member links are of the same type of call and at approximately the same speed.

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

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

4.1.5 Bandwidth on Demand

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

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

Table 4-2 BTR v MTR for BOD

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

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

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

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

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

4.1.6 Editing PPP Options

To edit the remote node PPP Options, move the cursor to the **Edit PPP Options** field in Menu 11.1 - Remote Node Profile, and use the space bar to select **Yes**. Press **Enter** to open Menu 11.2, as shown below.

```
Menu 11.2 - Remote Node PPP Options

Encapsulation= Standard PPP
Compression= No

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

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

Figure 4-3 Menu 11.2 - Remote Node PPP Options

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

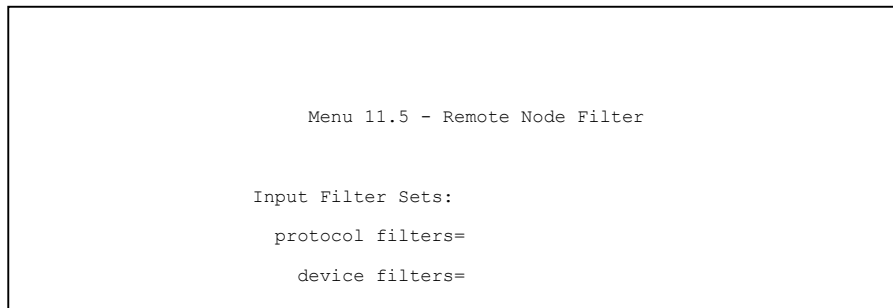
Table 4-3 Remote Node PPP Options Menu Fields

Field	Description	Option
Encapsulation	Select the CISCO PPP only when this remote node is a Cisco machine; otherwise, select the Standard PPP.	Standard PPP CISCO PPP
Compression	Turn on/off Stac Compression. The default for this field is Off .	On/Off (Default = Off)
Multiple Link Options:		
BOD Calculation	Select the direction of the traffic you wish to use in determining when to add or subtract a link. The default for this field is Transmit or Receive .	Default = Transmit or Receive
Base Trans Rate	Select the base data transfer rate for this remote node in Kbps. There are two choices for this field- 64 where only one channel is used or 128 where two channels are used as soon as a packet triggers a call	64/128
Max Trans Rate	Enter the maximum data transfer rate allowed for this remote node. This parameter is in kilobits per second. There are two choices for this field- same as above.	64/128
Target Utility (kbps)	Enter the two thresholds separated by a [-] for subtracting and adding the second port.	Default=10-20
Add Persist	This parameter specifies the number of seconds where traffic is above the adding threshold before the Prestige will bring up the second link.	Default = 5 sec
Subtract Persist	This parameter specifies the number of seconds where traffic is below the subtraction threshold before your Prestige drops the second link.	Default = 5 sec
Once you have completed filling in Menu 11.2 - Remote Node PPP Options, press [Enter] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] at any time to cancel.		

4.1.7 Remote Node Filter

Use **Menu 11.5 – Remote Node Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige and 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. For more information on defining the filters, *see Chapter 9*. The Prestige comes with a prepackaged filter set, NetBIOS_WAN, that blocks NetBIOS packets. You can include this in the call filter sets if you wish to prevent NetBIOS packets from triggering calls to a



remote node.

Figure 4-4 Menu 11.5 – Remote Node Filter

Chapter 5

Remote Node TCP/IP Configuration

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

5.1 LAN-to-LAN Application

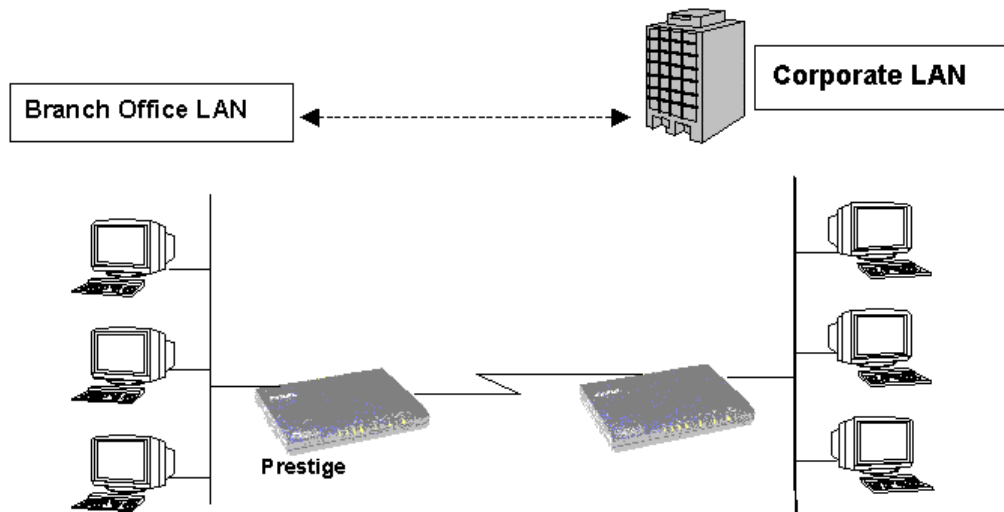


Figure 5-1 TCP/IP LAN-to-LAN Application

For the branch office, you need to configure a remote node in order to dial out to the headquarters. Additionally, you may also need to define static routes if some services reside beyond the immediate remote LAN.

5.1.1 Remote Node Setup

Follow the procedure in *Chapter 5 - Remote Node Configuration* to configure the protocol-independent parameters in Menu 11 - Remote Node Profile. For the TCP/IP parameters, follow the instructions below. If you are configuring your Prestige to receive incoming calls, you also need to set the default dial-in parameters in Menu 13.

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

In Menu 11.1, make sure **IP** is among the protocols in the Route field. (The Route field should display Route = IP or Route = IP + IPX.)

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

```

Menu 11.3 - Remote Node Network Layer Options

IP 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= No

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

IPX Options:
Dial-On-Query= N/A
Rem LAN Net #= N/A
My WAN Net #= N/A
Hop Count= N/A
Tick Count= N/A
W/D Spoofing(min)= N/A
SAP/RIP Timeout(min)= N/A

Bridge Options:
Dial-On-Broadcast= N/A
Ethernet Addr Timeout(min)= N/A

Enter here to CONFIRM or ESC to CANCEL:

```

Layer Options.

Figure 5-2 Menu 11.3- Remote Node TCP/IP Options

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

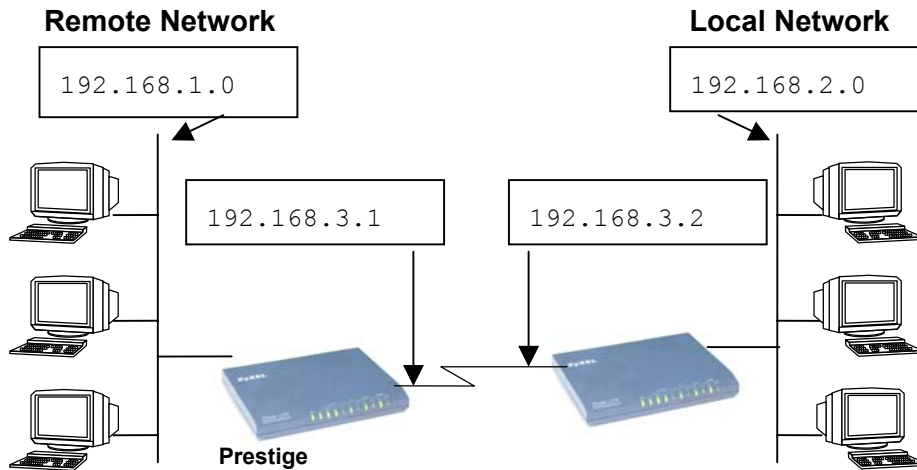


Figure 5-3 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection

To configure the TCP/IP parameters of a remote node, first configure the three fields in Menu 11 – Remote Node Profile, as shown in the table below. For more details on the IP Option fields, refer to *Chapter 3 – Internet Access Application*.

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

Field	Description	Option
Route	Make sure IP is among the protocols in the Route field in the Remote Node Profile.	IP
Rem IP Address	Enter the IP address of the remote gateway in Remote Node Profile.	
Edit IP/IPX/Bridge	Press the space bar to select Yes and press Enter to go to Menu 11.3 - Remote Node Network Layer Options Menu.	Yes (Yes/No)

	Options Menu.	
--	---------------	--

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

Table 5-2 TCP/IP Remote Node Configuration

Rem IP Address	This will show the IP address you entered for this remote node in the previous menu.	
Rem IP Subnet Mask	Enter the subnet mask for the remote network.	
My WAN Addr	Some implementations, especially the UNIX derivatives, require the ISDN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the ISDN port of your Prestige. Note that this is the address assigned to your local Prestige, not the remote router.	
Single User Account	Set this field to Yes to enable the Single User Account feature for your Prestige. Use the space bar to toggle between Yes and No . See <i>Chapter 3 - Internet Access Application</i> for more information on the Single User Account feature.	Yes/No
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	1 to 15
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to Yes , this route is kept private and not included in RIP broadcast. If No , the route to this remote node will be propagated to other hosts through RIP broadcasts.	Yes/No
RIP	Press the space bar to select the RIP direction from Both/In Only/Out Only .	(Default= Both)

Version=	Press the space bar to select the RIP version from RIP-1/RIP-2B/RIP-2M .	RIP-1 (default)
Once you have completed filling in the Network Layer Options Menu, press [Enter] to return to Menu 11. Press [Enter] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] at any time to cancel.		

5.1.2 Static Route Setup

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

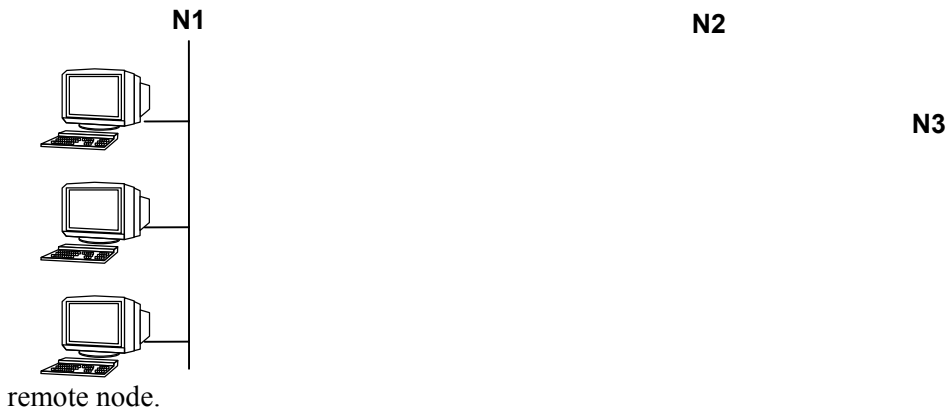


Figure 5-4 Example of Static Routing Topology

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

```
Menu 12 - Static Route Setup

1. IP Static Route
2. IPX Static Route
3. Bridge Static Route

Please enter selection:
```

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

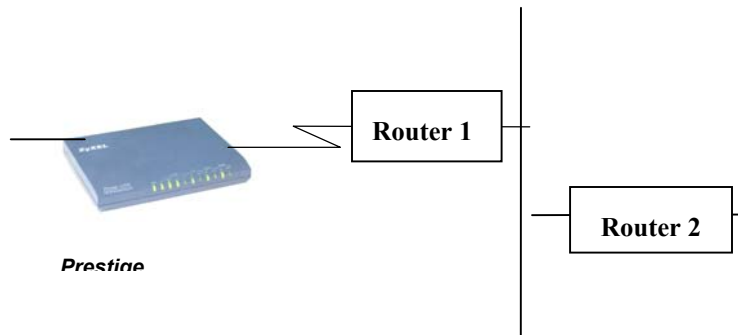


Figure 5-5 Menu 12 - Static Route Setup

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

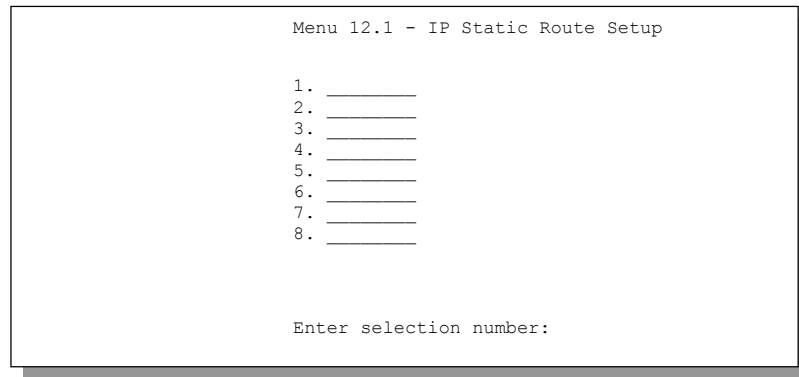


Figure 5-6 Menu 12.1 - IP Static Route Setup

Choosing a static route to edit produces the following screen.

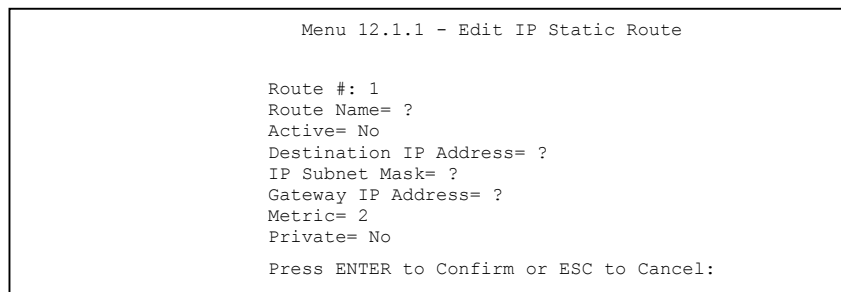


Figure 5-7 Edit IP Static Route

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

Table 5-3 Edit IP Static Route Menu Fields

Field	Description
Route Name	Enter a descriptive name for this route. This is for identification 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 subnet mask for this destination. Follow the discussion on IP subnet mask in this chapter.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Prestige that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Prestige; over WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Same meaning as those in the Remote Node Setup.
Private	Same meaning as those in the Remote Node Setup.

Chapter 6

IPX Configuration

This chapter shows you how to configure the IPX parameters of the Prestige.

6.1 IPX Network Environment

Novell bundles the protocol stack, the server software and routing functionality in their NetWare server products. So a NetWare server is not only a file or print server, it is also a router.

6.1.1 Network and Node Number

Every IPX machine has a network number and a node number, together they form the complete address of the machine. The IPX network number is a 32-bit quantity and is usually expressed in 8 hexadecimal digits, e.g., 0893A8CF. The host number is a 48-bit quantity and usually is taken from the MAC (Media Access Control) address of the Ethernet hardware, so you don't have to explicitly configure the node number.

An IPX client obtains its network number from a server that has the network numbers statically configured. If there are multiple servers on a network, only one server need to have the network numbers configured, and all other stations (clients and servers) can obtain the network numbers from it. The server with configured network numbers is called a seed router.

If you have a NetWare server on the same LAN as the Prestige, we recommend that you set up a NetWare server as a seed router. Even though the Prestige is capable as a seed router, a NetWare server offers a much more extensive facility for network management.

6.1.2 Frame Types

IPX can run on top of four different frame types on the Ethernet. These frame types are 802.2, 802.3, Ethernet II (DIX), and SNAP (Sub-Network Access Protocol). Each frame type is a separate logical network, even though they exist on one physical cable (see the following diagram).

Although there are four frame types available on the Ethernet, you should configure as few frame types as possible on your NetWare server and use automatic frame detection on the clients to simplify management and to reduce network overhead.

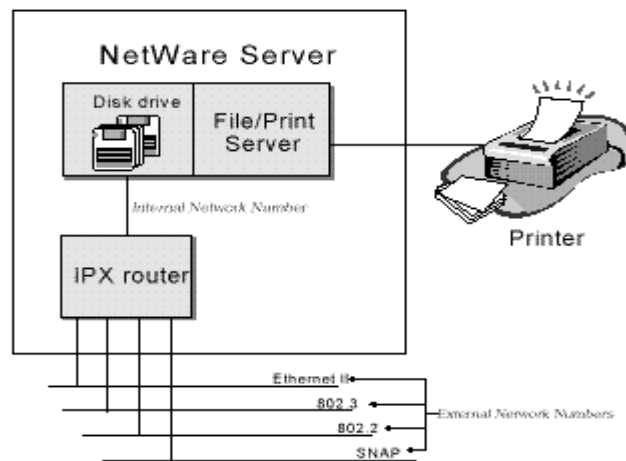


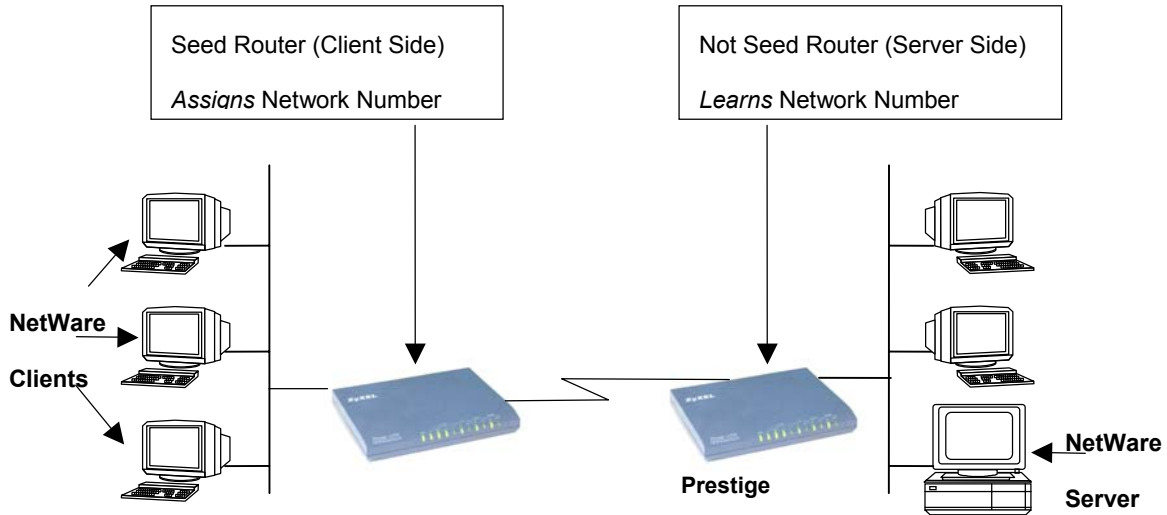
Figure 6-1 NetWare Server

6.1.3 External Network Number

Each of the four logical networks (based on frame type) has its own external network number.

6.1.4 Internal Network Number

In addition to the external network numbers, each NetWare server has its own internal network number that is a virtual network to which the server is attached. It is important to remember that every network number must be unique for that



entire internetwork, either internal or external.

6.2 Prestige in an IPX Environment

There are two scenarios in which your Prestige is deployed, depending on whether there is a NetWare server on the LAN, as depicted in the following diagram.

Figure 6-2 Prestige in an IPX Environment

6.2.1 Prestige on LAN with Server

If your Prestige is on a LAN with a seed router, you do not need to configure the LAN network numbers. Your Prestige will learn the network number from the seed router and add the routes to its routing table.

6.2.2 Prestige on LAN without Server

Each IPX network must have a seed router. If you only have NetWare clients on your network, then you must configure the Prestige as a seed router and set up unique network numbers for each frame type enabled using the Ethernet Setup Menu.

6.3 IPX Spoofing

Your Prestige comes with several pre-defined call filters designed to prevent certain IPX packets from triggering a call to a remote node.

The built-in call filters are defined as follows:

- Block periodical RIP (Routing Information Protocol) and SAP (Service Advertising Protocol) response messages.
- Block NetWare serialization packets.
- Allow SAP and RIP inquiry packets.

6.4 IPX Ethernet Setup

From Menu 3 - Ethernet Setup, select option **Novell IPX Setup** to go to Menu 3.3 - Novell IPX Ethernet Setup as shown in the figure below.

```

Menu 3.3 - Novell IPX Ethernet Setup

Seed Router= No

Frame Type 802.2= Yes
  IPX Network #= N/A

Frame Type 802.3= No
  IPX Network #= N/A

Frame Type Ethernet II= No
  IPX Network #= N/A

Frame Type SNAP= No
  IPX Network #= N/A

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

```

Figure 6-3 Menu 3.3 - Novell IPX Ethernet Setup

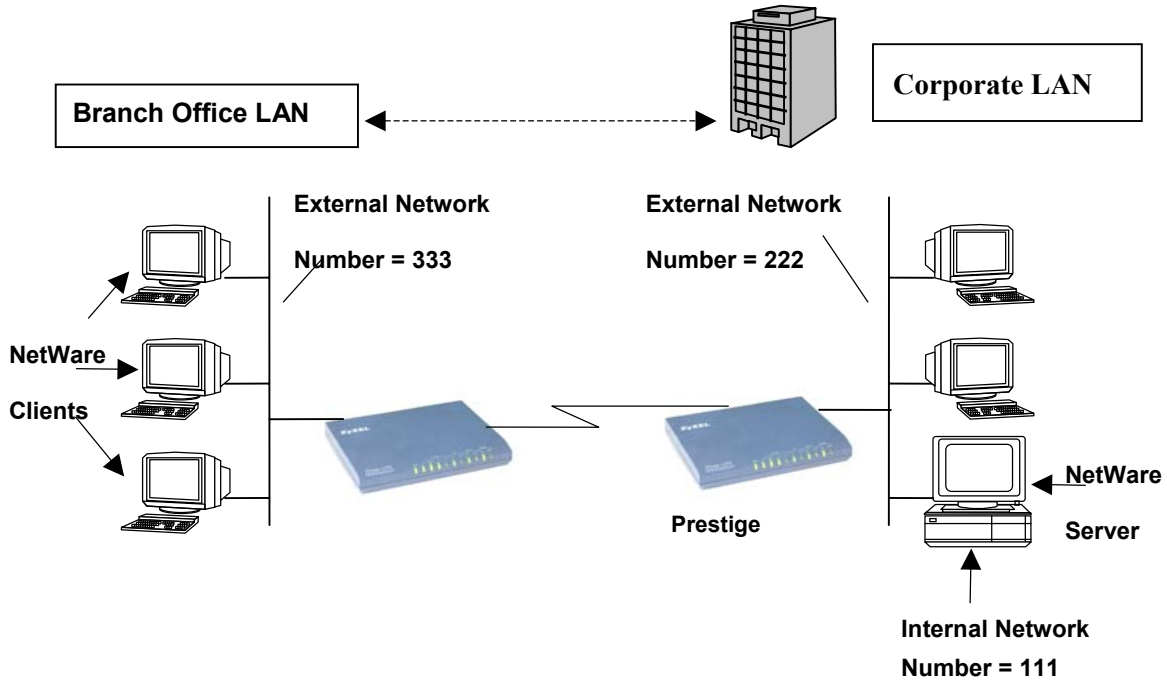
The following table describes the Novell IPX Ethernet Setup Menu.

Table 6-1 Novell IPX Ethernet Setup Fields

Field	Description	Options
Seed Router	Determine if your Prestige is to act as a seed router.	Yes/No
Frame Type	Enable/Disable the individual frame type. Remember to enable only the ones that are actually used on your network.	802.2 802.3 Ethernet II SNAP
IPX Network #	If your Prestige is a seed router, enter a unique network number for each frame type enabled.	

Press [Enter] at the message [Press ENTER to Confirm ...] to save your configuration, or press [Esc] at any time to cancel.

6.5 LAN-to-LAN Application with Novell IPX



A typical LAN-to-LAN application is to use your Prestige to call from a branch office to the corporate headquarters to enable the stations in the branch office to access the NetWare servers at the headquarters, as depicted in the figure below.

Figure 6-4 LAN-to-LAN Application with Novell IPX

6.5.1 IPX Remote Node Setup

Follow the procedure in *Chapter 5* to configure the protocol-independent parameters in Menu 11.1 - Remote Node Profile. For the IPX-specific parameters in Menu 11.3 - Remote Node Network Layer Options follow the instructions below. If you want the Prestige to receive incoming calls, you must also configure the default dial-in parameters in Menu 13.

To edit Menu 11.3 - Remote Node Network Layer Options shown below, follow these steps:

- Step 1.** In Menu 11.1, make sure **IPX** is among the protocols in the Route field. (The Route field should display Route = IPX or Route = IP + IPX.)
- Step 2.** Move the cursor to the **Edit IP/IPX/Bridge** field, then press the space bar to select **Yes** and press [Enter] to open Menu 11.3 - Network

```

Menu 11.3 - Remote Node Network Layer Options

IP Options:
Rem IP Addr:
Rem Subnet Mask= N/A
My WAN Addr= N/A
Single User Account= N/A
  Server IP Addr= N/A
Metric= N/A
Private= N/A
RIP Direction= N/A
  Version= N/A

IPX Options:
Dial-On-Query= No
Rem LAN Net #= 00000000
My WAN Net #= 00000000
Hop Count= 1
Tick Count= 2
W/D Spoofing(min)= 3
SAP/RIP Timeout(min)= 3

Bridge Options:
Dial-On-Broadcast= N/A
Ethernet Addr Timeout(min)= N/A

Enter here to CONFIRM or ESC to CANCEL:

```

Layer Options.

Figure 6-5 Menu 11.3 - Remote Node Novell IPX Options

The table below describes the IPX-specific parameters of the remote node setup.

Table 6-2 Remote Node Novell IPX Options

Field	Description	Option
Dial-On-Query	This field is necessary for your Prestige on the client side. When set to Yes , any Get Service SAP or RIP broadcasts will trigger your Prestige to make a call to that remote node.	Yes/No
Rem LAN Net #	In this field, enter the internal network number of the NetWare server on the remote LAN.	
My WAN Net #	In this field, enter the network number of the ISDN link. If you leave this field as 00000000 , your Prestige will determine automatically the network number through negotiation with the PPP peer.	00000000 (default)
Hop Count	This field indicates the number of intermediate networks that must be passed through to reach the remote node.	1 (default)
Tick Count	This field indicates the time-ticks required to reach the remote node.	2 (default)
W/D Spoofing (min)	This field is for the Prestige on the server side. Your Prestige can spoof a response to a server's WatchDog request after the connection is dropped. In this field, type in the time (number of minutes) that you want your Prestige to spoof the WatchDog response.	
SAP/RIP Timeout (min)	This field indicates the amount of time that you want your Prestige to maintain the SAP and RIP entries learned from this remote node in its internal tables after the connection has been dropped. If this information is retained, then your Prestige will not have to get the SAP information when the line is brought back up. Enter the time (number of minutes) in this field.	
Once you have completed filling in the Network Layer Options Menu, press [Enter] to return to Menu 11.1. Then press [Enter] at the message [Press ENTER to Confirm] to save your configuration, press [Esc] to cancel.		

6.5.2 IPX Static Route Setup

Similar to IP, IPX static routes tell the Prestige how to reach servers beyond a remote node before a connection to that remote node is established.

From Menu 12, select two, then select one of the IPX Static Routes to open Menu 12.2.1 - Edit IPX Static Route, as shown below.

```
Menu 12.2.1 - Edit IPX Static Route

Route #= 11
Server Name= ?
Active= Yes
Network #= ?
Node #= 000000000001
Socket #= 0451
Type #= 0004
Hop Count= 2
Tick Count= 3
Gateway Node= 1

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

Figure 6-6 Menu 12.2 - Edit IPX Static Route

The following table contains the instructions on how to configure the Edit IP Static Route Menu.

Table 6-3 Edit IPX Static Route Menu Fields

Field	Description
Server Name	In this field, enter the name of the server. This must be the <i>exact</i> name configured in the NetWare server.
Network #	This field contains the internal network number of the remote server that you wish to access. [00000000] or [FFFFFFFF] are reserved.
Node #	This field contains the address of the node on which the server resides. If you are using a Novell IPX implementation, this value is [000000000001].
Socket #	This field contains the socket number on which the server will receive service requests. The default for this field is hex [0451].
Type #	This field identifies the type of service the server provides. The default for this field is hex [0004].
Gateway Node	In this field, enter the number of the remote node that is the gateway for this static route.
Hop Count and Tick Count	These two fields have the same meaning as those in the Ethernet setup.
Once you have completed filling in the menu, press [Enter] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] to cancel to cancel.	

Chapter 7

Bridging Setup

This chapter shows you how to configure the bridging parameters of your Prestige.

7.1 Bridging in General

Bridging bases the forwarding decision on the MAC (Media Access Control), or hardware, address, while routing does it on the network layer (IP or IPX) address. Bridging allows the Prestige to transport packets of network layer protocols that the Prestige does not route, e.g., SNA, from one network to another. The caveat is that, compared to routing, bridging generates more traffic for the same network layer protocol and it also demands more CPU cycles and memory.

For efficiency reason, do *not* turn on bridging unless you need to support protocols other than IP and IPX on your network. For IP and IPX, enable the respective routing if you need it; do not bridge what the Prestige can route.

7.2 Bridge Ethernet Setup

Basically, all non-local packets are bridged to the WAN; however, your Prestige applies special handling for certain IPX packets to reduce the number of calls, depending on the setting of the **Handle IPX** field.

From Menu 3 - Ethernet Setup, enter option **Bridge Setup** and Menu 3.4 - Bridge Ethernet Setup displays as shown below.

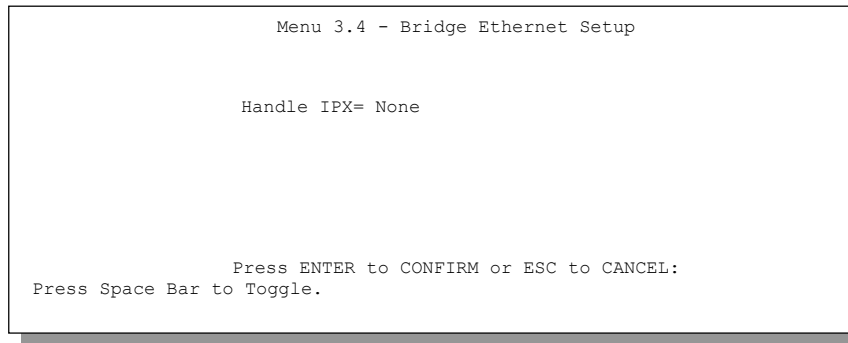


Figure 7-1 Menu 3.5 - Bridge Ethernet Setup

The following table describes how to configure the **Handle IPX** field in Menu 3.5.

Table 7-1 Bridge Ethernet Setup Menu - Handle IPX Field Configuration

Handle IPX Field (Menu 3.5)	Description
None	When there is no IPX traffic on the LAN or when you do not want to apply any special handling for IPX.
Client	When there are only client workstations on the LAN. RIP and SAP (Service Advertising Protocol) response packets will not trigger calls.
Server	When there are only IPX servers on the LAN. No RIP or SAP packets will trigger calls. In addition, during the time when the line is down, your Prestige will reply to watchdog messages from the servers on behalf of remote clients. The period of time that your Prestige will do this is linked to the Ethernet Address Timeout parameter in each remote node (see Remote Node Configuration). When a remote Ethernet address is aged out, there is no need to maintain its connection to the IPX server.

If there are both clients and servers on the LAN, and the local clients will access the remote servers, set this field to **Server** but turn on the **Dial-On-Broadcast** parameter in Menu 11.3 to allow the client queries to trigger calls.

7.2.1 Remote Node Bridging Setup

Follow the procedure in *Chapter 5* to configure the protocol-independent parameters in Menu 11.1 - Remote Node Profile. For bridging-specific parameters, you need to configure Menu 11.3 - Remote Node Network Layer Options.

To setup Menu 11.3 - Remote Node Network Layer Options, follow these steps:

Step 1. In Menu 11.1, make sure the **Bridge** field is set to **Yes**.

Step 2. Move the cursor to the **Edit IP/IPX/Bridge** field, then press the space

```
Menu 11.3 - Remote Node Network Layer Options

IP Options:
Rem IP Addr:
Rem Subnet Mask= N/A
My WAN Addr= N/A
Single User Account= N/A
  Server IP Addr= N/A
Metric= N/A
Private= N/A
RIP Direction= N/A
  Version= N/A

IPX Options:
Dial-On-Query= No
Rem LAN Net #= 00000000
My WAN Net #= 00000000
Hop Count= 1
Tick Count= 2
W/D Spoofing(min)= 3
SAP/RIP Timeout(min)= 3

Bridge Options:
Dial-On-Broadcast= No
Ethernet Addr Timeout(min)= 0

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

bar to select **Yes** and press [Enter] to open Menu 11.3 - Network Layer Options.

Figure 7-2 Menu 11.3 - Remote Node Bridging Options

The following table describes the bridging-specific parameters in the Remote Node Profile and Network Layers menus.

Table 7-2 Remote Node Network Layers Menu Bridge Options

Field	Description
Bridge	Make sure this field is set to Yes .
Edit IP/IPX/Bridge	Press the space bar to change it to Yes and press Enter] to go to the Network Layer Options Menu.
Dial-On-Broadcast	This field is necessary for your Prestige on the caller side LAN. When set to Yes , any broadcasts coming from the LAN will trigger your Prestige to make a call to this remote node. If it is set to No , your Prestige will not make the outgoing call.
Ethernet Addr Timeout (min)	In this field, enter the time (number of minutes) that you wish your Prestige to retain the Ethernet Addr information in its internal tables while the line is down. If this information is retained, your Prestige will not have to recompile the tables when the line is brought back up.
Once you have completed filling in the Network Layer Options Menu, press [Enter] to return to Menu 11.1. Then press [Enter] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] to cancel.	

7.3 Bridge Static Route Setup

Similar to network layer static routes, a bridging static route tells the Prestige about the route to a node before a connection is established. You configure bridge static routes in Menu 12.3.1, by pressing 3 in menu 12 and then selecting

```
Menu 12.3 - Bridge Static Route Setup
1. _____
2. _____
3. _____
4. _____

Enter selection number:
```

one of the bridge static routes as shown below.

Figure 7-3 Menu 12.3 - Bridge Static Route Setup

```
Menu 12.3 - Edit Bridge Static Route

Route #: 21
Route Name=
Active= No
Ether Address= ?
IP Address=
Gateway Node= 1

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

Figure 7-4 Menu 12.3.1 - Edit Bridge Static Route

The following table describes the Bridge Static Route Menu.

Table 7-3 Bridge Static Route Menu Fields

Field	Description
Route Name	Enter a name for the bridge static route for identification purposes.
Active	Activate/deactivate the static route.
Ether Address	Enter the MAC address of the destination machine that you wish to bridge the packets to.
IP Address	If available, enter the IP address of the destination machine that you wish to bridge the packets to.
Gateway Node	Enter the number of the remote node that is the gateway of this static route. When a packet's destination Ethernet (MAC) address matches the value entered above, it will trigger a call to this remote node.
Once you have completed filling in this menu, press [Enter] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] to cancel.	

Chapter 8

Dial-in Server Configuration

You can configure your Prestige to receive calls from remote dial-in users, e.g., telecommuters, as well as remote nodes. There are several differences between dial-in users and remote nodes, as summarized in the table below.

Table 8-1 Remote Dial-in Users/Remote Nodes Comparison Chart

Remote Dial-in Users	Remote Nodes
Your Prestige will only answer calls from remote dial-in users; it will not make calls to them.	Your Prestige can make calls to and receive calls from the remote node.
All remote dial-in users share one common set of parameters, as defined in the Default Dial In Setup (Menu 13).	Each remote node can have its own set of parameters such as Bandwidth On Demand, Protocol, Security, etc.

This chapter discusses how to setup default dial-in parameters for both remote node and remote dial-in users. The following sections give two examples of how your Prestige can be configured as a dial-in server.

Due to memory constraints, your Prestige can only store a finite number of users locally. If there are more remote dial-in users than what Prestige can support locally, you can use an external RADIUS server to provide authentication service. For details on using a RADIUS server, see the *Using RADIUS Authentication* section in *Chapter 13 - System Security*.

8.1 Remote Access Server

Telecommuting enables people to work at remote sites and yet still have access to the resources in the business office. Typically, a telecommuter will use a client workstation with TCP/IP and dial-out capabilities, e.g., a Windows PC or a Macintosh. For telecommuters to call in to your Prestige, you need to configure a dial-in user profile for each telecommuter. Additionally, you need to configure the Default Dial-In Setup to set the operational parameters for all dial-in users.

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

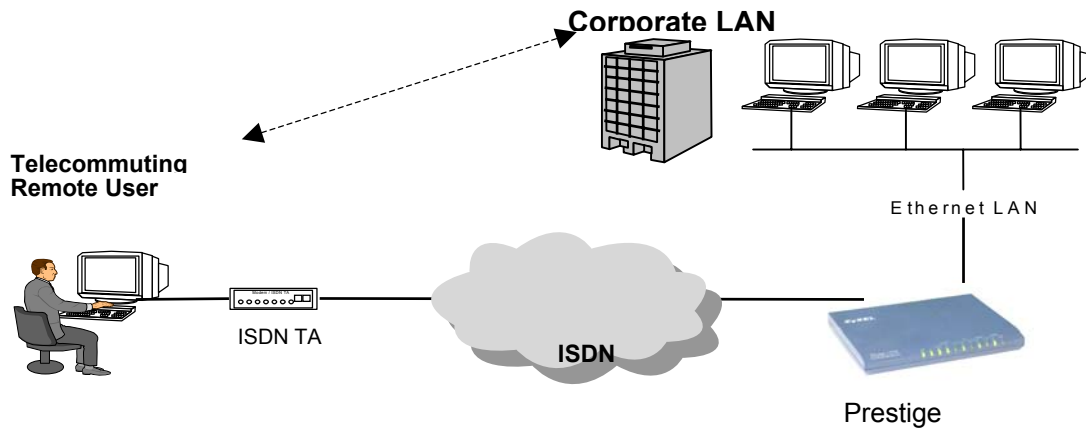
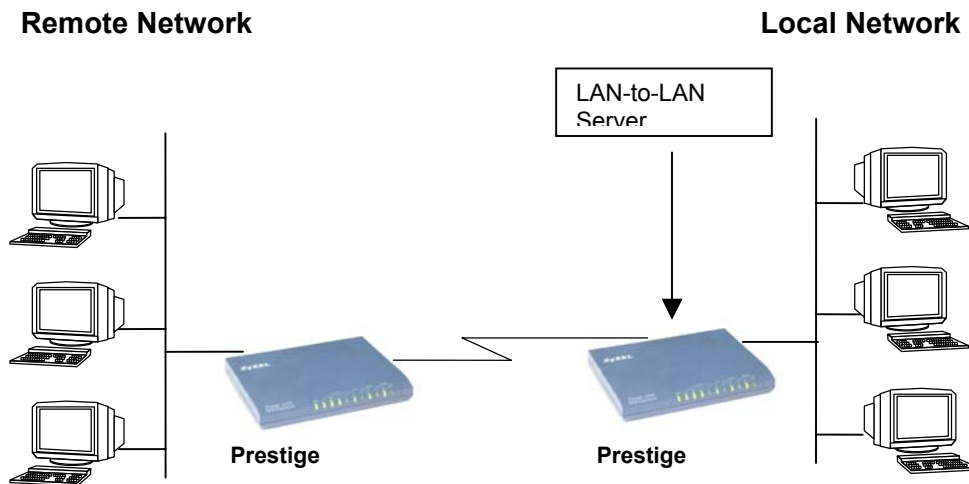


Figure 8-1 Example of Telecommuting

8.2 LAN-to-LAN Server Application

Your Prestige can also be used as a dial-in server for LAN-to-LAN application to provide access for the workstations on a remote network. For your Prestige to be set up as a LAN-to-LAN server, you need to configure the Default Dial-In Setup to set the operational parameters for incoming calls. Additionally, you must create a remote node for the router on the remote network (see *Chapter 5 - Remote Node Configuration*).



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

Figure 8-2 Example of a LAN-to-LAN Server Application

8.3 Default Dial-In Setup

This section covers the default dial-in parameters. The parameters in Menu 13 affect incoming calls from both remote dial-in users, and remote nodes until authentication is completed. Once authentication is completed and if it matches a

```
Menu 13 - Default Dial-in Setup

Telco Options:                               IP Address Supplied By:
  CLID Authen= None                          Dial-in User= Yes
                                              IP Pool= No
                                              IP Start Addr= N/A
                                              IP Count(1,2)= N/A

PPP Options:
  Recv Authen= CHAP/PAP                     IPX Net Num Supplied By:
  Compression= Yes                          IPX Pool= No
  Mutual Authen= No                         IPX Start Net Num= N/A
  PAP Login= N/A                             IPX Count(2,16)= N/A
  PAP Password= N/A

Multiple Link Options:
  Max Trans Rate= 128

Callback Budget Management:                  Session Options:
  Allocated Budget(min)=                    Edit Filter Sets= No
  Period(hr)=                               Idle Timeout= 300

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

remote node, your Prestige will use parameters from that particular remote node.

Figure 8-3 Menu 13 – Default Dial-in Setup

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

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

Table 8-2 Default Dial-in Setup Fields

Field	Description	Option
Telco Options: CLID Authen	This field sets the CLID authentication parameter for all incoming calls. There are three options for this field: <ul style="list-style-type: none"> ● None - No CLID is required. ● Required – CLID must be available, or the Prestige will not answer the call. ● Preferred - If the CLID is available then CLID will be used; otherwise, authentication is performed in PPP negotiation. 	None Required Preferred
PPP Options:		
Recv. Authen	This field sets the authentication protocol for incoming calls. For security reason, setting authentication to none is strongly discouraged. Options for this field are: <ul style="list-style-type: none"> ● CHAP/PAP - Your Prestige will try CHAP first, but PAP will be used if CHAP is not available. ● CHAP – Use CHAP only. ● PAP – Use PAP only. ● None – Your Prestige tries to acquire CHAP/PAP first, but no authentication is required if CHAP/PAP is not available. 	CHAP/PAP CHAP PAP None
Compression	Turn on/off Stac Compression. The default for this field is Off .	On Off
Mutual Authen	Some vendors, e.g., Cisco, require mutual authentication, i.e., the node that initiates the call will request a user name and password from the far end that it is dialing to. If the remote node requires mutual authentication, set this field to Yes .	Yes/No
PAP Login	This field is applicable only if the Mutual Authen . Field is set to Yes . Enter in the login name to be used to	

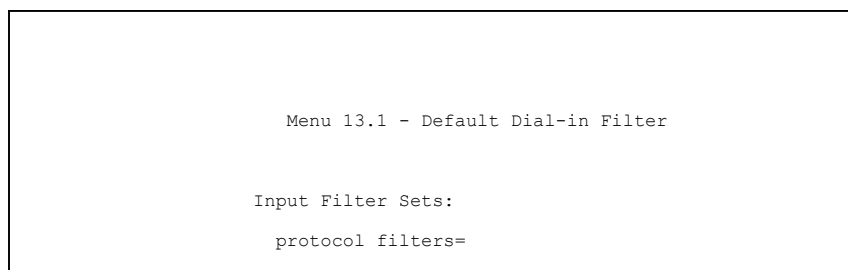
	respond to the far end's PAP authentication request. This field does not apply to CHAP authentication.	
PAP Password	This field is applicable only if the Mutual Authen. Field is set to Yes . Enter in the PAP password to be used to respond to the far end's authentication request. This field does not apply to CHAP authentication.	
Multiple Link Options:		
Max Trans Rate	Enter the maximum data transfer rate between your Prestige and the remote dial-in user. 64 - At most, one B channel is used. 128 - A maximum of two channels can be used.. When the Prestige calls back to the remote dial-in user, the maximum data transfer rate is always 64 .	64/128
Callback Budget Management:		
Allocated Budget (min)	This field sets the budget callback time for all the remote dial-in users. The default for this field is 0 for no budget control.	Default = 0
Period (hr)	This field sets the time interval to reset the above callback budget control.	
IP Address Supplied By:		
Dial-in User	If set to Yes , the Prestige will allow a remote host to specify its own IP address. If set to No , the remote host must use the IP address assigned by your Prestige from the IP pool, configured below. This is to prevent the remote host from using an invalid IP address and potentially disrupting the whole network.	(Default = Yes) Yes/No
IP Pool	This field tells your Prestige to provide the remote host with an IP address from the pool. This field is required if Dial-In IP Address Supplied By: Dial-in User is set to No . You can configure this field even if Dial-in User is set to Yes , in which case your Prestige will accept the IP address if the remote peer specifies one; otherwise, an IP address is assigned from the pool.	Yes/No (Default = No)

IP Pool: IP Start Addr	This field is applicable only if you selected Yes in the Dial-In IP Address Supplied By: IP Pool field. The IP pool contains contiguous IP addresses and this field specifies the first one in the pool.	
IP Count (1,2)	In this field, enter the number (1 or 2 ,) of addresses in the IP Pool. For example, if the starting address is 192.168.135.5 and the count is 2, then the pool will have 192.68.135.5 and 192.68.135.6	1, 2
IPX Net. Num. Supplied By:		
IPX Pool	This field tells your Prestige to provide the remote host with an IPX network number from the pool. Otherwise, your Prestige will generate a random IPX network number.	Yes/No (Default = No)
IPX Start Net Num	This field is applicable only if you selected Yes in the Dial-In IPX Net. Num. Supplied By: IPX Pool field. The IPX pool contains contiguous IPX network numbers and this field specifies the first one in the pool.	
IPX Count (2,16)	Enter the number (2 - 16) of network numbers in the IPX Pool. For example, if the starting number is 12345678, and the count is 2, then the IPX pool will have 12345678 and 12345679.	2 to 16
Session Options: Edit Filter Sets	Press Yes , then [Enter] to edit the filter sets. Keep in mind that the filter set(s) will only apply to remote dial-in users but not the remote nodes. Note that spaces and [-] symbol, are accepted in this field. For more information on customizing your filter sets, see <i>Chapter 9 - Filter Configuration</i> . The default is blank, i.e., no filters.	Default = blank
Once you have completed filling in Menu 13 - Default Dial-in Setup, press [Enter] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] at any time to cancel.		

8.3.1 Default Dial-in Filter

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

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



see Chapter 9.

Figure 8-4 Default Dial-in Filter

8.4 Dial-In Users Setup

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

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

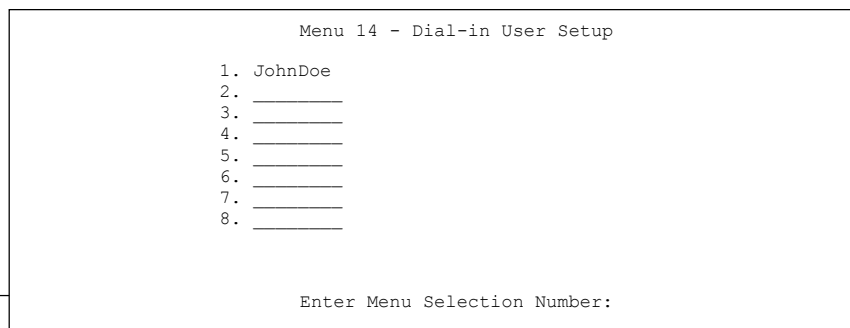


Figure 8-5 Menu 14 - Dial-in User Setup

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

```
Menu 14.1 - Edit Dial-in User

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

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

Figure 8-6 Edit Dial-in User

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

Table 8-3 Edit Dial-in User Menu Fields

Field	Description	Option
User Name	This is a required field. This will be used as the login name for authentication. Choose a descriptive word for login, for example, [JohnDoe].	
Active	You can disallow dial-in access to this user by setting this field to Inactive . Inactive users are displayed with a [-] (minus sign) at the beginning of the name in Menu 14.	Active Inactive
Password	Enter the password for the remote dial-in user.	
Callback	This field determines if your Prestige will allow call back to this user upon dial-in. If this option is enabled, your Prestige will call back to the user if requested. In such a case, your Prestige will disconnect the initial call from this user and dial back to the specified callback number (see below). <ul style="list-style-type: none"> ● No - The default is no callback. ● Optional - The user can choose to disable callback. ● Mandatory - The user can not disable callback. 	Default= No No Optional Mandatory
Phone # Supplied by Caller	This option allows the user to specify the call back telephone number on a call-by-call basis. This is useful when your Prestige returns a call back to a mobile user at different numbers, e.g., a sales rep. in a hotel. <ul style="list-style-type: none"> ● If the setting is Yes, the user can specify and send to the Prestige the callback number of his/her choice. ● The default is No, i.e., your Prestige always calls back to the fixed callback number. 	Default= No Yes No
Callback Phone #	If Phone # Supplied by Caller is No , then this is a required field. Otherwise, a N/A will appear in the field. Enter the telephone number to which your Prestige will call back.	

Table 8-4 Edit Dial-in User Menu Fields (continued)

Field	Description	Option
Rem CLID	If you enable CLID Authen field in Menu 13, then you need to specify the telephone number from which this user calls. Your Prestige will check the CLID in the incoming call against the CLIDs in the database. If they do not match and CLID Authen is Required, your Prestige will not answer the call.	
Idle Time-out	Enter the idle time (in seconds). This time-out determines how long the dial-in user can be idle before your Prestige disconnects the call when the Prestige is calling back. Idle time is defined as the period of time where there is no data traffic between the dial-in user and your Prestige. The default is 300 seconds (5 minutes).	Default=300 seconds
Once you have completed filling in Menu 14.1 - Edit Dial-in User, press [Enter] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] at any time to cancel.		

8.4.1 CLID Authentication

CLID (Calling Line IDentification) authentication affords you the security of limiting a user to only initiate connections from a fixed location. The Prestige uses the caller ID sent by the switch to match against the CLIDs in the database. Please note that for CLID authentication to work on the Prestige, your telephone company must support caller ID.

8.4.2 Callback

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

The other is ease of accounting. For instance, your company pays for the connection charges for telecommuting employees and you use your Prestige as the dial in server. When you turn on the callback option for the dial-in users, all

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

8.5 Multiple Servers behind 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 inside network appear as a single machine to the outside world. A service is identified by the port number, e.g., web service is on port 80 and FTP on port 21.

As an example, if you have a web server at 192.168.1.2 and an FTP server 192.168.1.3, then you need to specify for port 80 (web) the server at IP address 192.168.1.2 and for port 21 (FTP) another at IP address 192.168.1.3.

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.

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, Multiple Server Configuration**.

8.5.1 Configuring a Server behind SUA

Follow the steps below to configure a server behind SUA:

1. Enter 15 in the main menu to go to menu 15, Multiple Server Configuration.

2. Enter an index number in menu 15 to go to menu 15.1, SUA Server

```
Menu 15 - Multiple Server Configuration
Port #          IP Address
----          -
1.Default      0.0.0.0
2. 0           0.0.0.0
3. 0           0.0.0.0
4. 0           0.0.0.0
5. 0           0.0.0.0
6. 0           0.0.0.0
7. 0           0.0.0.0
8. 0           0.0.0.0

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

Configuration.

3. Enter the service port number in the Port # field and the inside IP address of the server in the IP Address field.
4. Press ENTER at the “Press ENTER to confirm ...” prompt to save your configuration after you define all the servers or press **ESC** at any time to cancel.

Figure 8-7 Multiple Server Configuration

The most often used port numbers are:

Table 8-5 Services vs. 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

Chapter 9

Advanced Phone Services

The Prestige 128+ supports a comprehensive set of advanced calling features known as Supplemental Services. These features include:

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

9.1 Getting Started

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

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

9.2 Setting Up Supplemental Phone Service

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

9.3 The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a “flash” key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manually tapping, if the duration is too long, it may be interpreted as hanging up by the Prestige.

9.4 Call Waiting

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

By default call waiting is disabled on both telephone ports, but can be enabled on either port from **Menu 2.1**.

9.4.1 How to use call waiting

The Call Waiting feature on your ISDN line works in exactly the same way as it does on a regular analog line (which almost everyone is familiar with). To put the

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

Dropping current call to switch to incoming/holding call.

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

Notes: An incoming caller receives a busy signal if

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

9.5 Three way calling

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

9.5.1 How To Use Three Way Calling

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

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

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

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

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

To drop yourself from the conference call:

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

9.6 Call Transfer

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

9.6.1 How To Use Call Transfer

Transferring an active call to a third party:

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

9.6.2 To Do A Blind Transfer:

- ◆ Once you have an active call (Caller A), press the flash key to put the existing call on hold and receive a dial tone.
- ◆ Dial the third party's telephone number (Caller B).

- ◆ Before Caller B picks up the call, you can transfer the call by pressing the flash key. The call is automatically transferred.

9.7 Call Forwarding

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

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

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

Table 9-1 Phone Flash Commands

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

#20#	Deactivate CFB
#21#	Deactivate CFU
#22#	Deactivate CFNR

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

Chapter 10

L2TP Support

This chapter shows how to reduce the cost of remote dial-up networking by taking advantage of the Internet using L2TP (Layer 2 Tunneling Protocol).

10.1 What is L2TP?

Tunneling is the key to L2TP (and other virtual dial-up services). With tunneling, protocol packets of one type of network are put inside or encapsulated in the protocol packets of another network for transport across that network. A tunnel has an entry point and an exit point that are essentially interfaces between two different types of networks, although they are defined in software.

Dial-up users typically use the PPP (Point-to-Point Protocol) for an Internet connection. PPP is a layer 2 protocol that frames data so it can be sent across a dial-up connection. The protocol allows users to run TCP/IP software such as Web browsers as if they were directly connected to the Internet. In fact, user TCP/IP packets are put into PPP frames for transport across the dial-up link to an ISP. The ISP then extracts the TCP/IP packets and forwards them on the Internet. L2TP enhances PPP by granting a means for a remote user to extend a PPP link across the Internet all the way to a corporate site. In essence, a tunnel is established across the Internet from the ISP to a corporate site and frames are transmitted through the tunnel. Once the tunnel is set up, the ISP is essentially out of the picture and the user communicates to the corporate network over what appears to be a direct dial-up connection.

L2TP authenticates the endpoints but does not encrypt the packets as they travel across the Internet.

10.2 Advantages of L2TP:

- ◆ Users can take advantage of the low cost of the Internet. Instead of making a long-distance call to connect directly with the corporate site's remote access server, remote users dial in to a local ISP and use the Internet to handle all long-distance connections.
- ◆ The protocol provides *virtual dial-up* because the user doesn't really dial in to the corporate network, but when the connection is complete, it's as if he does. This enables outsourcing of dial-up services to the ISP to support remote users.
- ◆ Because PPP framing is used, remote users can access corporate sites using a variety of protocols such as IP, IPX and so on.
- ◆ The corporate site assigns an IP address to a remote client instead of the ISP, allowing it to control the assignment of IP addresses.
- ◆ L2TP provides end-system transparency, meaning that the remote user does not require any special software to use the service in a secure way.
- ◆ An organization can control the authentication of users instead of the ISP.

10.3 How L2TP Works

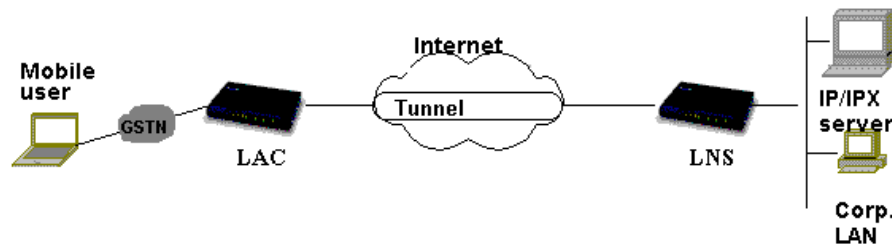


Figure 10-1 How L2TP works

In L2TP terminology, the NAS (network access server) at the ISP is the L2TP client and is called a LAC (L2TP Access Concentrator). The Prestige at the corporate LAN is the server and is called a LNS (L2TP Network Server). A tunnel exists between the LAC and the LNS. The (mobile) user utilizes L2TP for the Internet tunnel. In simple terms, a LAC forwards packets and must have a GSTN connection; a LNS negotiates PPP with a user but does not necessarily have a GSTN connection. Obviously, however, both the LAC and the LNS must have access to the Internet. Both the LNS and LAC are called an L2TP endpoint. After call connection, the user and the LNS negotiate PPP in exactly the same fashion as a direct connection. However, instead of interfacing to the physical device, e.g., ISDN, the LNS is talking to an L2TP tunnel, i.e., a logical device. Please refer to the diagram above.

10.3.1 LNS (L2TP Network Server)

The LNS terminates a PPP connection - it handles the server side of the L2TP protocol. Since L2TP runs on top of IP, the LNS may have only a single LAN or WAN interface yet still be able to terminate calls arriving at any LAC's full range of PPP interfaces (async, synchronous ISDN, V.120, etc.).

10.3.2 LAC (L2TP Access Concentrator)

The LAC relays the traffic between the LNS and the user. It may tunnel any protocol carried within PPP.

For incoming calls, the LAC may negotiate LCP and authentication to discover the apparent identity of the user; or it may use other mechanism, e.g., CLID. In the case of PPP authentication, the LAC only performs partial negotiation, i.e., receiving PAP request or sending CHAP challenge and receiving response. Once the user name (and hence the realm) is know, the LAC forwards all negotiation data thus far gathered (LCP and authentication) to the LNS.

Note that a Prestige can be a LAC for one connection and a LNS for another at the same time.

The remote user dials in to an ISP. A tunnel is then set up from the ISP across the Internet to a corporate gateway server. Once the tunnel is set up, mobile users access the corporate network as if they had dialed directly into that network.

10.3.3 Internet-based tunnel process:

1. The remote user dials the ISP and the ISP collects logon information from the user.
2. The ISP inspects the user name in the logon information and determines whether a virtual dial-up service is required. The ISP maintains a database (endpoint table) for a corporation that associates the user name (the realm or domain name) with a specific endpoint (i.e., the corporate gateway).
3. The ISP establishes a tunnel by contacting the corporate gateway.
4. The authentication information that was initially collected from the remote user in Step 1 is forwarded to the corporate gateway. Now the remote user is authenticated by the corporate LNS.
5. Now the user has an end-to-end PPP link.

At this point, the connection between the remote user and the corporate network is like any PPP connection. When the ISP receives frames from the remote user over the PPP link, they are encapsulated in L2TP, and forwarded over the tunnel to the LNS. The corporate gateway receives these frames, strips L2TP, and processes them as normal incoming PPP frames.

10.4 The Prestige and L2TP

We will describe scenarios where we use the Prestige as a LNS and/or LAC for both outgoing and incoming calls.

10.4.1 Endpoint Table

Both the LNS and the LAC refer to this table to find the tunnel endpoint. Please note that a receiving L2TP endpoint must have a fixed, globally unique IP address while an initiating endpoint may have a dynamic IP address.

10.4.2 Prestige as LNS

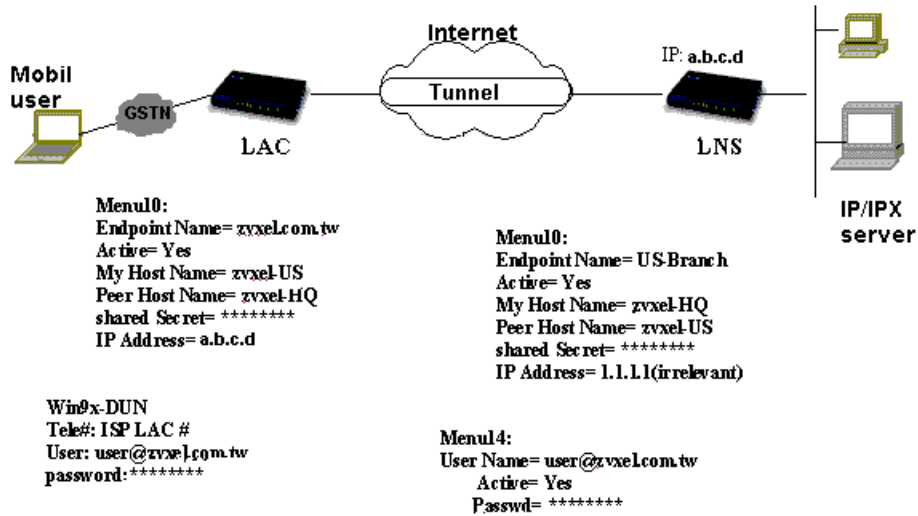


Figure 10-2 Prestige as LNS

Incoming Call

In this scenario, the ISP is the LAC. The LAC will search for the **Endpoint Name** (domain or realm name) in its endpoint table to know whether it should create a tunnel or not (i.e., ordinary Internet access). In the above example, a tunnel is created between the Prestige LNS and the LAC. The user name and password in Win 95's Dial-up-Networking must be defined in menu 14.1, the profile for this Dial-in User, so that PPP authentication can take place directly between the user and the Prestige LNS while the LAC (ISP) remains transparent to the process. An incoming L2TP call to the LNS is handled in exactly the same

```
Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe
Active= Yes
Call Direction= Outgoing
Tunneling Mode= Direct
Endpoint Index= 1
Incoming:
Rem Login= N/A
Rem Password= N/A

Route= IPX
Bridge= No
Edit PPP Options= No
Rem IP Addr= 0.0.0.0
Edit IP/IPX/Bridge= No
Telco Option:
Allocated Budget (min)= 0
```

way as a GSTN call.

Figure 10-3 SMT Menu 11.1

Outgoing Call.

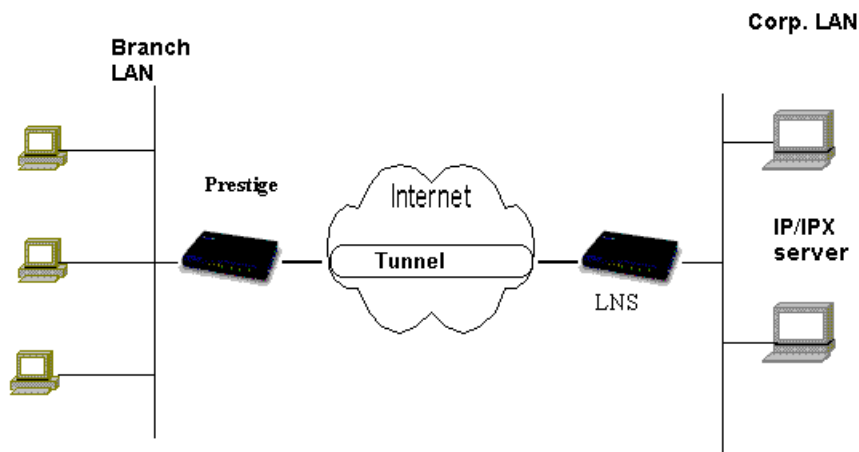
For a LNS to initiate an outbound L2TP call, it requires a remote node in the same fashion as a regular GSTN call. Moreover, you need to specify a mode of tunneling i.e., **None**, **Proxy** or **Direct**, and if tunneling is requested, you need to specify the L2TP endpoint. This can be done in Menu 11.1 – Remote Node Profile.

Table 10-1 SMT Menu 11.1- Remote Profile L2TP fields

Field	Description
Tunneling mode	Select mode of Layer 2 Tunneling Protocol (L2TP in menu 10). Choices are None , Direct or Proxy .
Endpoint Index	This is the corresponding index number of the endpoint tunnel in Menu 10.

Direct mode

In **Direct** mode, you use two Prestiges directly to implement L2TP as illustrated.

**Figure 10-4 Prestiges in Direct mode**

The LAC (home or branch office Prestige) can log in to the ISP with the SUA feature enabled, and when traffic needs to reach the corporate IPX (NetWare) server, a tunnel will be created to the LNS. The LNS needs to have a static IP address from the Internet. This is because when the LAC tries to setup a tunnel to the corporate network, it needs to know the LNS's IP address. In the above example, the LAC must enter the IP address of the LNS. However, for the LNS,

since the LAC's IP address could be dynamically assigned each time a call is made to the ISP, the user can enter any IP address in this case i.e., it is irrelevant – see Figure 10-2. The LNS will accept the tunnel setup request from any IP address as long as **My Host Name** and **Shared Secret** are correct.

The relevant SMT menus are as follows. See Chapter 6 for more information on remote nodes. Four tunnel endpoint profiles can be defined in Menu 10.

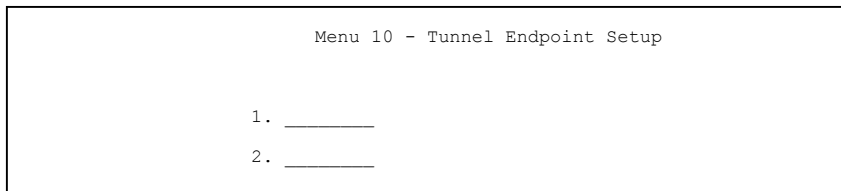


Figure 10-5 Menu 10 – Tunnel Endpoint Setup

Selecting one endpoint profile takes you to the following menu.

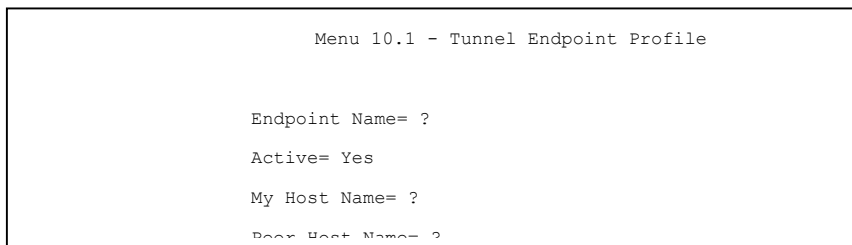


Figure 10-6 Menu 10.1 Tunnel Endpoint Profile

Table 10-2 Tunnel Endpoint Profile Fields

Field	Description
Endpoint Name	This tells the Prestige the far end of the desired tunnel.
Active	Select Yes to activate this endpoint node.
My Host Name	This is the name of the Prestige for L2TP authentication.

Peer Host Name	This is the name of the peer computer at the far end.
Shared Secret	This password must be the same for both endpoints.
IP Address	A receiving L2TP endpoint must have a fixed, globally unique IP address.

Proxy Mode

For the LNS in this case, choose **Proxy** for **Tunneling Mode** in menu 11.1 as the LNS is asking the LAC to place a call on its behalf. If outgoing calls are allowed and there is an idle phone line, the LAC will act as a proxy for the LNS. The menu 10.1 entries are the same as described above.

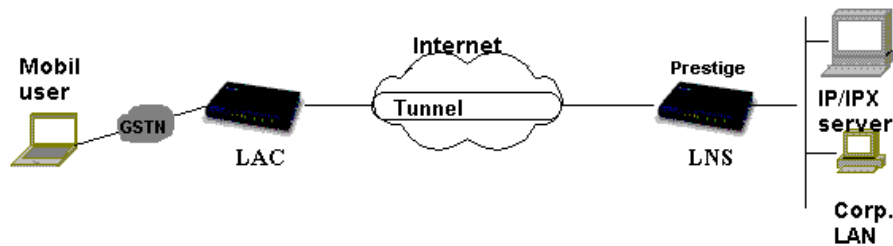


Figure 10-7 Prestige in Proxy mode.

10.4.3 Prestige as LAC

Endpoint Name in Menu 10.1 is the key setting for the LAC for both incoming and outgoing calls.

Incoming Call

For calls to a LAC, the long form of NAI (Network Access Identifier) is used. The NAI is in the form of *username@realm*, where *realm* is typically a domain name, e.g., *user@zyxel.com.tw*. The realm is the key in the search of the endpoint. The LAC will search for the **Endpoint Name** in its endpoint table to know whether to create a tunnel or not. If the realm matches the name of one of the endpoints in the LAC, then the LAC handles this as a request for L2TP

tunneling. In Figure 10-2 above, *zyxel.com.tw* is entered as the **Endpoint Name** for the LAC in order to set up a tunnel to ZyXEL-HQ.

Outgoing Call

Here, the LNS asks the Prestige LAC to place a call on its behalf. If outgoing calls are allowed and there is an idle phone line, the LAC will place the call. In this scenario, the LAC acts as a proxy for the LNS.

Chapter 11

Filter Configuration

11.1 About Filtering

Your Prestige uses filters to decide whether or not to allow passage of a data packet and/or to make a call. There are two types of filters: data filters and call filters.

Data filters screen the data to determine if the packet should be allowed to pass. Data filters are further divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Call filters are used to determine if a packet should be allowed to trigger a call.

Outgoing packets must pass through the data filters before they encounter the call filters. Call filters are divided into two groups, the built-in call filters and user-defined call filters. Your Prestige has built-in call filters that prevent administrative, e.g., RIP and SAP (Service Advertising Protocol), packets from triggering calls. These filters are always enabled and not accessible to you. Your Prestige applies the built-in filters first and then the user-defined call filters, if applicable, as illustrated in the figure below, *Figure 11-1 Outgoing Packet Filtering Process*.

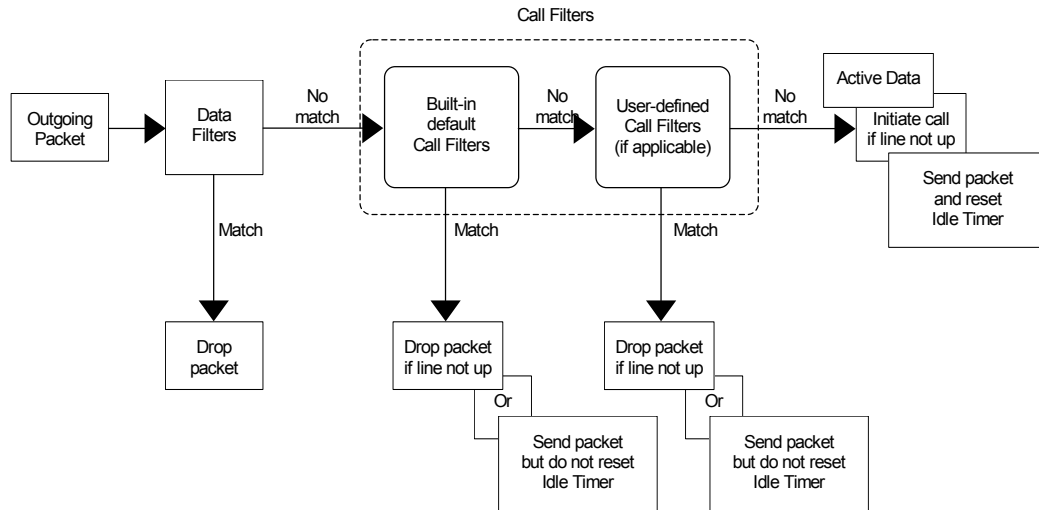


Figure 11-1 Outgoing Packet Filtering Process

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.

The Filter Structure of the Prestige

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

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

11.2 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 Set #      Comments      Filter Set #      Comments
-----
1                _____      7                _____
2                _____      8                _____
3                _____      9                _____
4                _____     10               _____
5                _____     11               _____
6                _____     12               _____

Enter Filter Set Number to Configure=
Edit Comments=
Press ENTER to CONFIRM or ESC to CANCEL:
```

Figure 11-2 Menu 21 - Filter Set Configuration

- Step 2.** Select the filter set you wish to configure (no. 1-12) and press [Enter].
- Step 3.** Enter a descriptive name or comment in the Edit Comments field and press Enter.
- Step 4.** Press [Enter] at the message: [Press ENTER to confirm] to open Menu 21.1 - Filter Rules Summary.

```

Menu 21.1 - Filter Rules Summary

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

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

```

Figure 11-3 Menu 21.1 - Filter Rules Summary

11.2.1 Filter Rules Summary Menu

This screen shows the summary of the existing rules in the filter set. The following tables contain a brief description of the abbreviations used in Menu 21.1.

Table 11-1 Abbreviations Used in the Filter Rules Summary Menu

Abbreviations	Description	Display
#	Refers to the filter rule number (1-6).	
A	Refers to Active.	[Y] means the filter rule is active. [N] means the filter rule is inactive.
Type	Refers to the type of filter rule. This shows GEN for generic, IP for TCP/IP and IPX for Novell IPX.	[GEN] for Generic [IP] for TCP/IP [IPX] for Novell IPX

**Table 11-2 Abbreviations Used in the Filter Rules Summary Menu
(continued)**

Abbreviations	Description	Display
Filter Rules	The filter rule parameters will be displayed here (see below).	
M	Refers to More.	[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. [D] means to drop the packet. [N] means check the next rule.
n	Refers to Action Not Matched	[F] means to forward the packet. [D] means to drop the packet. [N] means check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

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

Table 11-3 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 IPX, the following abbreviations listed in the following table will be used.

Table 11-4 Abbreviations Used If Filter Type Is IPX

Abbreviation	Description
PT	IPX Packet Type
SS	Source Socket
DS	Destination Socket

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

Table 11-5 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.

11.3 Configuring a Filter Rule

To configure a filter rule, enter its number in Menu 21.1 - Filter Rules Summary and press Enter to open Menu 21.1.1 for the rule.

There are three types of filter rules: TCP/IP, IPX and Generic. Depending on the type of rule, the parameters below the type will be different. Use the space bar to select the type of rule that you wish to create in the Filter Type field and press Enter to open the respective menu.

The network layer (TCP/IP and IPX) filters are collectively called protocol filters. When NAT/SUA (Network Address Translation/Single User Account) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the Prestige applies the protocol filters to the “native” IP address and port number before NAT/SUA for outgoing packets and after NAT/SUA for incoming packets. On the other hand, the generic, or device, filters are applied to the raw packets that appear on the wire.

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

11.3.1 TCP/IP Filter Rule

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

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

```
Menu 21.1.1 - TCP/IP Filter Rule

Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= No
IP Protocol= 0      IP Source Route= No
Destination: IP Addr=
              IP Mask=
              Port #= 0
              Port # Comp= None
Source: IP Addr=
        IP Mask=
        Port #= 0
        Port # Comp= None
TCP Estab= 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 11-4 Menu 21.1.1 - TCP/IP Filter Rule

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

Table 11-6 TCP/IP Filter Rule Menu Fields

Field	Description	Option
Active	This field activates/deactivates the filter rule.	Yes/No
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. This value must be between 0 and 255	0-255
IP Source Route	If Yes , the rule applies to packet with IP source route option; else the packet must not have source route option. The majority of IP packets do not have source route.	Yes/No
Destination: IP Addr	Enter the destination IP Address of the packet you wish to filter. This field is a don't-care if it is 0.0.0.0.	IP address
Destination: IP Mask	Enter the IP subnet mask to apply to the Destination: IP Addr.	Subnet mask
Destination: Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is a don't-care if it is 0.	0-65535
Destination: Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in Destination: Port #.	None/Less/Greater/Equal/Not Equal]
Source: IP Addr	Enter the source IP Address of the packet you wish to filter. This field is a don't-care if it is 0.0.0.0.	IP Address
Source: IP Mask	Enter the IP subnet mask to apply to the Source: IP Addr.	IP Mask
Source: Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is a don't-care if it is 0.	0-65535
Source: Port # Comp	Select the comparison to apply to the source port in the packet against the value given in Source: Port #.	Yes/No

Field	Description	Option
TCP Estab	This field is applicable only when IP Protocol field is 6, TCP. If yes, the rule matches only established TCP connections; else the rule matches all TCP packets.	Yes/No
More	If yes, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according the action fields. If More is Yes , then Action Matched and Action Not Matched will be N/A .	Yes / N/A
Log	Select the logging option from the following: <ul style="list-style-type: none"> ● None – No packets will be logged. ● Action Matched - Only packets that match the rule parameters will be logged. ● Action Not Matched - Only packets that do not match the rule parameters will be logged. ● Both – All packets will be logged. 	None Action Matched Action Not Matched Both
Action Matched	Select the action for a matching packet.	Check Next Rule Forward Drop
Action Not Matched	Select the action for a packet not matching the rule.	Check Next Rule Forward Drop
Once you have completed filling in Menu 21.1.1 - TCP/IP Filter Rule, press [Enter] at the message [Press Enter to Confirm] to save your configuration, or press [Esc] to cancel. This data will now be displayed on Menu 21.1 - Filter Rules Summary.		

11.3.2 Generic Filter Rule

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

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

To configure a generic rule, select Generic Filter Rule in the Filter Type field and

```
Menu 21.1.2 - Generic Filter Rule

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

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

press Enter to open Menu 21.1.2 - Generic Filter Rule, as shown below.

Figure 11-5 Menu 21.1.2 - Generic Filter Rule

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

Table 11-7 Generic Filter Rule Menu Fields

Field	Description	Default
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.	
Once you have completed filling in Menu 21.1.2 - generic Filter Rule, press [Enter] at the message [Press Enter to Confirm] to save your configuration, or press [Esc] to cancel. This data will now be displayed on Menu 21.1 - Filter Rules Summary.		

11.4 Novell IPX Filter Rule

This section shows you how to configure an IPX filter rule. IPX filters allow you to base the rules on the fields in the IPX headers.

To configure an IPX rules, select IPX Filter Rule from the Filter Type field and press Enter to open Menu 21.1.3 IPX Filter Rule, as shown in the figure below.

```
Menu 21.1.3 - IPX Filter Rule

Filter #: 1,1
Filter Type= IPX Filter Rule
Active= No
IPX Packet Type=
Destination: Network #=
              Node #=
              Socket #=
              Socket # Comp= None
Source: Network #=
          Node #=
          Socket #=
          Socket # Comp= None

Operation= 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 11-6 Menu 21.1.3 - IPX Filter Rule

The table below describes the IPX Filter Rule.

Table 11-8 IPX Filter Rule Menu Fields

Field	Description
IPX Packet Type	Enter the IPX packet type (1-byte in hexadecimal) you wish to filter. The popular types are (in hexadecimal): 01 - RIP 04 - SAP 05 - SPX (Sequenced Packet eXchange) 11 - NCP (Netware Core Protocol) 14 - Novell NetBIOS
Destination/Source Network #	Enter the destination/source network numbers (4-byte in hexadecimal) of the packet that you wish to filter.
Destination/Source Node #	Enter in the destination/source node number (6-byte in hexadecimal) of the packet you wish to filter.
Destination/Source Socket #	Enter the destination/source socket number (2-byte in hexadecimal) of the packets that you wish to filter.
Destination/Source Socket # Comp	Select the comparison you wish to apply to the destination/source socket in the packet against that specified above.
Operation	This field is applicable only if one of the Socket # fields is 0452 or 0453 indicating SAP and RIP packets. There are seven options for this field that specify the type of the packet. <ul style="list-style-type: none">● None.● RIP Request.● RIP Response.● SAP Request.● SAP Response.● SAP Get Nearest Server Request.● SAP Get Nearest Server Response

Once you have completed filling in Menu 21.1.3 - IPX Filter Rule, press [Enter] at the message [Press Enter to Confirm] to save your configuration, or press [Esc] to cancel. This data will now be displayed on Menu 21.1 - Filter Rules Summary.

Chapter 12

SNMP Configuration

12.1 About SNMP

SNMP (Simple Network Management Protocol) is a protocol for network management and monitoring. Your Prestige supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige through the network. Keep in mind that SNMP is only available if TCP/IP is configured on your Prestige.

12.2 Configuring SNMP

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

```
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 12-1 Menu 22 - SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 12-1 SNMP Configuration Menu Fields

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

Chapter 13

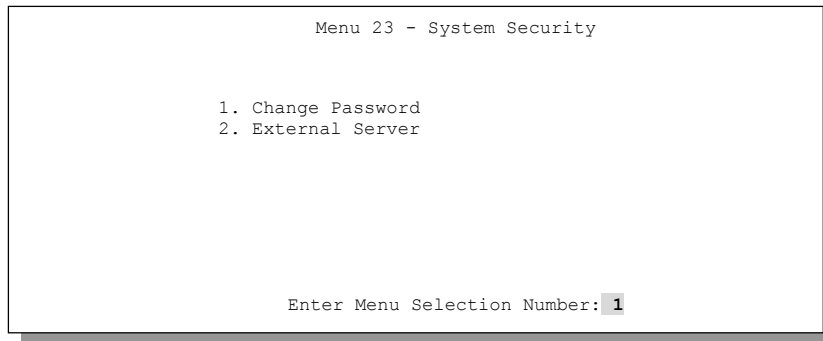
System Security

This chapter covers Menu 23, which is for you to change the system password and to configure an external authentication server.

13.1 Changing the System Password

To change the system password, following steps below:

Step 1. Select option **System Security** in the Main Menu to open Menu 23



– System Security as shown below.

Figure 13-1 Menu 23 - System Security

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

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

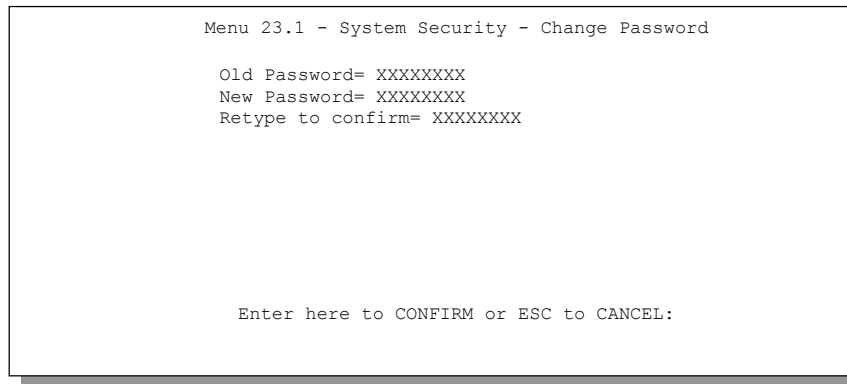


Figure 13-2 Menu 23.1 - System Security - Change Password

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

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

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

13.2 Using RADIUS Authentication

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

13.2.1 Installing a RADIUS Server

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

You can obtain the RADIUS server software, along with documentation, at <http://www.livingston.com/Tech/FTP/pub-le-radius.shtml> or <ftp://ftp.livingston.com/pub/le/radius/>

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

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

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

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

These changes add the support for CLID authentication, as described in the section below.

13.2.2 RADIUS Server Configuration

To configure the RADIUS server, select option 23, System Security, from the Main Menu to open Menu 23 - System Security. Select option 2, External Server from this menu to open Menu 23.2 - System Security - External Server, shown below. The radius authentication port has changed from 1645 to 1812. It is necessary to reboot your Prestige after changing the RADIUS port number before

```
Menu 23.2 - System Security - External Server

Authentication Server:
Active= No
Type: RADIUS
Server Address= ?
Port #= 1812
Key= ?

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

the change takes effect.

Figure 13-3 Menu 23.2 - System Security - External Server

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

Table 13-1 System Security - External Server Menu Fields

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

13.2.3 The Key Field

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

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

After you configure a RADIUS server, your Prestige will use it to authenticate all users that it can not find in its internal dial-up user list (*see* Menu 14)

13.2.4 Adding Users to the RADIUS Database

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

```
Joeuser Password = "joepassword"
```

13.2.5 Using RADIUS Authentication for CLID

To use RADIUS for CLID authentication, create a user record in the `users` file where the user name (the first field) is the telephone number, and the password (the second field) is always `Zyxel-CLID` (case-sensitive). The regular user name is put in a `User-Name` field. The following is an example of a CLID user record:

```
5551212 Password = "Zyxel-CLID"  
User-Name = "joeuser"  
Zyxel-Callback-Option = Mandatory  
Zyxel-Callback-Phone-Source = Preconfigured  
Dialback-No = "5551212"
```

Note that if CLID is turned off in your Prestige, you need to have a separate user record for `joeuser` so the regular user name/password mechanism still works.

Chapter 14

Telnet Configuration and Capabilities

14.1 About Telnet Configuration

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

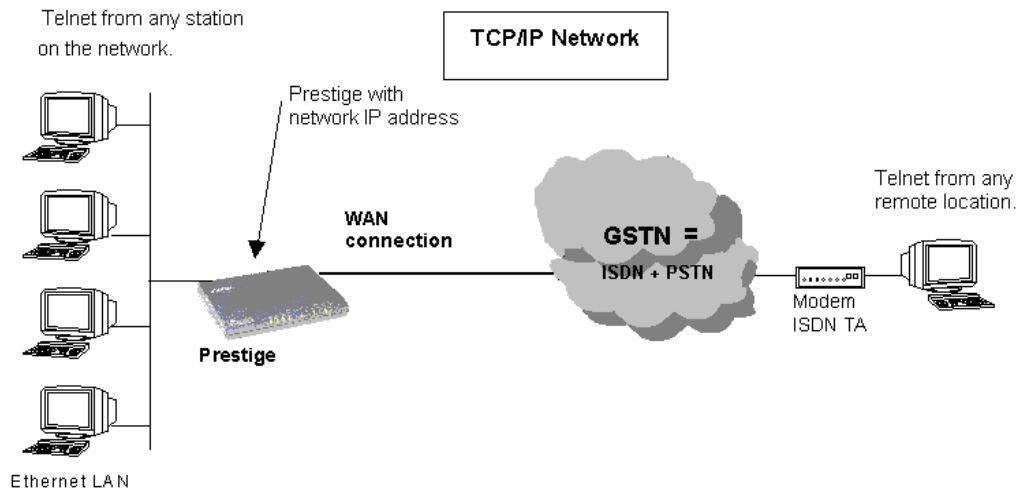


Figure 14-1 Telnet Configuration on a TCP/IP Network

If your Prestige is configured for IPX but not IP routing in Menu 1, telnet is still available provided you assign the Prestige a correct IP address and subnet mask. When IP routing is disabled, the Prestige can still function as a host.

14.2 Telnet Under SUA

When Single User Account (SUA) is enabled and an inside server is specified, telnet connections from the outside will be forwarded to the inside server. So to configure the Prestige via telnet from the outside, you must first telnet to the inside server, and then telnet from the server to the Prestige using its inside LAN IP address. If no insider server is specified, telnetting to the SUA's IP address will connect to the Prestige directly.

14.3 Telnet Capabilities

14.3.1 Single Administrator

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

14.3.2 System Timeout

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

Chapter 15

System Maintenance

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

Select menu 24 in the main menu to open Menu 24 - System Maintenance, as

```
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. Software Update
8. Command Interpreter Mode
9. Call Control

Enter Menu Selection Number:
```

shown below.

Figure 15-1 Menu 24 - System Maintenance

15.1 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 below. System Status is a tool that can be used to monitor your Prestige. Specifically, it gives you information on your system software version, ISDN telephone line status, number of packets sent and number of packets received.

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

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

Menu 24.1 -- System Maintenance - Status									
Chan	Link	Type	TXPkts	RXPkts	Errors	CLU	ALU	Up Time	
--	Down	0Kbps	0	0	0	0%	0%	0:00:00	
--	Down	0Kbps	0	0	0	0%	0%	0:00:00	
Total Outcall Time:			0:00:00						
Ethernet:					WAN:				
Status: Down					Chan 1 IP Addr:				
TX Pkts: 0					Chan 2 IP Addr:				
RX Pkts: 0					Port 1 CLID:				
Collisions: 0					Port 2 CLID:				
LAN Packet Which Triggered Last Call:									
Press Command:									
COMMANDS: 1-Drop B1 2-Drop B2 3-Reset Counters 4-Drop All ESC-Exit									

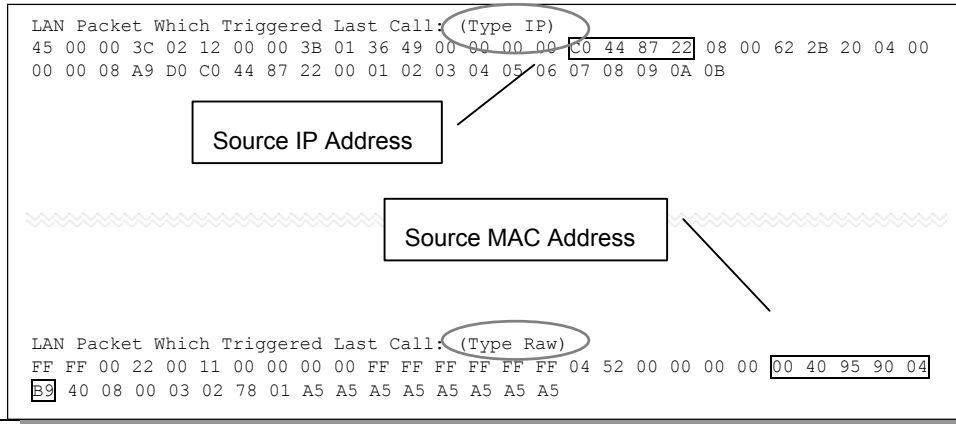
Figure 15-2 Menu 24.1 - System Maintenance – Status

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

Table 15-1 System Maintenance - Status Menu Fields

Field	Description
Chan	Shows statistics for B1 and B2 channels respectively. This is the information displayed for each channel:
Link	Shows the name of the remote node or the user the channel is currently connected to or the status of the channel (Idle, Calling or Answering).
Type	The current connecting speed.
TXPkt	The number of transmitted packets on this channel.
RXPkt	The number of received packets on this channel.
Error	The number of error packets on this channel.
CLU	(Current Line Utilization) percentage of current bandwidth used on this channel
ALU	(Average Line Utilization) a 5-second moving average of channel usage for this channel.
Up Time	Time this channel has been connected to the current remote node.
Total Outgoing call Time	Shows the total outgoing call time for both B1 and B2 channels since the system has been powered up.
Ethernet	(Ethernet connection).
Status	Shows the current transmission speed and mode of the LAN.
TX Pkt	The number of transmitted packets to the LAN.
RX Pkt	The number of received packets from the LAN.
Collision	Number of collisions.
WAN	

Chan 1 IP Addr	Refers to the IP address of the Prestige on Channel 1.
Chan 2 IP Addr	Refers to the IP address of the Prestige on Channel 2.
Chan 1 CLID	Shows the Calling Line Identification of the peer on Chan 1.



Chan 2 CLID	Shows the Calling Line Identification of the peer on Chan 2.
LAN Packet Which Triggered Last Call	Shows the first 48 octets of the LAN packet that triggered the last outgoing call.

The figure below shows two examples of triggering packets from the LAN: the first of an ICMP ping packet (Type: IP) and the second a SAP broadcast packet (Type: Raw). With this information, you can determine the workstation from the source IP address or the source MAC address of the packet.

Figure 15-3 LAN Packet That Triggered Last Call

15.1.1 System Information

```

Menu 24.2.1 - System Maintenance - Information

Name:P128Plus

Routing: IP
RAS S/W Version: V2.20(B.00)B05 | 11/16/98
ISDN F/W Version: V 082
Country Code: 238

LAN

Ethernet Address:00:a0:c5:02:34:56
IP Address: 192.168.1.1
IP Mask: 255.255.255.0
DHCP: Server

Press ESC or RETURN to Exit:

```

Figure 15-4 System Maintenance - Information

Table 15-2 Fields in System Maintenance

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

15.1.2 Console Port Speed

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

```
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.
```

desired speed in Menu 24.2.2, as shown below.

Figure 15-5 Menu 24.2.2 – System Maintenance – Change Console Port Speed

15.2 Log and Trace

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

15.2.1 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 will have the option to clear the error log.

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



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

below.

Figure 15-6 Examples of Error and Information Messages

15.2.2 Syslog And Accounting

The Prestige uses the UNIX syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured

```
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.
```

in Menu 24.3.2 - System Maintenance - Syslog and Accounting, as shown below.

Figure 15-7 Menu 24.3.2 - System Maintenance - Syslog and Accounting

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

Table 15-3 System Maintenance Menu Syslog Parameters

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

Your Prestige sends three types of syslog messages: call information messages (i.e. CDR), error information messages and session information messages. Some examples of these syslog messages are shown below:

1. Call Information Messages:

```
line 1 channel 1, call 41, C01, Incoming Call, 40001
line 1 channel 1, call 41, C01, ANSWER Connected, 49K 40001
line 1 channel 1, call 41, C01, Incoming Call, Call
Terminated
```

2. Error Information Messages:

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

3. Session Information Messages:

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

15.3 Diagnostic

The diagnostic facility allows you to test the different aspects of your Prestige to determine if it is working properly. Menu 24.4 allows you to choose among

```
Menu 24.4 - System Maintenance - Diagnostic

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

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

Enter Menu Selection Number:
Manual Call Remote Node= N/A
Host IP Address= N/A
```

various types of diagnostic tests to evaluate your system, as shown below.

Figure 15-8 Menu 24.4 - System Maintenance - Diagnostic

Follow the procedure below to get to Diagnostic

- Step 1.** From the Main Menu, select option 24 to open Menu 24 - System Maintenance.
- Step 2.** From this menu, select option 4. Diagnostic. This will open Menu 24.4 - System Maintenance - Diagnostic.

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

Table 15-4 System Maintenance Menu Diagnostic

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

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

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

Figure 15-9 Trace Display for a Successful Manual Call

This figure shows a trace example where authentication failed.

```
Start dialing for node <1>
### Hit any key to continue. ###
Dialing chan<2> phone<last 9-digit>:23456
Call CONNECT speed<64000> chan<2> prot<1>
LCP up
CHAP send response
***Login to remote failed. Check name/passwd.
Receive Terminal REQ
IPCP down
Line Down chan<2>
```

Figure 15-10 Trace Display for a Failed Authentication

15.4 Backup Configuration

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

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

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

15.5 Restore Configuration

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

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

15.6 Software Update

Software updates are only possible through the RS-232 cable connection. You cannot use `telnet` to update the software version of your Prestige. Please note that this function will delete the old software before installing the new software. Do not attempt to utilize this menu unless you have the new software version. There are two different software updates: RAS code and ISDN code.

RAS and ISDN code update - Type 'atur' and wait until the Prestige responds with an OK to begin uploading the new software (upload procedure varies depending on the type of software used to access the Prestige). You must use the XMODEM protocol to perform the upload. After uploading is successful, type 'atgo' to start your Prestige.

To update software, system needs to be rebooted.
 After system is rebooted, 'Enter Debug Mode' will be displayed.

Figure 15-11 Menu 24.7 - System Maintenance - Upload Firmware

15.6.1 Boot module commands

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

	<pre> ===== Debug Command Listing ===== ATHE print help ATGO boot system ATUR upload RAS code ATUR3 upload RAS configuration file ATBAx change baud rate. 1:38.4,2:19.2,3:9.6,4:57.6,5:115.2 ATTD download configuration to PC ATSE display seed for password generation ATSH display Revision and etc </pre>	
15-14		<i>Maintenance</i>

Figure 15-12 Boot module commands

15.7 Command Interpreter Mode

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

```
Enter Menu Selection Number: 8

P128plus> ?
Valid commands are:
sys          exit          device        ether
isdn        l2tp          radius        ip
ppp         bridge       ipx
P128plus>
```

Support Group.

Figure 15-13 Command mode

15.8 Call Control

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

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

The budget management function allows you to set a limit on the total outgoing call time of the Prestige over a period of time. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

The blacklist function prevents the Prestige from re-dialing to an unreachable phone number. It is a list of phone numbers, up to a maximum of 14, to which the Prestige will not make an outgoing call. If the Prestige tries to dial to a phone number and fails a certain number of times (configurable in Menu 24.9.1), then the phone number is put in the blacklist. You will have to enable the number manually before the Prestige will dial that number again.

Call history chronicles preceding incoming and outgoing calls.

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

```
Menu 24.9 - System Maintenance - Call Control

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

Enter Menu Selection Number:
```

Figure 15-14 Menu 24.9 - System Maintenance - Call Control

15.8.1 Call Control Parameters

```
Menu 24.9.1 - Call Control Parameters

Dialer Timeout:
Digital Call(sec)= 30

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

Figure 15-15 Call Control Parameters

Table 15-5 Call Control Parameters Fields

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

15.8.2 Blacklist

The phone numbers on the blacklist are numbers that the Prestige had problems connecting in the past. The only operation allowed is for you to take a number off the list by entering its index number.

Menu 24.9.2 shows the list of telephone numbers that have been blacklisted.

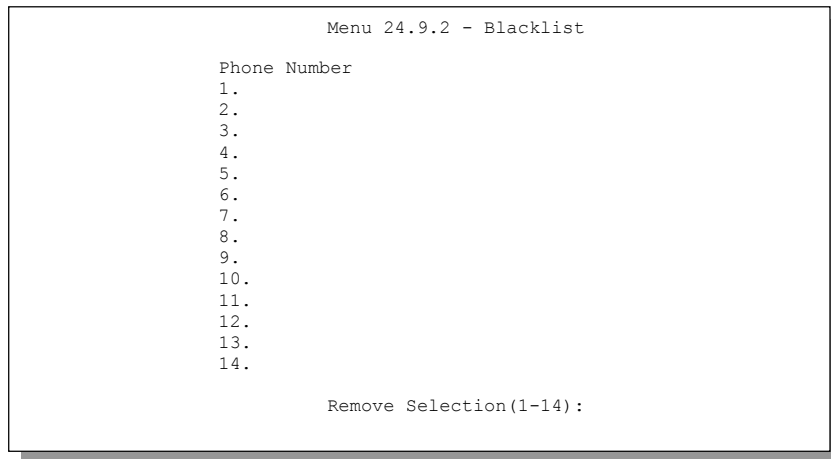
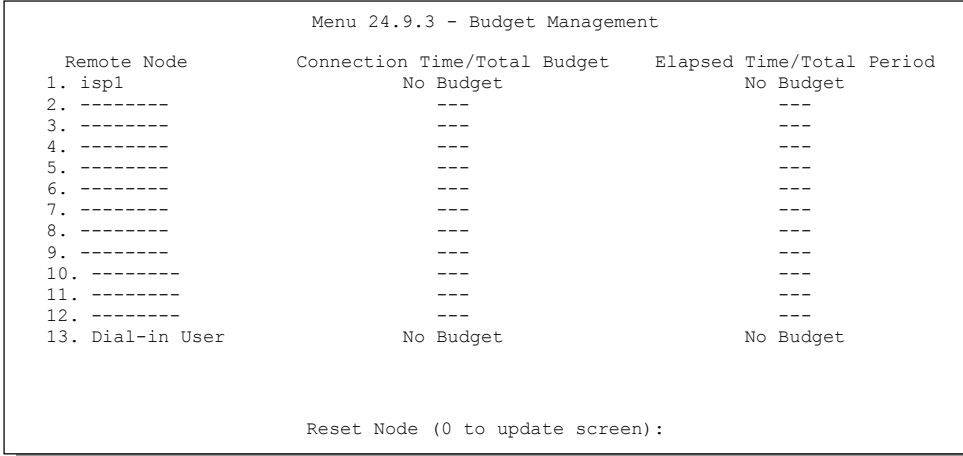


Figure 15-16 Menu 24.9.2 - Blacklist

15.8.3 Budget Management

Menu 24.9.3 shows the budget management statistics for outgoing calls.



```
Menu 24.9.3 - Budget Management

Remote Node      Connection Time/Total Budget      Elapsed Time/Total Period
1. isp1          No Budget                          No Budget
2. -----          ---
3. -----          ---
4. -----          ---
5. -----          ---
6. -----          ---
7. -----          ---
8. -----          ---
9. -----          ---
10. -----         ---
11. -----         ---
12. -----         ---
13. Dial-in User      No Budget                          No Budget

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

Figure 15-17 Menu 24.9.3 - Budget Management

The total budget is the time limit on the accumulated time for outgoing call to a remote node or for calling back to the dial-in users collectively. When this limit is reached, the call will be dropped and further outgoing calls to that remote node or dial-in user (callback) will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node or the dial-in users. The budget and the reset period can be configured in the Menu 11 and 13 for a remote node and for the dial-in user, respectively.

15.8.4 Call History

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

Menu 24.9.4 - Call History						
Phone Number	Dir	Rate	#call	Max	Min	Total
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						

Enter Entry to Delete(0 to exit):

Figure 15-18 Call History

Table 15-6 Call History Fields

Field	Description
Phone Number	This is the telephone number of past incoming and outgoing calls.
Dir	This shows whether the call was incoming or outgoing.
Rate	This is the transfer rate of the call.

#call	This is the number of calls made to or received from that telephone number.
Max	This is the length of time of the longest telephone call.
Min	This is the length of time of the shortest telephone call.
Total	This is the total length of time of all the telephone calls to/from that telephone number.

Chapter 16

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.

16.1 Problems Starting Up the Prestige

Table 16-1 Troubleshooting the Start-Up of your Prestige

Problem	Corrective Action	
None of the LED's are on when you power on the Prestige	Check the connection between the AC adapter and the Prestige. If the error persists, you may have a hardware problem. In this case you should contact technical support.	
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
		No parity, 8 Data bits, 1 Stop bit.

16.2 Problems With the ISDN Line

Table 16-2 Troubleshooting the ISDN Line

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

16.3 Problems with the Ethernet Connection

Table 16-3 Troubleshooting the Ethernet Connection

Problem	Corrective Action
Can't ping any station on the external LAN	Check the Ethernet LED's on the front panel. The LNK LED should be on when the Prestige has made a successful Ethernet connection. If it is off, check the cables between your Prestige and the station.
	Verify that the IP address and the subnet mask are consistent between the Prestige and the workstations.

16.4 Problems Connecting to a Remote Node or ISP

Table 16-4 Troubleshooting a Connection to a Remote Node or ISP

Problem	Corrective Action
Can't connect to a remote node or ISP	Check Menu 24.1 to verify the line status. If it indicates [down], then refer to the section on the line problems.
	In Menu 24.4.5, do a manual call to that remote node. Observe the messages and take appropriate actions.

16.5 Problems for Remote User to Dial-in

Table 16-5 Troubleshooting for Remote Users to Dial-in

Problem	Corrective Action
A remote user cannot dial-in	First verify that you have configured the authentication parameters in Menu 13. These would be CLID Authen and Recv. Authen.
	In Menu 14, verify the user name and password for the remote dial-in user.

	If the remote dial-in user is negotiating IP, verify that the IP address is supplied correctly in Menu 13. Check that either the remote dial-in user is supplying a valid IP address, or that the Prestige is assigning a valid address from the IP pool.
	If the remote dial-in user is negotiating IPX, verify that the IPX network number is valid from the IPX pool (if it is being used).

Setup Information Worksheet

General Setup Information			
System Name			
Protocol Routing	<input type="checkbox"/> TCP/IP	<input type="checkbox"/> IPX	
ISDN Setup Information			
Switch Type	<input type="checkbox"/> AT&T 5ESS Point to Point	<input type="checkbox"/> AT&T 5ESS Multipoint	
	<input type="checkbox"/> Northern Telecom NI-1	<input type="checkbox"/> Northern Telecom Custom	
	<input type="checkbox"/> AT&T 5ESS NI-1	<input type="checkbox"/> DSS1	
B-Channel Usage	<input type="checkbox"/> Switch/Switch	<input type="checkbox"/> Switch/Unused	
North America ISDN Switches (AT&T, Northern Telecom)			
1st Phone Number			
1st SPII Number			
Analog Call	<input type="checkbox"/> Phone1	<input type="checkbox"/> Phone2	<input type="checkbox"/> DOVBS
2nd Phone Number			
2nd SPII Number			
Analog Call	<input type="checkbox"/> Phone1	<input type="checkbox"/> Phone2	<input type="checkbox"/> DOVBS
Supplemental Service Activation Keys <i>(defaults for North America)</i>			
Conference Call	<input type="checkbox"/> default: '60'	<input type="checkbox"/> other:	
Call Transfer	<input type="checkbox"/> default: '61'	<input type="checkbox"/> other:	
Drop Call	<input type="checkbox"/> default: '62'	<input type="checkbox"/> other:	
Call Forwarding	<input type="checkbox"/> default: '57'	<input type="checkbox"/> other:	
European ISDN (DSS1)			
ISDN Data Number & Subaddress			
A/B 1 Number & Subaddress			
A/B 2 Number &			

Subaddress			
Outside Line Prefix			
PABX # (S/T bus)			
Incoming Number Matchin	<input type="checkbox"/> MSN	<input type="checkbox"/> CDSA	<input type="checkbox"/> Don't Care
Analog Call Routing	<input type="checkbox"/> A/B #1	<input type="checkbox"/> A/B #2	<input type="checkbox"/> Ignore
Global Analog Call	<input type="checkbox"/> Accept		<input type="checkbox"/> Ignore
Ethernet Setup Information			
Ethernet Interface	<input type="checkbox"/> UTP		<input type="checkbox"/> AUI
IP Address	_____ : _____ : _____		
IP Subnet Mask	_____ : _____ : _____		

Acronyms and Abbreviations

BAP/BACP	Bandwidth Allocation Protocol/Bandwidth Allocation Control protocol
BOD	Bandwidth on Demand
CDR	Call Detail Record
CHAP	Challenge Handshake Authentication Protocol
CLID	Calling Line IDentification
CSU/DSU	Channel Service Unit/Data Service Unit
DCE	Data Communications Equipment
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DTE	Data Terminal Equipment
IANA	Internet Assigned Number Authority
IP	Internet protocol
IPCP	IP Control Protocol
IPX	Internetwork Packet eXchange
ISDN	Integrated Service Digital Network
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Media Access Control
MP	(PPP) Multilink Protocol
NAT	Network Address Translation
PAP	Password Authentication Protocol
POTS	Plain Old Telephone Service

PPP	Point to Point Protocol
PSTN	Public Switched Telephone Network
RADIUS	Remote Authentication Dial-In User Service
RIP	Routing Information Protocol
SAP	(IPX) Service Advertising Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SUA	Single User Account
TA	(ISDN) Terminal Adapter
TFTP	Trivial File Transfer Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair (cable)
WAN	Wide Area Network

Index

- 10Base2, 2-4
- 10Base5. *See* AUI
- 10Base-T, 2-4
- 802.2, 6-1
- 802.3, 6-1
- A/B Adapter, xxiii
- AUI, 2-4
- authentication, 4-4, 4-6, 8-5
- backup, 15-12
- BACP, 4-7
- Bandwidth on Demand. *See* BOD
- BAP, 4-7
- Base Transmission Rate, 4-7
- blacklist, 15-16
- BOD, 4-7
- bridge. *See* bridging
- Bridge Ethernet Setup, 7-1
- bridge static route, 7-5
- bridging, 4-4, 7-1
- BTR. *See* Base Transmission Rate
- budget, 8-6, 15-17
- call control, 15-14
- call direction, 4-3
- callback, 4-4, 8-6, 8-10, 8-11
- CHAP, 4-4
- CLID, 4-3, 8-5, 8-11
- community, 12-1
- console port, 2-4
- contact person, 2-12
- Default Dial-In Setup, 8-4
- DHCP, 1-3, 3-3
- diagnostic, 15-9
- dial-in user, 8-1
- Dial-In Users Setup, 8-8
- dial-on-broadcast, 7-4
- dial-on-query, 6-9
- Direct mode, 10-6
- DIX, 6-1
- DNS, 3-3, 3-6
- DSS1, xxiii

encapsulation, 4-9	IPX node number, 6-1
Ethernet, 2-17	IPX Spoofing, 6-5
Ethernet II, 6-1	IPX static route, 6-10
filter, 2-18, 4-10, 8-8, 11-1	ISP, 3-14
frame type, 6-1, 6-6	L2TP, 1-1, 10-1
gateway, 5-7, 6-11, 7-6	LAC, 10-3
General Setup, 2-11	LAN, 15-3
generic filter rule, 11-11	LAN-to-LAN, 5-1, 8-3
hop count, 6-11	LNS, 10-3
IANA, 3-2	location, 2-12
idle timeout, 4-5	log, 15-6
Internet access, 1-4, 3-1	login, 4-3
IP address, 3-2, 3-7, 4-5, 5-4, 5-7, 7-6, 8-6	MAC, 7-1
IP Address, xxiii	Main Menu, 2-8
IP network number, 3-2	Max. Transmission Rate, 4-7
IP Pool, 3-3	Media Access Control. <i>See</i> MAC
IP static route, 5-5	metric, 5-4, 5-7
IP Subnet Mask, xxiv	MP, 1-2, 3-10, 4-6
IPX, 4-5, 6-1	Multilink. <i>See</i> MP. <i>See</i> MP
IPX Ethernet Setup, 6-6	mutual authentication, 8-5
IPX filter rule, 11-13	PABX, 2-14, 2-15
IPX LAN-to-LAN, 6-7	PAP, 4-4, 8-5
IPX network number, 6-1, 6-2, 8-7	password, 2-6, 2-9, 4-3, 4-4, 13-1

Ping, 15-10

Point-to-Point Protocol/Multilink Protocol.
 See PPP/MP

POTS, xxiii

power adapter, 2-4

PPP, 4-5, 4-8

PPP/MP, 1-5

private, 5-4, 5-7

protocols, 2-12

Proxy mode, 10-8

RADIUS, 1-3, 13-3

remote node, 4-1, 8-1

Remote Node, 4-9, 15-3, 15-10

restore, 15-12

RIP, 3-2, 3-7, 5-4, 6-9

route, 4-4

RS-232, 15-12

SAP, 6-9

seed router, 6-6

server, 6-11

Single User Account, 3-10. *See* SUA

SMT, 2-7

SNAP, 6-1

SNMP, 12-1

socket, 6-11

software update, 15-12

SUA, 1-5, 3-11, 5-4

subnet mask, 3-2, 3-7, 5-4, 5-7

switch types, xxiii, 16-2

syslog, 15-7

system name, 2-12

system status, 15-2

Target Utility, 4-7

TCP/IP, xxiii, xxiv, 5-1, 15-10

TCP/IP filter rule, 11-7

Telco Options, 3-10

Telecommuter, 8-2

telnet, 14-1, 15-12

tick count, 6-9, 6-11

trace, 15-6

troubleshooting, 16-1

VT100, 2-5

WAN address, 5-4

watchdog, 6-9

worksheet, xxii, xxiii

