

Prestige 1100

WAN Access Router

User's Guide

Version 2.50

Nov 1999

ZyXEL

TOTAL INTERNET ACCESS SOLUTION

Prestige 1100

WAN Access Router

Copyright

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

Trademarks

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

ZyXEL Limited Warranty

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

Note

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

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

Customer Support

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

Method	EMAIL – Support	Telephone	Web Site	Regular Mail
Region	EMAIL – Sales	Fax	FTP Site	
Worldwide	support@zyxel.com.tw support@europe.zyxel.com	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, HsinChu, Taiwan.
	sales@zyxel.com.tw	+886-3-578-2439	ftp.europe.zyxel.com	
North America	support@zyxel.com	+1-714-632-0882 800-255-4101	www.zyxel.com	ZyXEL Communications Inc., 1650 Miraloma Avenue, Placentia, CA 92870, U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.zyxel.com	
Scandinavia	support@zyxel.dk	+45-3955-0700	www.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark.
	sales@zyxel.dk	+45-3955-0707	ftp.zyxel.dk	
Austria	support@zyxel.at	+43-1-4948677-0 0810-1-ZyXEL (= 0810-1-99935)	www.zyxel.at	ZyXEL Communications Services GmbH., Thaliastrasse 125a/2/2/4, A-1160 Vienna, Austria
	sales@zyxel.at	+43-1-4948678	ftp.zyxel.at Note: for Austrian users with *.at domain only!	
Germany	support@zyxel.de	+49-2405-6909-0 0180-5213247 Tech Support hotline 0180-5099935 RMA/Repair hotline	www.zyxel.de	ZyXEL Deutschland GmbH., Adenauerstr. 20/A4, D-52146 Wuerselen, Germany.
	sales@zyxel.de	+49-2405-6909-99	ftp.europe.zyxel.com	

Table of Contents

Customer Support	iv
Table of Contents	v
List of Figures	xi
List of Tables	xiii
Preface	xiv
Chapter 1: Getting to Know Your Bridge/Router	1-1
1.1 Quick Feature Overview of the Prestige 1100.....	1-1
1.2 Detailed Features of the Prestige 1100.....	1-1
1.3 Front Panel LEDs and Back Panel Ports	1-3
1.3.1 Front Panel LEDs	1-3
1.3.2 Prestige 1100 Back Panel.....	1-4
1.4 Applications for Prestige 1100.....	1-4
1.4.1 Internet Access	1-4
Chapter 2: Hardware Installation & Initial Setup	2-1
2.1 Unpacking your Bridge/Router.....	2-1
2.2 Additional Installation Requirements	2-1
2.3 Connect your <i>WAN Bridge/Router</i>	2-2
2.3.1 Prestige 1100 Connections	2-2
2.4 Power On Your Prestige 1100.....	2-3
2.5 Navigating the SMT Interface.....	2-5
2.6 Changing the System Password.....	2-7
2.7 General Setup.....	2-9
2.7.1 Note on Bridging	2-10
2.8 WAN Setup	2-11
2.8.1 Prestige 1100 WAN Port Setup.....	2-11
2.9 Ethernet Setup.....	2-12
2.10 General Ethernet Setup	2-13
2.11 Protocol Dependent Ethernet Setup.....	2-13

Chapter 3: Internet Access.....	3-1
3.1 Route IP Setup	3-1
3.2 TCP/IP Parameters	3-2
3.2.1 IP Address and Subnet Mask.....	3-2
3.2.2 RIP Setup	3-2
3.2.3 DHCP Configuration.....	3-3
3.3 TCP/IP and DHCP Ethernet Setup.....	3-3
3.4 IP Multicast.....	3-5
3.5 Internet Access Configuration.....	3-6
3.6 Single User Account.....	3-8
3.6.1 Advantages of SUA	3-9
3.6.2 Single User Account Configuration.....	3-9
3.6.3 Ethernet SUA.....	3-10
3.7 LANs & WANs.....	3-11
3.7.1 LANs, WANs and the Prestige.....	3-11
Chapter 4: Remote Node Configuration for LAN to LAN	4-1
4.1 Leased Line Remote Node Profile	4-1
4.2 Outgoing Authentication Protocol.....	4-3
4.3 Editing PPP Options	4-3
Chapter 5: Remote Node TCP/IP Configuration.....	5-1
5.1 LAN-to-LAN Application.....	5-1
5.2 Remote Node Setup.....	5-2
5.3 Static Route Setup.....	5-6
Chapter 6: IPX Configuration.....	6-1
6.1 IPX Network Environment	6-1
6.1.1 Network and Node Number.....	6-1
6.1.2 Frame Types	6-1
6.1.3 External Network Number.....	6-2
6.1.4 Internal Network Number.....	6-2
6.2 Prestige 1100 in an IPX Environment.....	6-2
6.2.1 Prestige 1100 on LAN with Server.....	6-3
6.2.2 Prestige 1100 on LAN without Server.....	6-3
6.3 IPX Ethernet Setup.....	6-4

6.4	LAN-to-LAN Application with Novell IPX.....	6-5
6.4.1	IPX Remote Node Setup.....	6-6
6.4.2	IPX Static Route Setup.....	6-8
Chapter 7: Bridging Setup.....		7-1
7.1	Bridging in General.....	7-1
7.2	Bridge Ethernet Setup.....	7-1
7.2.1	Remote Node Bridging Setup.....	7-2
7.2.2	Bridge Static Route Setup.....	7-4
Chapter 8: Filter Configuration.....		8-1
8.1	About Filtering.....	8-1
8.2	The Filter Structure of the Prestige.....	8-1
8.3	Configuring a Filter Set.....	8-3
8.3.1	Filter Rules Summary Menu.....	8-4
8.4	Configuring a Filter Rule.....	8-6
8.4.1	Filter Types and SUA.....	8-6
8.4.2	TCP/IP Filter Rule.....	8-7
8.4.3	Novell IPX Filter Rule.....	8-11
8.4.4	Device Filter Rule.....	8-13
8.5	Applying a Filter.....	8-15
8.5.1	Ethernet traffic.....	8-15
8.5.2	Remote Node Filters.....	8-16
Chapter 9: SNMP Configuration.....		9-1
9.1	About SNMP.....	9-1
9.2	SNMP Configuration.....	9-1
Chapter 10: System Security.....		10-1
10.1	Changing the System Password.....	10-1
Chapter 11: Telnet Configuration and Capabilities.....		11-1
11.1	About Telnet Configuration.....	11-1
11.2	Telnet Under SUA.....	11-2
11.3	Telnet Capabilities.....	11-2
11.3.1	Single Administrator.....	11-2
11.3.2	System Timeout.....	11-2

Chapter 12: System Maintenance12-1

12.1	System Status.....	12-2
12.2	System Information.....	12-4
12.2.1	Console Port Speed.....	12-5
12.3	Log and Trace.....	12-5
12.3.1	Viewing Error Log.....	12-5
12.3.2	Syslog And Accounting.....	12-6
12.4	Diagnostic	12-7
12.5	Filename conventions	12-8
12.6	Back up Configuration.....	12-9
12.6.1	Backup using the Console Port.....	12-9
12.6.2	Back up using FTP.....	12-10
12.6.3	Back up using TFTP.....	12-10
12.7	Restore Configuration.....	12-11
12.7.1	Restore using the Console Port.....	12-11
12.7.2	Restore using FTP.....	12-11
12.7.3	Restore using TFTP.....	12-12
12.8	Upload Firmware	12-12
12.8.1	Dual Firmware Block Structure.....	12-13
12.8.2	Upload Router Firmware via the Console Port.....	12-13
12.8.3	Upload Router Firmware using FTP.....	12-14
12.8.4	Upload Router Firmware using TFTP.....	12-15
12.9	Upload Router Configuration File	12-15
12.9.1	Upload Router Configuration File using the Console Port.....	12-15
12.9.2	Upload Router Configuration File using FTP.....	12-16
12.9.3	Upload Router Configuration File using TFTP	12-17
12.9.4	Boot Module Commands.....	12-18
12.10	Command Interpreter Mode	12-19

Chapter 13: IP Policy Routing.....13-1

13.1	Introduction.....	13-1
13.1.1	Benefits.....	13-1
13.1.2	Routing Policy	13-1
13.1.3	IP Policy Routing Setup	13-2
13.2	Applying an IP Policy.....	13-6
13.2.1	Ethernet IP Policies	13-6
13.2.2	Remote Node IP Routing Policies	13-6

Chapter 14: Troubleshooting 14-1

 14.1 Problems Starting Up the Prestige 1100.....14-1

 14.2 Problems With the WAN Port14-2

 14.3 Problems with the LAN Interface.....14-2

 14.4 Problems Connecting to a Remote Node or ISP14-2

Acronyms and Abbreviations A

Index..... C

List of Figures

<i>Figure 1-1 Remote Configuration</i>	1-2
<i>Figure 1-2 Prestige 1100 Front Panel</i>	1-3
<i>Figure 1-3 Back Panel</i>	1-4
<i>Figure 1-4 Internet Access Application</i>	1-5
<i>Figure 1-5 LAN-to-LAN Application</i>	1-6
<i>Figure 2-1 P1100 Connections</i>	2-2
<i>Figure 2-2 Power-On Display</i>	2-3
<i>Figure 2-3 Login Screen</i>	2-4
<i>Figure 2-4 SMT Main Menu</i>	2-6
<i>Figure 2-5 Menu 23 - System Security</i>	2-7
<i>Figure 2-6 Menu 23.1 - System Security - Change Password</i>	2-8
<i>Figure 2-7 Menu 1 - General Setup</i>	2-9
<i>Figure 2-8 Menu 2 - WAN Port Setup</i>	2-11
<i>Figure 2-9 Menu 3 - Ethernet Setup - Select LAN</i>	2-12
<i>Figure 2-10 Menu 3 – Ethernet Setup</i>	2-12
<i>Figure 2-11 Menu 3.1 - General Ethernet Setup</i>	2-13
<i>Figure 3-1 Menu 1 - General Setup</i>	3-1
<i>Figure 3-2 Menu 3.2 - TCP/IP and DHCP Ethernet Setup</i>	3-4
<i>Figure 3-3 Menu 4 - Internet Access Setup</i>	3-6
<i>Figure 3-4 Single User Account Topology</i>	3-8
<i>Figure 3-5 Menu 4 - Internet Access Setup for Single User Account</i>	3-9
<i>Figure 3-6 Ethernet SUA Example</i>	3-10
<i>Figure 3-7 LAN & WAN IPs</i>	3-11
<i>Figure 3-8 Ethernet as WAN port</i>	3-11
<i>Figure 4-1 Menu 11.1 - Remote Node Profile for Leased Lines</i>	4-1
<i>Figure 4-2 Menu 11.2 - Remote Node PPP Options</i>	4-4
<i>Figure 5-1 LAN-to-LAN Application with TCP/IP</i>	5-1
<i>Figure 5-2 Menu 11.3- Remote Node TCP/IP Options</i>	5-2
<i>Figure 5-3 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection</i>	5-3
<i>Figure 5-4 Example of Static Routing Topology</i>	5-6
<i>Figure 5-5 Menu 12 - Static Route Setup</i>	5-7
<i>Figure 5-6 Menu 12.1 - IP Static Route Setup</i>	5-7
<i>Figure 5-7 Edit IP Static Route</i>	5-7
<i>Figure 6-1 NetWare Network Numbers</i>	6-2
<i>Figure 6-2 Prestige in an IPX Environment</i>	6-3
<i>Figure 6-3 Menu 3.3 - Novell IPX Ethernet Setup</i>	6-4
<i>Figure 6-4 LAN-to-LAN Application with Novell IPX</i>	6-5
<i>Figure 6-5 Menu 11.3 - Remote Node Novell IPX Options</i>	6-6
<i>Figure 6-6 Menu 12.2.1 - Edit IPX Static Route</i>	6-8
<i>Figure 7-1 Menu 3.5 - Bridge Ethernet Setup</i>	7-2

<i>Figure 7-2 Menu 11.3 - Remote Node Bridging Options.....</i>	<i>7-3</i>
<i>Figure 7-3 Menu 12.3.1 - Edit Bridge Static Route.....</i>	<i>7-4</i>
<i>Figure 8-1 Filter Rule Process.....</i>	<i>8-2</i>
<i>Figure 8-2 Menu 21 - Filter Set Configuration.....</i>	<i>8-3</i>
<i>Figure 8-3 Menu 21.1 - Filter Rules Summary.....</i>	<i>8-4</i>
<i>Figure 8-4 Protocol and Device Filter Sets.....</i>	<i>8-7</i>
<i>Figure 8-5 Menu 21.1.1 - TCP/IP Filter Rule.....</i>	<i>8-8</i>
<i>Figure 8-6 Executing an IP Filter.....</i>	<i>8-10</i>
<i>Figure 8-7 Menu 21.1.1 - IPX Filter Rule.....</i>	<i>8-11</i>
<i>Figure 8-8 Menu 21.1.2 - Device Filter Rule.....</i>	<i>8-14</i>
<i>Figure 8-9 Filtering Ethernet Traffic.....</i>	<i>8-15</i>
<i>Figure 8-10 Filtering Remote Node traffic.....</i>	<i>8-16</i>
<i>Figure 9-1 Menu 22 - SNMP Configuration.....</i>	<i>9-1</i>
<i>Figure 10-1 Menu 23 - System Security.....</i>	<i>10-1</i>
<i>Figure 10-2 Menu 23.1 - System Security - Change Password.....</i>	<i>10-2</i>
<i>Figure 11-1 Telnet Configuration on a TCP/IP Network.....</i>	<i>11-1</i>
<i>Figure 12-1 Menu 24 - System Maintenance.....</i>	<i>12-1</i>
<i>Figure 12-2 Menu 24.1 - System Maintenance – Status.....</i>	<i>12-2</i>
<i>Figure 12-3 System Maintenance – Information.....</i>	<i>12-4</i>
<i>Figure 12-4 Menu 24.2.2 – System Maintenance – Change Console Port Speed.....</i>	<i>12-5</i>
<i>Figure 12-5 Examples of Error and Information Messages.....</i>	<i>12-6</i>
<i>Figure 12-6 Menu 24.3.2 - System Maintenance - Syslog and Accounting.....</i>	<i>12-6</i>
<i>Figure 12-7 Menu 24.4 - System Maintenance - Diagnostic.....</i>	<i>12-7</i>
<i>Figure 12-8 Menu 24.5 –Backup Configuration using the Console Port.....</i>	<i>12-10</i>
<i>Figure 12-9 Backup Configuration using FTP.....</i>	<i>12-10</i>
<i>Figure 12-10 Menu 24.6 –Restore Configuration using the Console Port.....</i>	<i>12-11</i>
<i>Figure 12-11 Restore Configuration using FTP.....</i>	<i>12-12</i>
<i>Figure 12-12 Menu 24.7 -- System Maintenance - Upload Firmware.....</i>	<i>12-13</i>
<i>Figure 12-13 Menu 24.7.1 –Upload ZYNOS Code using the Console Port.....</i>	<i>12-14</i>
<i>Figure 12-14 Menu 24.7.1. – Upload Router Firmware using FTP.....</i>	<i>12-14</i>
<i>Figure 12-15 Menu 24.7.2 –Upload Router Configuration File.....</i>	<i>12-16</i>
<i>Figure 12-16 Menu 24.7.2 – Upload Router Configuration File using FTP.....</i>	<i>12-16</i>
<i>Figure 12-17 Boot module commands.....</i>	<i>12-18</i>
<i>Figure 12-18 Command mode.....</i>	<i>12-19</i>
<i>Figure 13-1 IP Routing Policy Setup.....</i>	<i>13-2</i>
<i>Figure 13-2 Menu 25 - IP Routing Policy Summary.....</i>	<i>13-3</i>
<i>Figure 13-3 IP Routing Policy.....</i>	<i>13-4</i>
<i>Figure 13-4 Menu 3.1.1 - General Ethernet Setup.....</i>	<i>13-6</i>
<i>Figure 13-5 Menu 11.3 - Remote Node Network Layer Options.....</i>	<i>13-7</i>

List of Tables

<i>Table 1-1 LED Functions</i>	1-3
<i>Table 2-1 Main Menu Commands</i>	2-5
<i>Table 2-2 Main Menu Summary</i>	2-6
<i>Table 2-3 General Setup Menu Fields</i>	2-10
<i>Table 2-4 WAN Setup Menu Fields</i>	2-11
<i>Table 3-1 DHCP Ethernet Setup Menu Fields</i>	3-4
<i>Table 3-2 TCP/IP Ethernet Setup Menu Fields</i>	3-5
<i>Table 3-3 Internet Account Information</i>	3-6
<i>Table 3-4 Internet Access Setup Menu Fields</i>	3-7
<i>Table 3-5 Single User Account Menu Fields</i>	3-10
<i>Table 4-1 Remote Node Profile Menu Fields for Leased Lines</i>	4-2
<i>Table 4-2 Remote Node PPP Options Menu Fields</i>	4-4
<i>Table 5-1 TCP/IP related fields in Remote Node Profile</i>	5-3
<i>Table 5-2 Remote Node TCP/IP Configuration</i>	5-4
<i>Table 5-3 Edit IP Static Route Menu Fields</i>	5-8
<i>Table 6-1 Novell IPX Ethernet Setup Fields</i>	6-4
<i>Table 6-2 Remote Node Novell IPX Options</i>	6-7
<i>Table 6-3 Edit IPX Static Route Menu Fields</i>	6-9
<i>Table 7-1 Remote Node Bridge Options</i>	7-3
<i>Table 7-2 Bridge Static Route Menu Fields</i>	7-4
<i>Table 8-1 Abbreviations Used in the Filter Rules Summary Menu</i>	8-4
<i>Table 8-2 Abbreviations Used If Filter Type Is IP</i>	8-5
<i>Table 8-3 Abbreviations Used If Filter Type Is IPX</i>	8-6
<i>Table 8-4 Abbreviations Used If Filter Type Is Dev</i>	8-6
<i>Table 8-5 TCP/IP Filter Rule Menu Fields</i>	8-8
<i>Table 8-6 IPX Filter Rule Menu Fields</i>	8-12
<i>Table 8-7 Device Filter Rule Menu Fields</i>	8-14
<i>Table 9-1 SNMP Configuration Menu Fields</i>	9-2
<i>Table 12-1 System Maintenance - Status Menu Fields</i>	12-3
<i>Table 12-2 Fields in System Maintenance</i>	12-4
<i>Table 12-3 System Maintenance Menu Syslog Parameters</i>	12-7
<i>Table 12-4 System Maintenance Menu Diagnostic</i>	12-8
<i>Table 12-5 Filename Conventions</i>	12-9
<i>Table 13-1 IP Routing Policy Summary</i>	13-4
<i>Table 13-2 IP Routing Policy</i>	13-5
<i>Table 14-1 Troubleshooting the Start-Up of your Prestige 1100</i>	14-1
<i>Table 14-2 Troubleshooting a WAN Port Connection</i>	14-2
<i>Table 14-3 Troubleshooting the LAN Interface</i>	14-2
<i>Table 14-4 Troubleshooting a Connection to a Remote Node or ISP</i>	14-2

Preface

About Your Bridge/Router

The Prestige 1100 is a high-performance bridge/router that offers a complete solution for your WAN applications such as Internet access and multi-protocol LAN-to-LAN connections for SMB (Small & Medium Size Businesses). It integrates the routing and bridging functions in a single package and is easy to install and to configure since you do not need to set any switches.

In addition, the Prestige 1100 supports synchronous mode on its WAN port, allowing it to connect to T1/E1 or FT1/FE1 (Fractional T1/E1) leased lines via CSU/DSUs (Channel Service Unit/Data Service Units).

About This User's Guide

This user's guide covers all operations of the Prestige 1100 and shows you how to get the best out of the multiple advanced features of your Prestige router. It is designed to help you configure the Prestige correctly for various applications.

Related Documentation

➤ *Supporting Disk*

More detailed information about the Prestige and examples of its use can be found in our Supporting Disk. This disk contains a Prestige Bulletin (a release note highlighting new features), a FAQ, a Configuration Guide, Support Tools for extra configuration, CI Commands Reference, Cable Pin assignments and Reference Documentation (Training Material and Support Accessories).

➤ *Packing List Card*

You should have a Packing List Card that lists all items that should have come with your Prestige.

Syntax Conventions

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

Chapter 1: Getting to Know Your Bridge/Router

The Prestige 1100 is a high-performance bridge/router that offers a complete solution for your WAN applications such as Internet access and multi-protocol LAN-to-LAN connections for SMB (Small & Medium Size Businesses). It integrates the routing and bridging functions in a single package and is easy to install and to configure since you do not need to set any switches.

In addition, the Prestige 1100 supports synchronous mode on its WAN port, allowing it to connect to T1/E1 or FT1/FE1 (Fractional T1/E1) leased lines via CSU/DSUs (Channel Service Unit/Data Service Units).

1.1 Quick Feature Overview of the Prestige 1100

- One WAN port with various interface support: RS-449/V.35/X.21/EIA 530/RS-232
- Two auto-sensing 10/100M Ethernet interfaces
- PPP for WAN connection
- IP/IPX and transparent bridging
- IP Multicast
- IP Policy Routing to support traffic management
- Network Address Translation for private IP address support
- Remote Management
- SNMP manageable
- IP packet filtering, including network level and device level filtering
- 100V~240V internal power supply and rack size for MIS environment

1.2 Detailed Features of the Prestige 1100

The following are the key features of the P1100.

One WAN port for various WAN Solutions

Your Prestige 1100 provides one WAN port with a 68-pin D type connector. It supports several interfaces (RS-449/V.35/X.21/EIA 530/RS-232) to connect to various WAN devices for up to E1 speed (2.048Mbps).

Two 10/100 Ethernet LANs

One 10/100M Ethernet interface is designed for high performance LAN environment. The other 10/100M Ethernet interface can be reserved for connecting to a Web/FTP server for public Internet access.

Most Complete NAT Support

ZyXEL NAT technology supports not only private IP for Internet access sharing and security protection, but also popular Internet multimedia applications such as Microsoft NetMeeting and CuSeeMe.

Multiple Protocol Support

- TCP/IP (Transmission Control Protocol/Internet Protocol) network layer protocol.
- Novell IPX (Internetwork Packet eXchange) protocol.
- Transparently bridging for network layer protocols that the Prestige 1100 does not route.
- PPP (Point-to-Point Protocol) link layer protocol.
- SUA™ (Single User Account) for NAT (Network Address Translation).

Remote Configuration

The P1100 may be remotely configured via the console port as well as the WAN port. A modem can be attached directly to the console port (DTE) for easy, alternative, remote configuration. See *Page 2-2* for more information on P1100 connections.

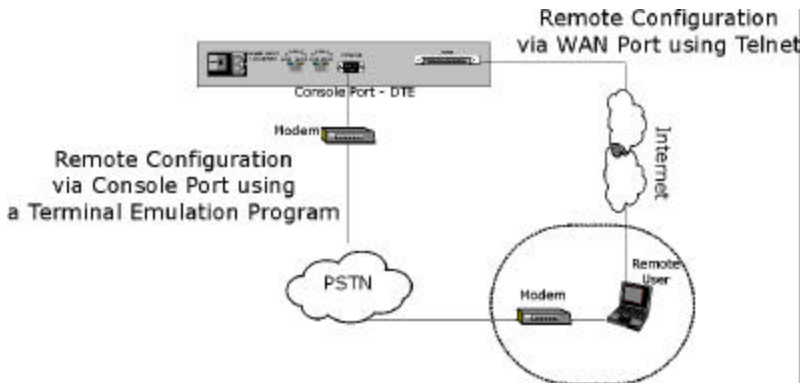


Figure 1-1 Remote Configuration

Full Network Management

Your Prestige 1100 supports SNMP (Simple Network Management Protocol) in addition to menu-driven network management via the console port or a telnet connection. With remote management, built-in diagnostic tools and syslog support, users can manage the P1100 with no extra effort.

DHCP Support

DHCP (Dynamic Host Configuration Protocol) allows you to dynamically and automatically assign IP address to hosts on your network.

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.

1.3 Front Panel LEDs and Back Panel Ports



Figure 1-2 Prestige 1100 Front Panel

1.3.1 Front Panel LEDs

The LED lights on the front panel indicate the operational status of your Prestige. Table 1-1 (next) describes the LED functions:

Table 1-1 LED Functions

PWR	The PWR (power) LED is on when power is applied to the Prestige.
SYS	A steady on SYS (system) LED indicates the Prestige is on and functioning properly while an off SYS LED indicates the system is not ready or a malfunction. The system is rebooting when the SYS LED is blinking.
LAN-1_10M	A steady green light indicates a 10Mbps Ethernet connection. The LED blinks when data is being sent or received.
LAN-1_100M	A steady orange light indicates a 100Mbps Ethernet Connection. The LED blinks when data is being sent or received.
LAN-2_10M	A steady green light indicates a 10Mbps Ethernet connection. The LED blinks when data is being sent or received.
LAN-2_100M	A steady orange light indicates a 100Mbps Ethernet Connection. The LED blinks when data is being sent or received.
WAN	The WAN LED is on when the Prestige is connected successfully to a WAN device. The LED blinks when data is sent or received. The LED is off when the link is down.

1.3.2 Prestige 1100 Back Panel



Figure 1-3 Back Panel

The diagram above shows the rear panel of your Prestige 1100. Refer to this diagram when making connections.

- ①: POWER INPUT = Power cord receptacle and switch
- ②: LAN1 = RJ-45 10/100 Mbps Ethernet port
- ③: LAN2 = RJ-45 10/100 Mbps Ethernet port
- ④: CONSOLE = DB-9 Console port
- ⑤: WAN = 68-pin D-type connector

1.4 Applications for Prestige 1100

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

1.4.1 Internet Access

The Prestige 1100 is the ideal high-speed Internet access solution. Your Prestige 1100 supports the TCP/IP protocol that the Internet uses exclusively. A typical Internet access application is shown below:

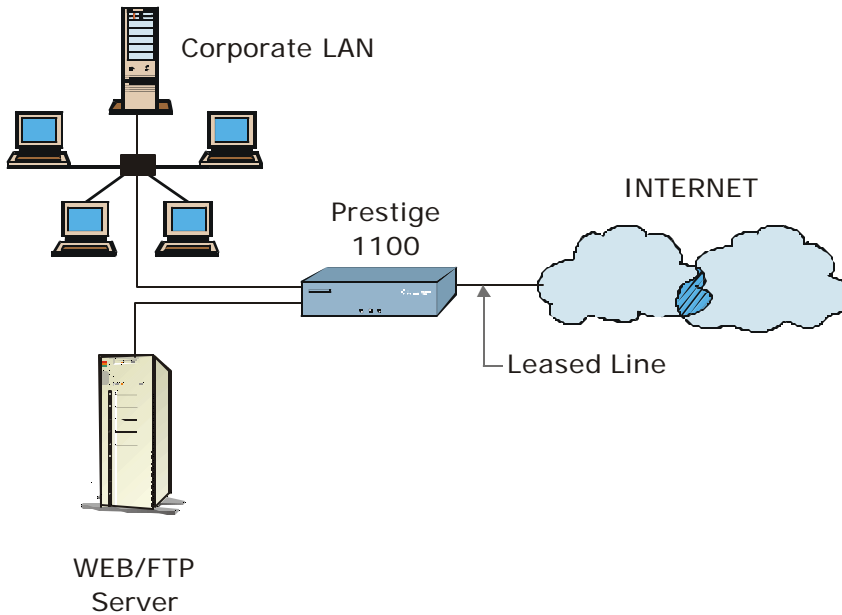


Figure 1-4 Internet Access Application

Internet Single User Account

For a business environment, your Prestige offers the 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. The SUA address mapping can also be used for other LAN to LAN connections.

Multi-protocol/Multilink LAN-to-LAN Connection

You can use the Prestige to connect two geographically dispersed networks over the WAN connection. The Prestige supports TCP/IP and Novell IPX routing, as well as transparent bridging for other network layer protocols. A typical LAN-to-LAN application for your Prestige is shown below:

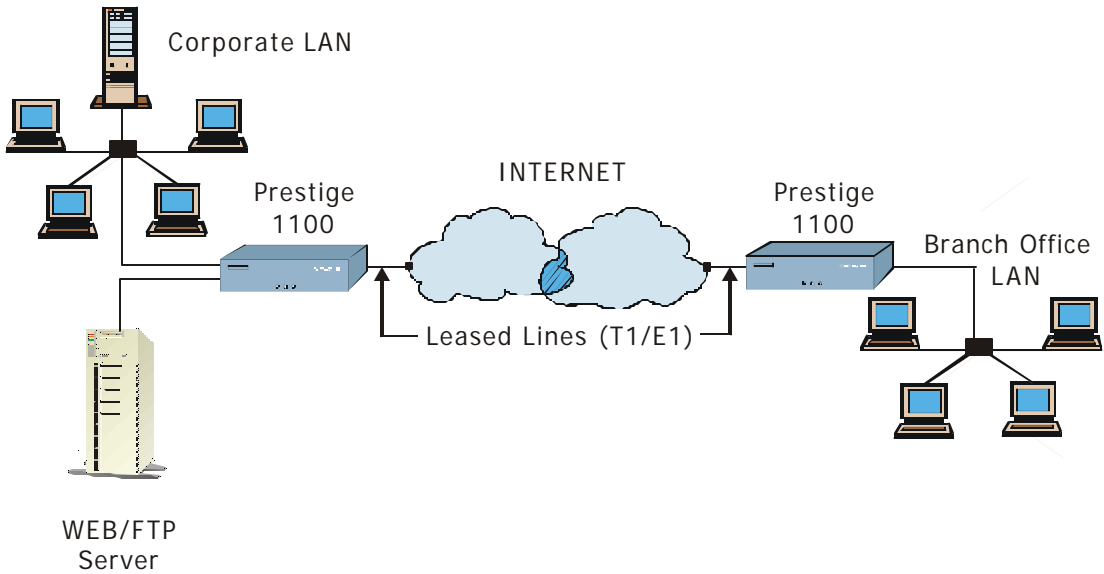


Figure 1-5 LAN-to-LAN Application

Chapter 2: Hardware Installation & Initial Setup

2.1 Unpacking your Bridge/Router

This chapter explains how to connect to the hardware and to perform the initial setup. Before installing be sure that all components listed with the enclosed packing slip are included.

2.2 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:

- A computer with Ethernet 10Base-T or 100Base-TX NIC (Network Interface Card).
- A computer equipped with communications software configured to the following parameters:
 - VT100 terminal emulation.
 - 9600 Baud.
 - No parity, 8 Data bits, 1 Stop bit.
 - Flow Control set to None.

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

2.3 Connect your WAN Bridge/Router

2.3.1 Prestige 1100 Connections

This section outlines how to make the connections to your Prestige 1100. Please refer to the following figure when making connections to the P1100.

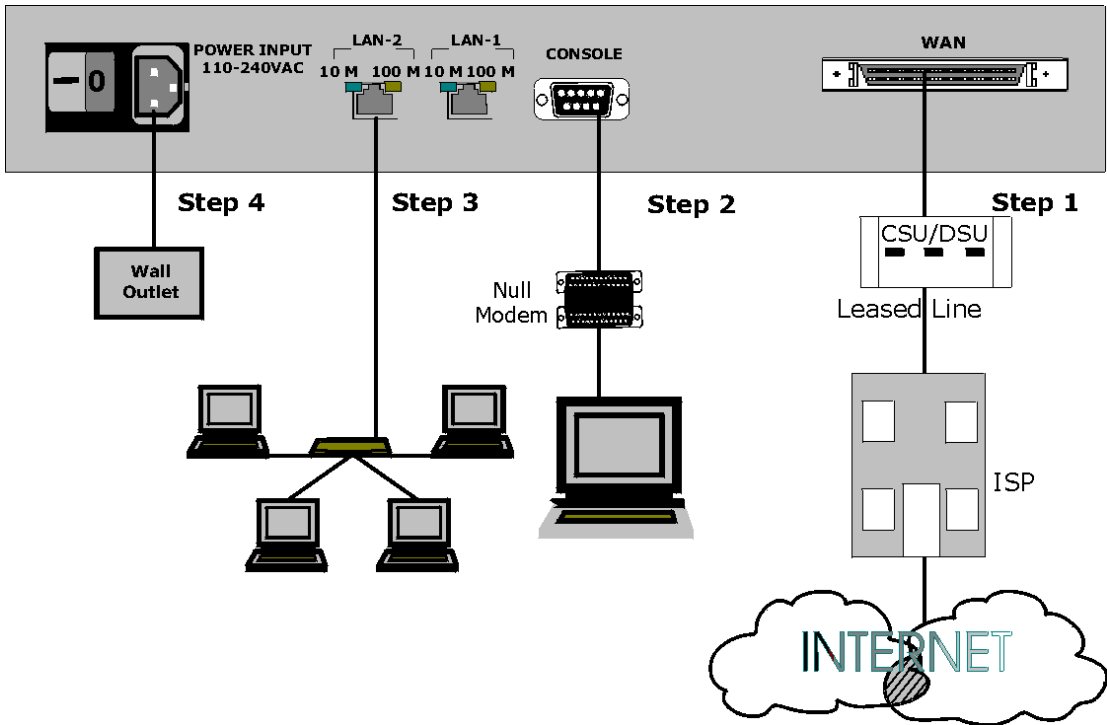


Figure 2-1 P1100 Connections

Step 1. Connect WAN Devices to your Prestige 1100

Connect the port of a WAN device to the WAN port on the Prestige 1100 using an appropriate cable. Please consult the documentation of your WAN device for detailed information when making the connections.

Step 2. Connecting the Console Port

For the initial configuration of your Prestige, you need to use terminal emulator software on a workstation and connect it to the Prestige through the console port. A modem can be connected directly to the Prestige console port for remote configuration (see *Figure 1-1*). The PC - Prestige console port direct connection must be made via a null modem (supplied). The Prestige console port is

a DTE (Data Terminal Equipment) device, not a DCE (Data Circuit-terminating Equipment) device, so the null modem is needed to allow connection to the workstation console port, which is of course a DTE device also. Connect the 9-pin (smaller) end of the console cable to the console port of the Prestige and the 25-pin (bigger) end to the null modem. Then connect the null modem 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 or via a modem connection. See the *Telnet Configuration and Capabilities* chapter for more information on using telnet to configure your Prestige.

Step 3. Connect your Prestige 1100 to Ethernet

Connect one end of a STP (Shielded Twisted Pair) cable to the Ethernet port of the Prestige 1100 and the other to a hub using a straight-through cable with RJ-45 connectors. If you connect the Prestige 1100 to a workstation directly without a hub, you must use a crossover cable.

Step 4. Connect the Power Cord to your Prestige 1100

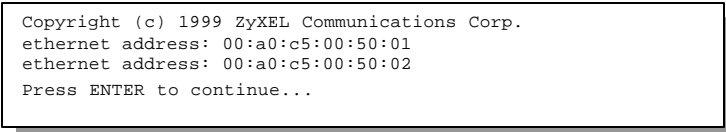
Connect the power cord to the port labeled POWER INPUT on the rear panel of your Prestige 1100.

2.4 Power On Your Prestige 1100

At this point, you should have connected the console cable, the WAN device, the Ethernet cable(s), and the power cord. You can now power on your Prestige 1100 by flipping the power switch to on. (Note: “**I**” = ON, “**O**” = OFF)

Initial Screen

When you power on your Prestige 1100, the router performs several internal tests and initializes the WAN devices. After the initialization, the Prestige asks you to press [ENTER] to continue, as shown below:



```
Copyright (c) 1999 ZyXEL Communications Corp.  
ethernet address: 00:a0:c5:00:50:01  
ethernet address: 00:a0:c5:00:50:02  
Press ENTER to continue...
```

Figure 2-2 Power-On Display

Step 1. Enter Password

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

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

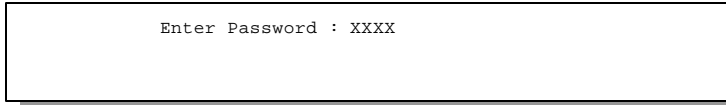


Figure 2-3 Login Screen

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

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 Table 2-1.

Table 2-1 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 [ENTER] key to move back to the previous menu.
Move to a "hidden" menu	Press the [Space bar] to change [No] to [Yes] then press [ENTER].	Fields beginning with "Edit" lead to hidden menus and have a default setting of [No]. Press the [Space bar] to change [No] to [Yes], then press [ENTER] to go to a "hidden" menu.
Move the cursor	[ENTER] or [Up]/[Down] arrow keys	Within a menu, press [ENTER] to move to the next field. You can also use the [Up]/[Down] arrow keys to move to the previous and the next field, respectively.
Enter information	Fill in, or Press the [Space bar] to toggle	There are two types of fields that you will need to fill in. The first requires you to type in the appropriate information. The second gives you choices to choose from. In the second case, press the [Space bar] to cycle through the available choices.
Required fields	<?>	All fields with the symbol <?> must be filled in order to be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is not available.
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.

The SMT displays the Main Menu, as shown below:

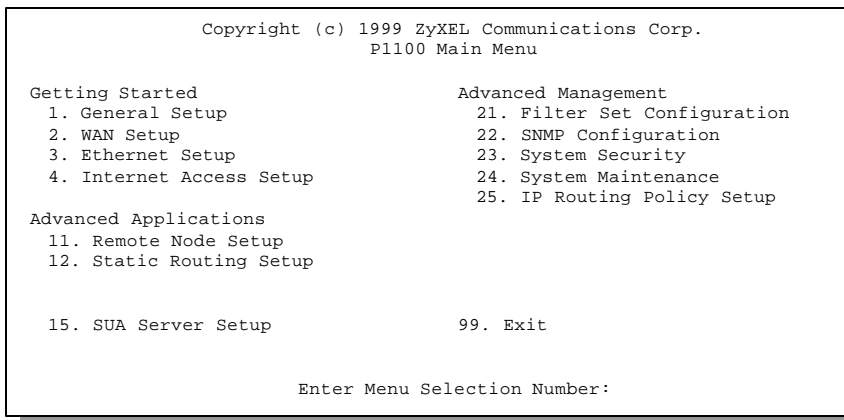


Figure 2-4 SMT Main Menu

The following table shows the Main Menu Summary,

Table 2-2 Main Menu Summary

#	Menu Title	Description
1	General Setup	Use this menu to setup general information and enable routing or bridging of specific protocols.
2	WAN Setup	Use this menu to setup the WAN port configuration.
3	Ethernet Setup	Use this menu to setup the Ethernet configuration.
4	Internet Access Setup	A quick and easy way to setup Internet connection.
11	Remote Node Setup	Use this menu to setup the remote node for LAN-to-LAN connection, including Internet connection.
12	Static Routing Setup	Use this menu to setup static route for different protocols. There are eight static routes for each protocol.
15	SUA Server Setup	Use this menu to specify inside servers when SUA is selected.
21	Filter Set Configuration	Setup filters to be used in Menu 3 and Menu 11 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	Provides system status, diagnostics, firmware upload, etc.
25	IP Routing Policy Setup	Setup configuration for Routing Policies.
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.** Select option **23. System Security** in the Main Menu. This will open Menu 23 - System Security as below:

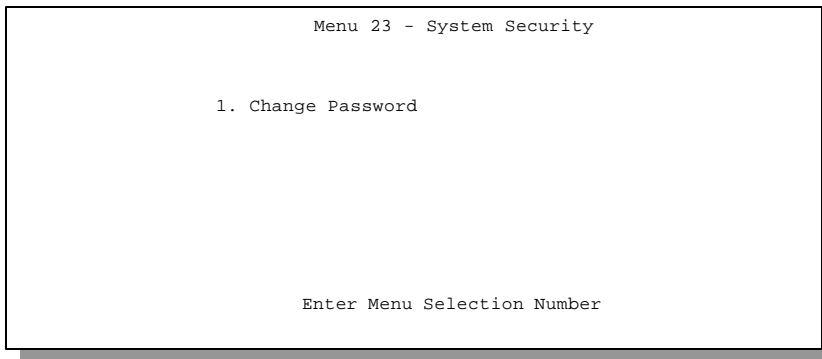


Figure 2-5 Menu 23 - System Security

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

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

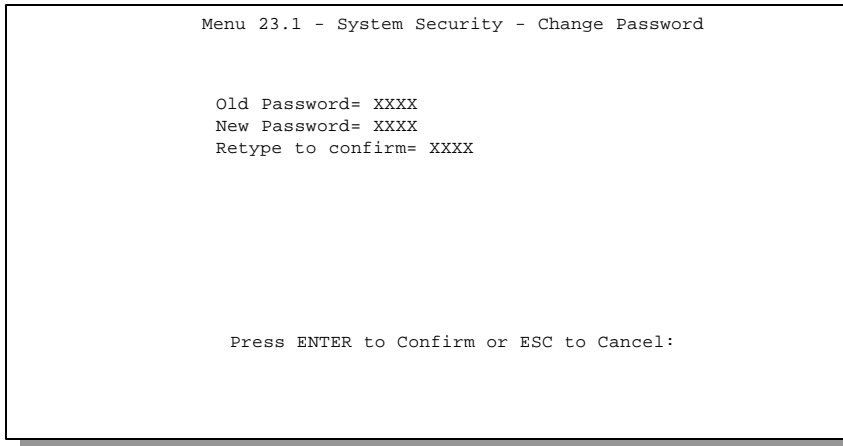


Figure 2-6 Menu 23.1 - System Security - Change Password

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

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

2.7 General Setup

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

- Step 1.** Select option **1. General Setup** in the Main Menu by typing 1 at the menu selection number prompt.
- Step 2.** The Menu 1 - General Setup screen appears, as shown. Fill in the required fields marked [?] and turn on the individual protocols for your particular application, as explained in the following table.

```
Menu 1 - General Setup

System Name= pl100
Location= location
Contact Person's Name= name

Route IP= Yes
Route IPX= No
Bridge= No

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

Figure 2-7 Menu 1 - General Setup

Table 2-3 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 and will be displayed at the prompt in the Command Mode.	P1100
Location (optional)	Enter the geographic location (up to 31 characters) of your Prestige 1100.	location
Contact Person's Name (optional)	Enter the name (up to 8 characters) of the person in charge of this Prestige 1100.	name
Protocols:	Turn on or off the individual protocols for your particular application.	Press space-bar to toggle
Route IP	Selecting [Yes] to enable IP routing. You must enable IP routing for Internet access.	[Yes/No]
Route IPX	Selecting [Yes] to enable IPX routing.	[Yes/No]
Bridge	Selecting [Yes] to enable bridging. Packets that the Prestige 1100 does not route are transparently bridged.	[Yes/No]

2.7.1 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 layer protocol, and uses more CPU cycles and memory.

2.8 WAN Setup

This section describes how to configure the WAN port and a WAN device using Menu 2- WAN Setup. When you finish the setup, the Prestige uses this information to initialize the WAN port and the attached WAN device.

2.8.1 Prestige 1100 WAN Port Setup

Select option **2. WAN Setup** in the Main Menu by typing **2** at the menu selection number prompt.

```

Menu 2 - WAN Port Setup

Clock Source = External
Port Speed = N/A

Press Enter to Confirm or ESC to Cancel:

Press Spacebar to Toggle

```

Figure 2-8 Menu 2 - WAN Port Setup

Table 2-4 WAN Setup Menu Fields

Field	Description	Example
Clock Source	An external device controls timing. The P1100 currently <i>only</i> supports an external clock source.	External
Port Speed	Set by External Device	N/A

2.9 Ethernet Setup

This section describes how to configure the Ethernet using Menu 3 – Ethernet Setup. There are actually three Menu 3s:

- 1st. **Menu 3 – Ethernet Setup** – allows you to select the LAN (1 or 2) you wish to configure.
- 2nd. **Menu 3 - Ethernet Setup (LAN 1)** – allows you to configure the LAN 1 Ethernet interfaces. Choose 1 from the first Menu 3 to get to this menu.
- 3rd. **Menu 3 - Ethernet Setup (LAN 2)** – allows you to configure the LAN 2 Ethernet interfaces. Choose 2 from the first Menu 3 to get to this menu.

From the Main Menu, enter 3 to bring up (the first) **Menu 3 – Ethernet Setup**. Select the LAN that you wish to configure.

```
Menu 3 - Ethernet Setup

1. LAN1
2. LAN2
```

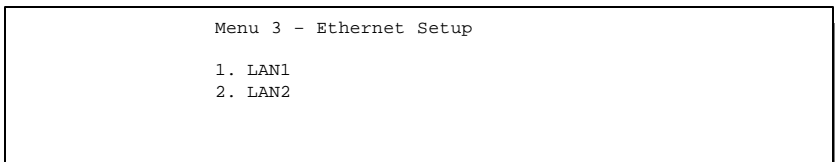


Figure 2-9 Menu 3 - Ethernet Setup - Select LAN

Select 1 to bring you to **Menu 3 - Ethernet Setup (LAN 1)** that you will use to configure the Ethernet interfaces. These submenus are also identical for **Menu 3 - Ethernet Setup (LAN 2)**.

```
Menu 3 - Ethernet Setup (LAN 1)

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

Enter Menu Selection Number:
```

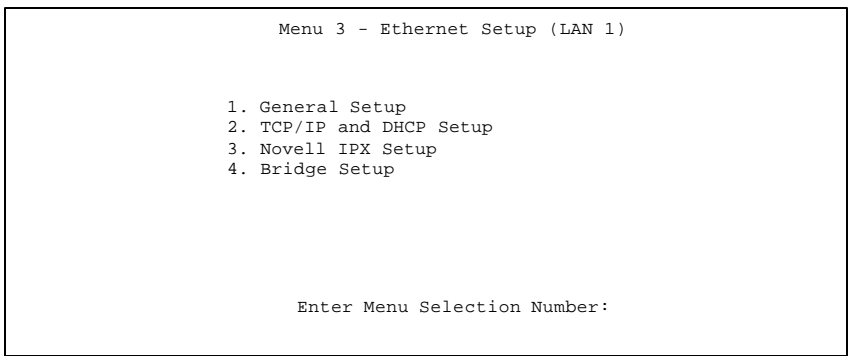


Figure 2-10 Menu 3 – Ethernet Setup

2.10 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 sets may be useful to block certain packets, reducing traffic and preventing security breaches.

From Menu 3 - Ethernet Setup, enter 1 to go to Menu 3.1 -General Ethernet Setup.

```
Menu 3.1 - General Ethernet Setup

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

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

Figure 2-11 Menu 3.1 - General Ethernet Setup

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

2.11 Protocol Dependent Ethernet Setup

For the protocol-dependent setup, go to the appropriate section for details:

- For TCP/IP Ethernet Setup refer to - *Internet Access Application*.
- For Novell IPX Ethernet Setup refer to - IPX Ethernet Setup in - *Novell IPX Configuration for LAN-to-LAN*.
- For Bridge Ethernet Setup refer to - *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 **1. General Setup** and press [ENTER]. Set the [Route IP] field to [Yes] by pressing the space bar as shown in Figure 3-1.

```
Menu 1 - General Setup

System Name= pl100
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 (Internet Service Provider) 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 1100. 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 1100.

The subnet mask specifies the network number portion of an IP address. Your Prestige 1100 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 1100 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 1100 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 1100 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 1100 has the DHCP server capability built-in. The DHCP server is disabled when [DHCP=] is [None.] When [DHCP=] is [Client,]the Prestige requests an IP address from a DHCP server on the Ethernet on which the [DHCP] field is set to [Client].

IP Pool Setup

The Prestige 1100 is pre-configured with a pool of 6 IP addresses.

DNS Server Address(es)

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(s) is extremely important because without it, you must know the IP address of a machine before you can access it. The DNS server address(es) that you enter in the DHCP setup is passed to the client machines along with the assigned IP address and subnet mask. Make sure that you obtain the IP address of the DNS server(s) from your ISP. Your workstations will need this information even if you don't use the Prestige 1100's DHCP server.

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 and DHCP Ethernet Setup

You will now use Menu 3.2 to configure the Ethernet of your Prestige 1100 for TCP/IP.

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

```

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= 192.168.1.1
IP Subnet Mask= 255.255.255.0
RIP Direction= Both
Version= RIP-2B
Multicast = IGMP-v2
IP Policies=
SUA= No

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

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

Table 3-1 DHCP Ethernet Setup Menu Fields

Field	Description	Example
DHCP Setup		
DHCP=	This field enables/disables the DHCP server or client. If it is set to [Server], your Prestige will act as a DHCP server. If set to [None], the DHCP server will be disabled. If set to [Client], the Prestige will request an IP address from the Ethernet that has this field set to [Client.]The Ethernet that has this field set to [Client]also has multicast support ([Multicast= None]) disabled.	[None](default) [Server] [Client]
Client IP Pool Starting Address	When DHCP [Server] is used, the following items need to be set: This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size, or count, of the IP address pool.	6
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	

Follow Table 3-2 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 1100 in dotted decimal notation.	192.168.1.1
IP Subnet Mask	Your Prestige 1100 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the value computed by the Prestige 1100.	255.255.255.0
RIP Direction	Press the space bar to select the RIP direction among [Both]/[In Only]/[Out Only]/[None]	[Both] (default)
Version	Press the space bar to select the RIP version among [RIP-1]/[RIP-2B]/[RIP-2M].	[RIP-1] (default)
Multicast	Turn on/off IGMP support and select the version from [IGMP-v2]/[IGMP-v1]/[None]. This field is disabled if [DHCP=]is set to [Client].	[IGMP-v2]
IP Policies	You can apply up to four IP Policy sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11	
SUA	Press the space bar to select [Yes]to enable SUA on the Ethernet.	[No] (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 IP Multicast

Traditionally, IP packets are transmitted in two ways - unicast or broadcast. Multicast is a third way to deliver IP packets to a group of hosts. Host groups are identified by class D IP addresses, i.e., those with “1110” as their higher-order bits. In dotted decimal notation, host group addresses range from 224.0.0.0 to 239.255.255.255. Among them, 224.0.0.1 is assigned to the permanent IP hosts group, and 224.0.0.2 is assigned to the multicast routers group.

IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC2236). IP hosts use IGMP to report their multicast group membership to any immediate-neighbor multicast routers so the multicast routers can decide if a multicast packet needs to be forwarded. At start up, the Prestige queries all directly connected networks to gather group membership. After that, the Prestige updates the information by periodic queries. The Prestige implementation of IGMP

is also compatible with version 1. The multicast setting can be turned on or off on Ethernet and remote nodes.

For IP routing policy information, please refer to Chapter 13: IP Routing Policy.

3.5 Internet Access Configuration

Menu 4 allows you to enter the Internet access parameters in one screen. Menu 4 is actually a simplified setup for one of the remote nodes that you can access through menu 11. Before you configure your Prestige 1100 for Internet access, you need to collect your Internet account information from your ISP. Use Table 3-3 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)	—
Login Name	—
Password	—
DNS server address(es) for your workstations	—

From the Main Menu, enter option **4** to go to **Menu 4 - Internet Access Setup**, as displayed in the next figure.

```
Menu 4 - Internet Access Setup
      ISP's Name= ?
      My Login=
      My Password= *****
      Single User Account= No
      My IP Addr= N/A

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

Figure 3-3 Menu 4 - Internet Access Setup

Table 3-4 contains instructions on how to configure your Prestige 1100 for Internet access.

Table 3-4 Internet Access Setup Menu Fields

Field	Description	Observation
ISP's Name	Enter the name of your Internet Service Provider. (This information is for identification purposes only.)	myISP
My Login Name	Enter the login name assigned to you by your ISP.	(required)
My Password	Enter the password associated with the login name above. Note that this login name/password pair is only for your Prestige 1100 to connect to the ISP's gateway. For TCP/IP applications, e.g., FTP, you will need a separate login name and password for each server.	(required)
Single User Account	See Section 3.5 for a detailed discussion on the Single User Account feature.	[Yes/No]
Press [ENTER] at the message [Press ENTER to Confirm ...] to confirm your configuration, or press [ESC] at any time to cancel.		

3.6 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).

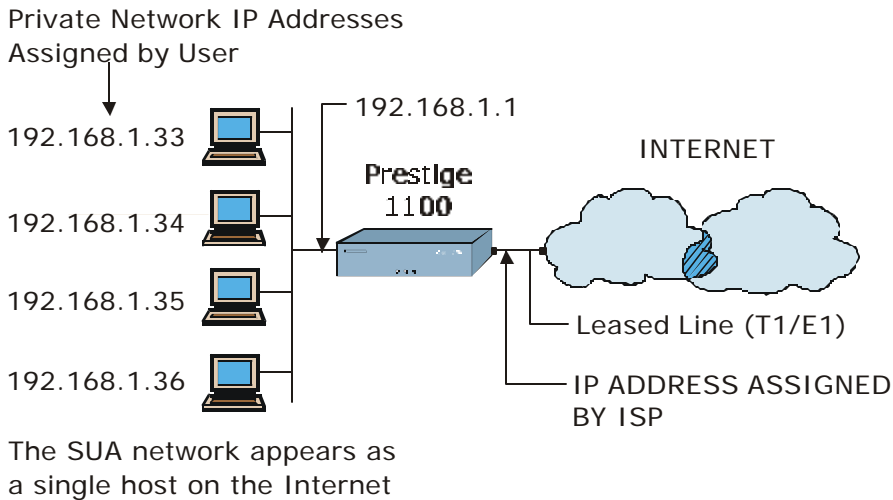


Figure 3-4 Single User Account Topology

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. In addition, you can designate servers, e.g., a web server, on your local network and make them accessible to 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)*.

3.6.1 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 any server. All incoming inquiries will be filtered out by your Prestige 1100.
- UDP and TCP datagrams can be routed. In addition, partial ICMP, including echo (ping) and trace route, is supported.

3.6.2 Single User Account Configuration

The steps for configuring your Prestige for Single User Account are identical to the conventional Internet access (See configuration instructions in Table 3-4) with the exception that you need to fill in two extra fields in **Menu 4 - Internet Access Setup**, as shown in the following figure. SUA here is applied solely to the output interface and is valid *only* for LAN -- WAN connections and *not* for connections between LANs.

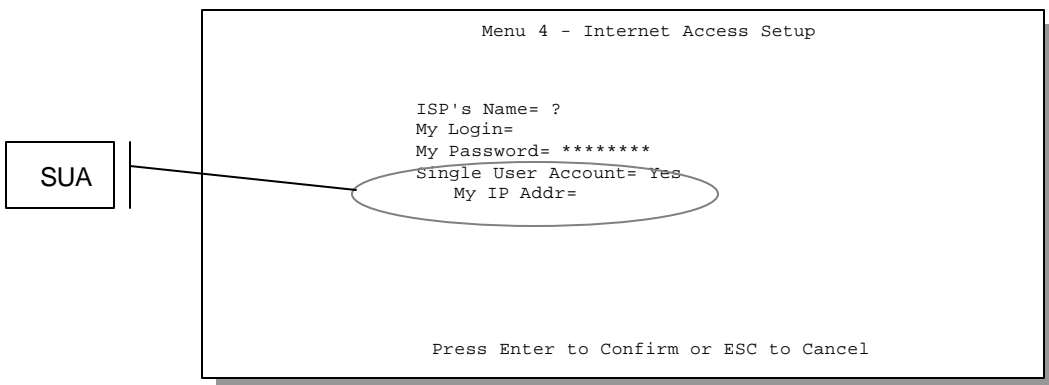


Figure 3-5 Menu 4 - Internet Access Setup for Single User Account

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 in the following table.

Table 3-5 Single User Account Menu Fields

Field	Description
Single User Account	Select [Yes] to enable SUA.
My IP Addr.	If your ISP did <i>not</i> assigns you a static IP address, enter [0.0.0.0]; 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.	

3.6.3 Ethernet SUA

The Single User Account (SUA) feature can also apply to Ethernet ports. This feature is useful if you connect a broadband device such as a xDSL modem or cable modem via the Ethernet port. As there can be only one interface to the Internet at any one time you should not enable both the WAN SUA (Menu 4) and Ethernet SUA (Menu 3.2) at the same time. In the example in Figure 3-6 Ethernet SUA, the ADSL modem is configured as a bridge, so the DHCP server – Ethernet connection is equivalent to a LAN-to-LAN connection. When [DHCP=] [Client] on the Ethernet in Menu 3.2, then the Prestige will request an IP address from the DHCP server as shown. Address translation takes place when [SUA=] [Yes] (in Menu 3.2). The Single User Account (SUA) feature in Menu 3.2 applies solely to the Ethernet interface.

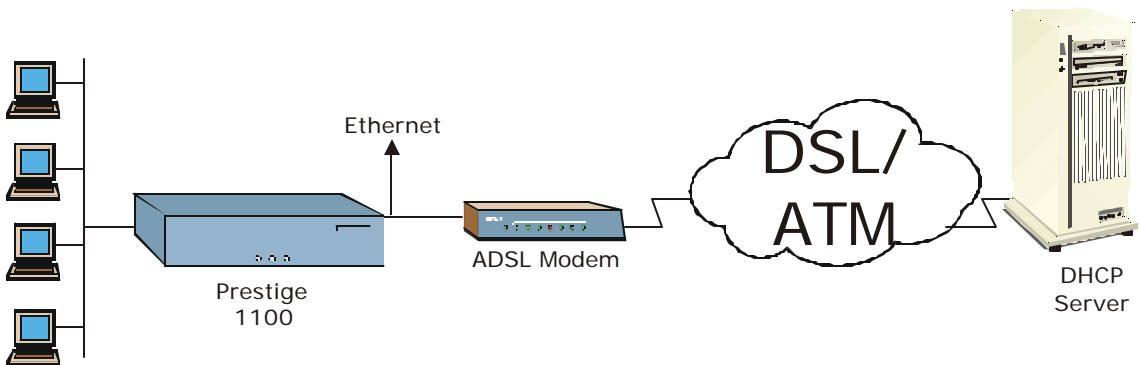


Figure 3-6 Ethernet SUA Example

3.7 LANs & WANs

A LAN (Local Area Network) is a computer network limited to the immediate area, usually the same building or floor of a building. A WAN (Wide Area Network), on the other hand is an outside connection to another network or the Internet.

3.7.1 LANs, WANs and the Prestige

The actual physical connection determines whether the Prestige ports are LAN or WAN ports. There are two separate IP networks, one inside, the LAN network; the other outside, the WAN network as shown next.

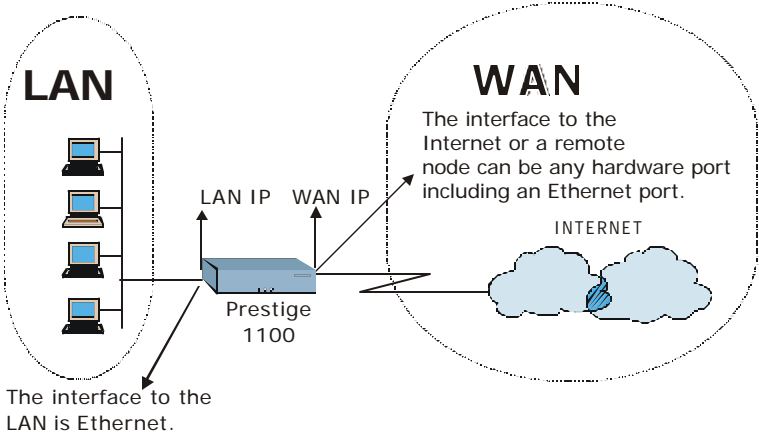


Figure 3-7 LAN & WAN IPs

The following diagram illustrates the Ethernet port as a WAN port.

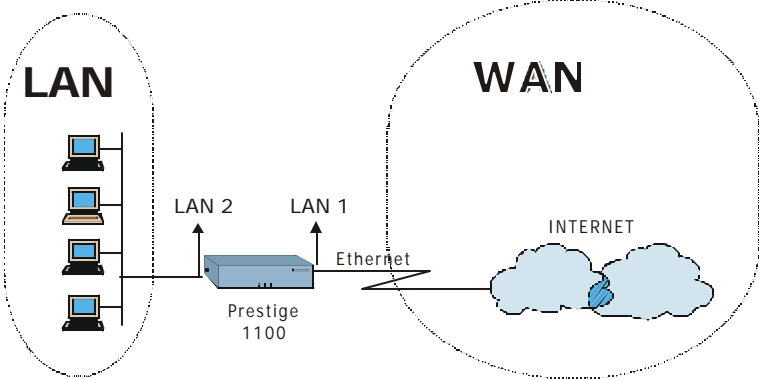


Figure 3-8 Ethernet as WAN port

Chapter 4: Remote Node Configuration for LAN to LAN

A remote node is required for placing calls to a remote gateway. A remote node represents both the gateway and the network behind it across a WAN connection. Note that when you use Menu 4 to set up Internet access, you are actually configuring the remote node.

In this chapter, we will discuss the parameters that are protocol independent. The protocol-dependent configuration will be covered in subsequent chapters.

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

4.1 Leased Line Remote Node Profile

To configure a remote node, enter 11 to select Menu 11.1 - Remote Node Setup.

```

Menu 11.1 - Remote Node Profile

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

                               Edit PPP Options= No
Incoming:                  Rem IP Addr= ?
  Rem Login= ?             Edit IP/IPX/Bridge= No
  Rem Password= *****

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

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

```

Figure 4-1 Menu 11.1 - Remote Node Profile for Leased Lines

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

Table 4-1 Remote Node Profile Menu Fields for Leased Lines

Field	Description	Options
Rem Node Name	This is a required field [?]. Enter a descriptive name for the remote node, e.g., 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].	Press space bar to toggle [Yes/No]
Incoming: Rem Node Login Name	Enter the login name that this remote node will use when it calls your Prestige 1100. The login name in this field combined with the Rem Node Password will be used to authenticate this node.	
Incoming: Rem Node Password	Enter the password used when this remote node calls your Prestige 1100.	
Outgoing: My Login Name	Enter the login name for your Prestige 1100 when it calls this remote node.	
Outgoing: My Password	Enter the password for your Prestige 1100 when it calls this remote node.	
Outgoing: Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: <ul style="list-style-type: none"> ● CHAP/PAP - Your Prestige 1100 will accept either CHAP or PAP when requested by this remote node. ● CHAP - accept CHAP only. ● PAP – accept PAP only. 	[CHAP/PAP] (default) [CHAP] [PAP]
Route	This field determines the protocols that your Prestige 1100 will route.	[IP]/[IPX]/[IP+IPX]/[None]
Bridge	Bridging is used for protocols that the Prestige 1100 does not route, e.g., SNA, or not turned on in the previous Route field. When bridging is enabled, your Prestige 1100 will forward any packet that it does not route to this remote node; otherwise, the packets are discarded. .	Press space bar to toggle [Yes/No]

Field	Description	Options
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> .	Press space bar to toggle [Yes] then press [Enter]
Rem IP Addr	This is a required field [?] if IP routing is enabled. 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.	Press space bar to select [Yes] then press [ENTER]
Session Options: Input Filter Sets, Output Filter Sets	In these fields, enter the filter set(s) you wish to apply to the incoming and outgoing traffic between this remote node and your Prestige 1100. You can choose from 12 different filter sets. In addition, you can link up to 4 filter sets together for further customization, e.g., 1, 5, 9, 12. Note that spaces are accepted in this field. For more information on customizing your filter sets, <i>see Chapter 8</i> . The default is blank, i.e., no filters defined.	Default= Blank
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.		

4.2 Outgoing Authentication Protocol

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

4.3 Editing PPP Options

To edit the remote node 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.

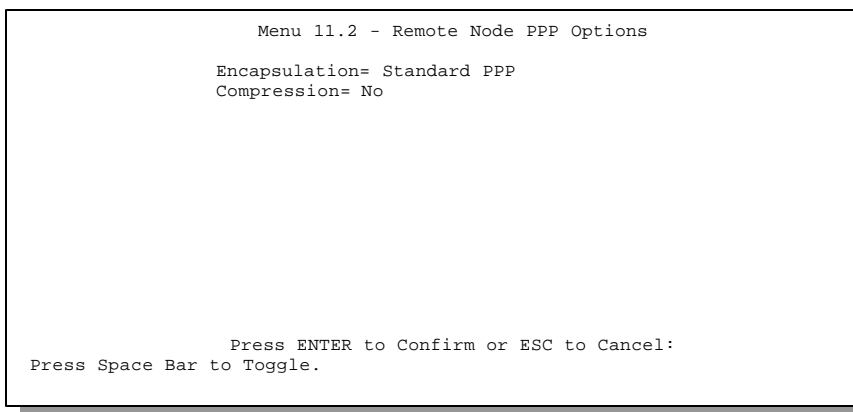


Figure 4-2 Menu 11.2 - Remote Node PPP Options

Table 4-2 Remote Node PPP Options Menu Fields describes the Remote Node PPP Options Menu, and contains instructions on how to configure the PPP options fields.

Table 4-2 Remote Node PPP Options Menu Fields

Field	Description	Option
Encapsulation	<p>Select the vendor-specific encapsulation for the link. The default is Standard PPP. Select Cisco PPP only when the remote gateway is a Cisco machine.</p> <ul style="list-style-type: none"> ● Standard PPP - Standard PPP encapsulation will be used. ● CISCO PPP - Cisco PPP encapsulation will be used. 	<p>[Standard PPP]</p> <p>[CISCO PPP]</p>
Compression	<p>Turn on/off Stac data compression. The default for this field is Off.</p>	<p>[On/Off]</p> <p>(Default = Off)</p>
<p>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.</p>		

Chapter 5: Remote Node TCP/IP Configuration

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

5.1 LAN-to-LAN Application

A typical LAN-to-LAN application is to use your Prestige to connect a branch office to the headquarters, as depicted in the following Figure 5-1.

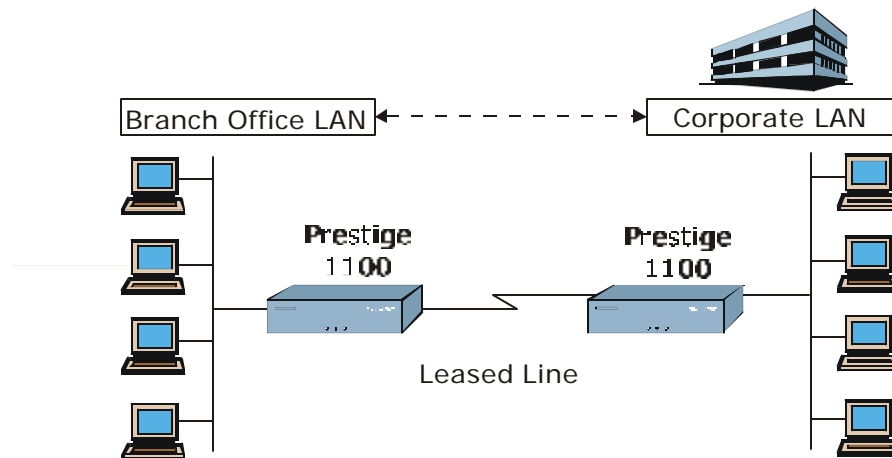


Figure 5-1 LAN-to-LAN Application with TCP/IP

For the branch office, you need to configure static routes if some services reside beyond the immediate remote LAN.

5.2 Remote Node Setup

Follow the procedure in the *Remote Node Configuration Chapter* to configure the protocol-independent parameters in Menu 11 - Remote Node Profile. For the TCP/IP parameters, follow the instructions below.

Follow the steps below to edit **Menu 11.3 - Remote Node Network Layer Options** shown in Figure 5-2:

- Step 1.** 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.)
- Step 2.** Move the cursor to the [Edit IP/IPX/Bridge] field, then press the space bar to toggle and set the value to [Yes], and press [ENTER] to edit **Menu 11.3 - Network Layer Options**.

```
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
  Multicast = IGMP-v2
  IP Policies=

IPX Options:
  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:
  Ethernet Addr Timeout(min)= N/A

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

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

The following diagram in Figure 5-3 explains the Sample IP Addresses to help you to understand the field of My Wan Address in Menu 11.3.

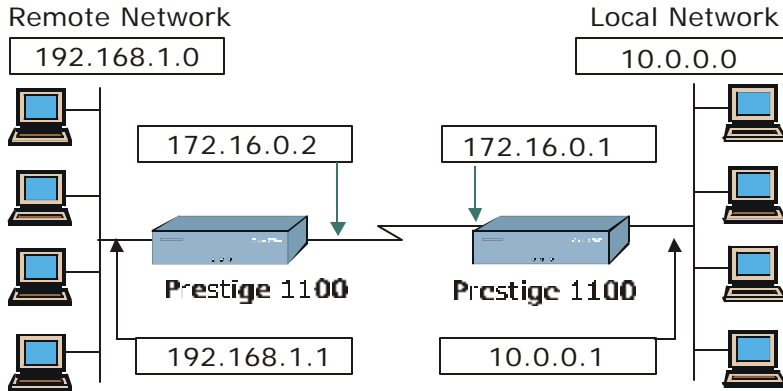


Figure 5-3 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection

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

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 Menu 11.1 - Remote Node Profile. You must fill in either the remote Prestige WAN IP address or the remote Prestige LAN IP address. This depends on the remote router's WAN IP (for the Prestige, the [My WAN Addr] in Menu 11.3 – Remote Node Network Layer Options). For example, if the remote WAN IP is 172.16.0.2 (the remote router's WAN IP), then you should enter 172.16.0.2 in the [Rem IP Address] field. If the remote WAN IP is 0.0.0.0, then enter 192.168.1.1 (the remote router's LAN IP) in the [Rem IP Address] field.	
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])

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

Table 5-2 Remote Node TCP/IP Configuration

Field	Description	Option
Rem IP Address	This shows the IP address you entered for this remote node in the previous menu, Remote Node Profile.	
Rem IP Subnet Mask	Enter the subnet mask for the remote network.	
My WAN Addr	Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your Prestige 1100. Note that this is the address assigned to your local Prestige 1100, not the remote router. (See Figure 5-3 for an explanation of [My WAN Addr] with Sample IP Addresses)	
Single User Account	Set this field to [Yes] to enable the Single User Account feature for your Prestige 1100. Use the space bar to toggle between [Yes] and [No].	[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 [16]. In practice, [2] or [3] is usually a good number.	[1] to [15]
Private	This parameter determines if the Prestige 1100 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]

Field	Description	Option
RIP Direction=	Press the space bar to select the RIP direction from [Both]/[In Only]/[Out Only]/[None].	[Both]/[In Only]/[Out Only]/[None]
Version=	Press the space bar to select the RIP version from [RIP-1]/[RIP-2B]/[RIP-2M].	[RIP-1] [RIP-2B] [RIP-2M]
Multicast	Sets IGMP to version 1, version 2 or disables IGMP.	[IGMP-v2] [IGMP-v1][None]
IP Policies	You can apply up to four IP Policy sets (from twelve) by entering their numbers separated by commas.	e.g., 3, 4, 5, 6
<p>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.</p>		

5.3 Static Route Setup

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

Each remote node specifies only the network to which the gateway is directly connected, and the Prestige has no knowledge of the networks beyond. For instance, the Prestige knows about network N2 in the following diagram through remote node R1. However, the Prestige is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node R1 (via gateway R2). The static routes are for you to tell the Prestige about the networks beyond the remote nodes.

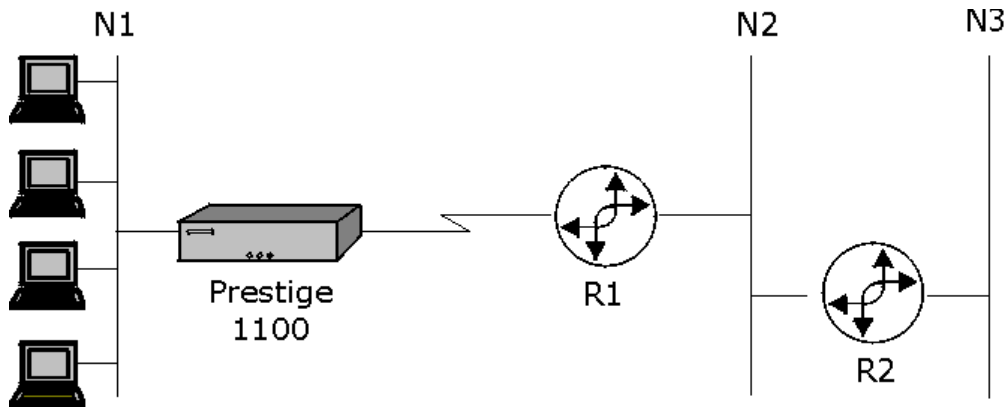


Figure 5-4 Example of Static Routing Topology

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

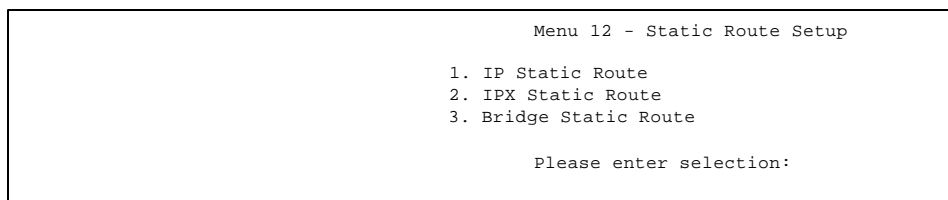


Figure 5-5 Menu 12 - Static Route Setup

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

```
Menu 12.1 - IP Static Route Setup

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

Enter selection number:
```

Figure 5-6 Menu 12.1 - IP Static Route Setup

Choosing a static route to edit produces the following screen.

```
Menu 12.1.1 - Edit IP Static Route

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

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

Figure 5-7 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	Options
Route #	This is the index number of the route as listed in Menu 12.1 – IP Static Route Setup.	
Route Name	Enter a descriptive name for this route. This is for identification purpose only.	
Active	This field allows you to activate/deactivate this static route.	[Yes]/[No]
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.	
IP Subnet Mask	Enter the subnet mask for this destination. Follow the discussion on IP subnet mask in this chapter.	
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Prestige that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Prestige; over WAN, the gateway must be the IP address of one of the remote nodes.	
Metric	Same meaning as those in the Remote Node Setup.	[1] to [15]
Private	Same meaning as those in the Remote Node Setup.	[Yes]/[No]

Chapter 6: IPX Configuration

This chapter shows you how to configure the IPX parameters of the Prestige 1100.

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 1100, we recommend that you set up a NetWare server as a seed router. Even though the Prestige 1100 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 network.

Even though 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.

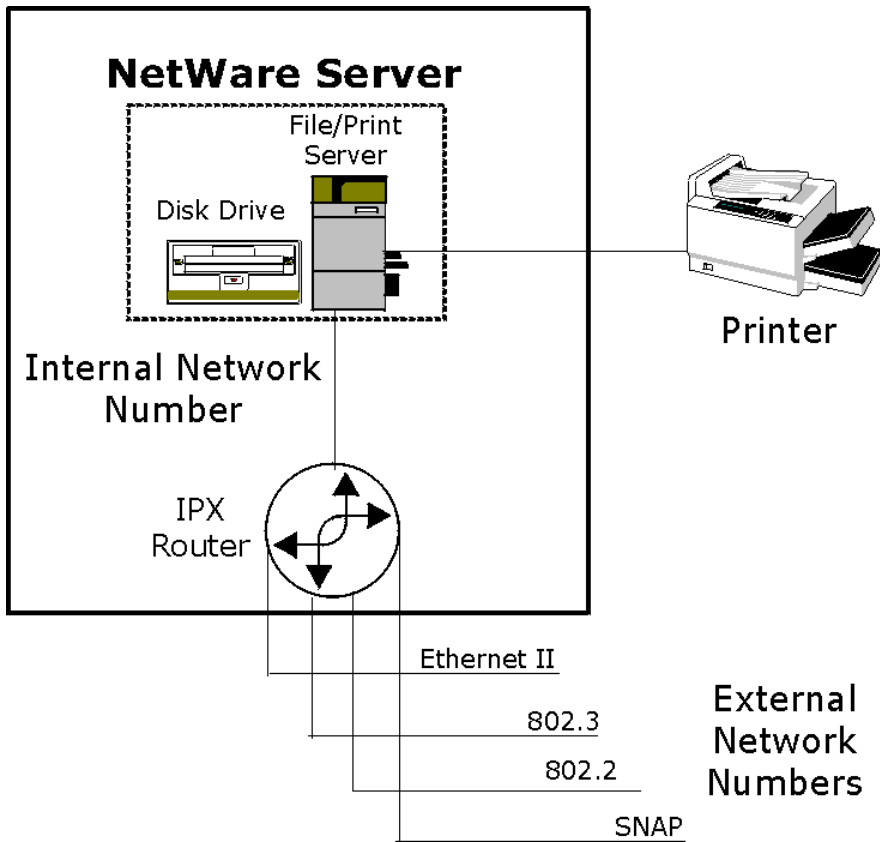


Figure 6-1 NetWare Network Numbers

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 1100 in an IPX Environment

There are two different scenarios in which your Prestige 1100 is deployed:

- LAN with a server (server side)
- LAN without a server (client side)

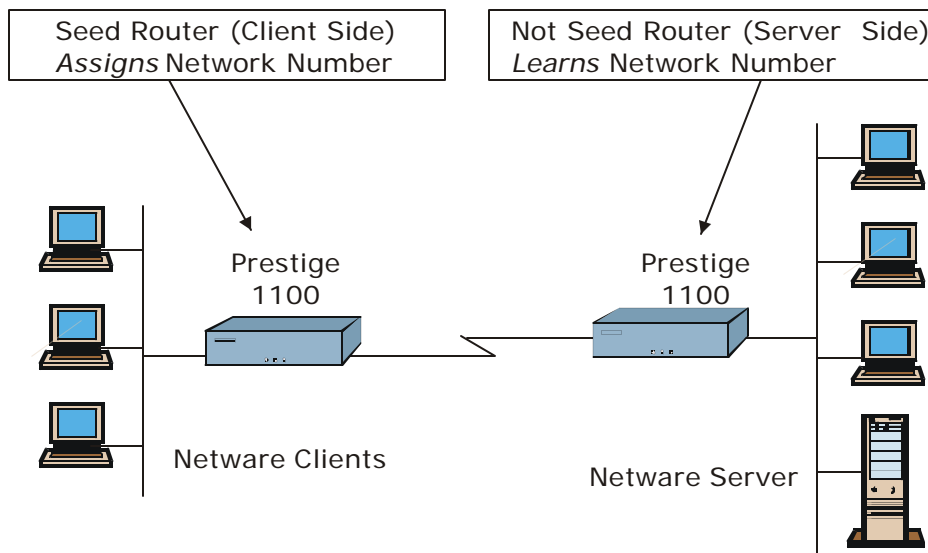


Figure 6-2 Prestige in an IPX Environment

6.2.1 Prestige 1100 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 1100 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 Ethernet Setup

From Menu 3 - Ethernet. Setup, select option **3. Novell IPX Setup** from the appropriate LAN to go to Menu 3.3 - Novell IPX Ethernet Setup as shown in Figure 6-3.

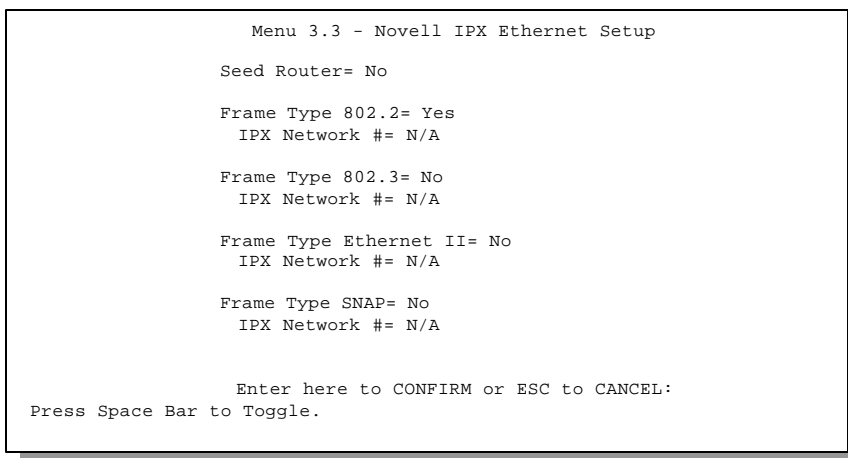


Figure 6-3 Menu 3.3 - Novell IPX Ethernet Setup

The following Table 6-1 describes the Novell IPX Ethernet Setup Menu.

Table 6-1 Novell IPX Ethernet Setup Fields

Field	Description	Options
Seed Router	Determine if your Prestige 1100 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 1100 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.		

6.4 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 Figure 6-4

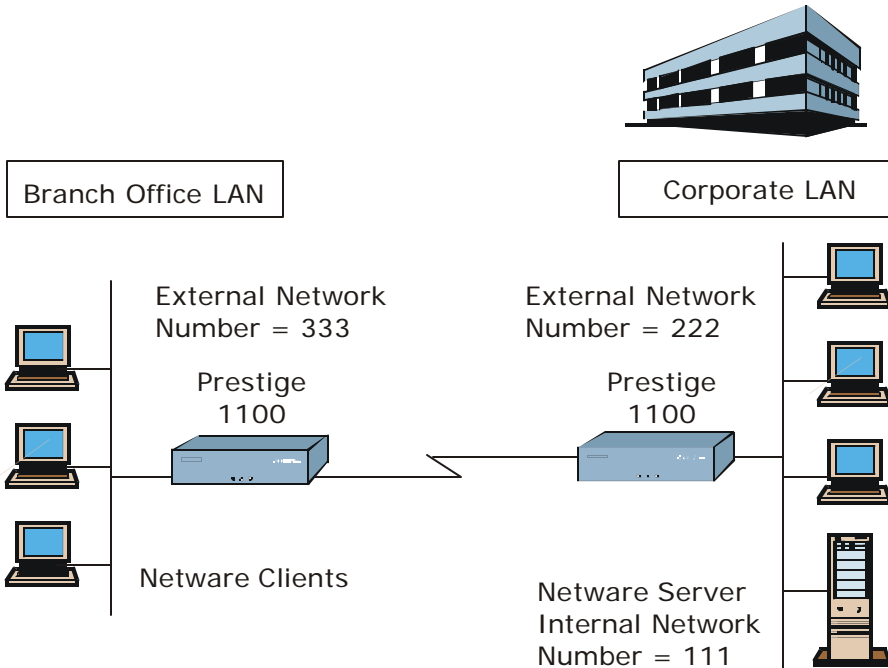


Figure 6-4 LAN-to-LAN Application with Novell IPX

6.4.1 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-related parameters in Menu 11.3 - Remote Node Network Layer Options, follow the instructions below.

To edit Menu 11.3 - Remote Node Network Layer Options shown in Figure 6-5, follow these steps:

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.)

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

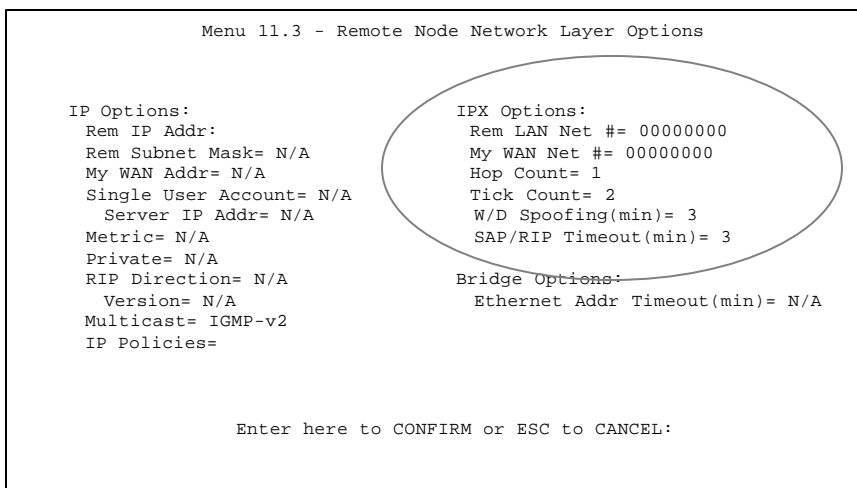


Figure 6-5 Menu 11.3 - Remote Node Novell IPX Options

Table 6-2 describes the IPX protocol-dependent parameters of the remote node Setup.

Table 6-2 Remote Node Novell IPX Options

Field	Description	Option
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 WAN link. If you leave this field as [00000000], your Prestige 1100 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 1100 on the server side. Your Prestige 1100 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 1100 to spoof the WatchDog response.	
SAP/RIP Timeout (min)	This field indicates the amount of time that you want your Prestige 1100 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 1100 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.		

6.4.2 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

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

Figure 6-6 Menu 12.2.1 - 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
Route #	This is the index number of the route as listed in Menu 12.2 – IPX Static Route Setup.
Server Name	In this field, enter the name of the server. This must be the <i>exact</i> name configured in the NetWare server.
Active	This field allows you to activate/deactivate this static route.
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].
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.	

Chapter 7: Bridging Setup

This chapter shows you how to configure the bridging parameters of your Prestige 1100.

7.1 Bridging in General

Bridging bases the forwarding decision on the MAC (Media Access Control), or hardware address, while routing does on the network layer (IP or IPX) address. Bridging allows the Prestige 1100 to transport packets of network layer protocols that the Prestige 1100 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 1100 can route.

7.2 Bridge Ethernet Setup

Basically, all non-local packets are bridged to the WAN, however, your Prestige 1100 applies special handling for certain IPX packets to reduce the number of calls, depending on the setting.

From **Menu 3 - Ethernet Setup**, enter option **4. Bridge Setup** for the appropriate LAN and **Menu 3.4 - Bridge Ethernet Setup** displays as shown in Figure 7-1.

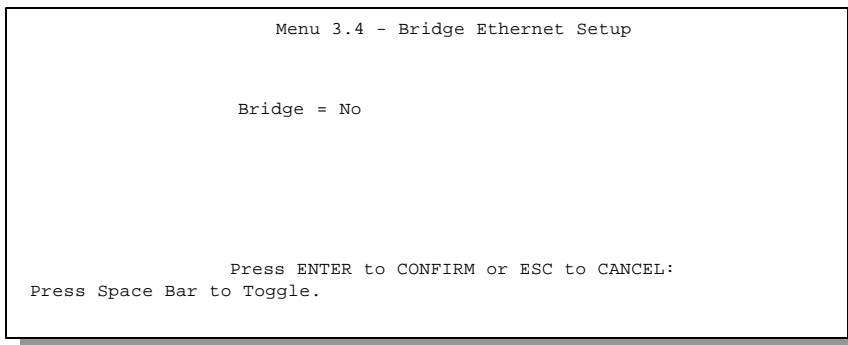


Figure 7-1 Menu 3.5 - Bridge Ethernet Setup

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-related parameters, you need to configure **Menu 11.3 - Remote Node Network Layer Options**.

To setup **Menu 11.3 - Remote Node Network Layer Options** shown in Figure 7-2 Menu 11.3 - Remote Node Bridging 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 bar to toggle and set the value to [Yes], and press [ENTER] to edit **Menu 11.3 - Network Layer Options**.

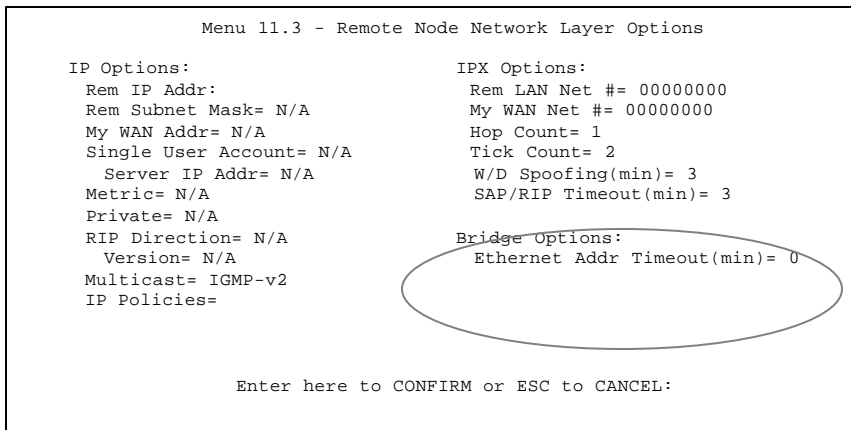


Figure 7-2 Menu 11.3 - Remote Node Bridging Options

Table 7-1 describes the bridging-dependent parameters in the Remote Node Profile and Network Layers menus.

Table 7-1 Remote Node Bridge Options

Field	Description
Bridge (Menu 11)	Make sure this field is set to [Yes].
Edit IP/IPX/Bridge (Menu 11)	Press the space bar to change it to [Yes] and press [ENTER] to go to the Network Layer Options Menu.
Ethernet Addr Timeout (min) (Menu 11.3 above)	In this field, enter the time (number of minutes) that you wish your Prestige 1100 to retain the Ethernet Addr information in its internal tables while the line is down. If this information is retained, your Prestige 1100 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.	

7.2.2 Bridge Static Route Setup

Similar to network layer static routes, a bridging static route tells the Prestige 1100 about the route to a node before a connection is established. You configure bridge static routes in Menu 12.3.1 (go to Menu 12, choose option 3, then choose a static route to edit) as shown in Figure 7-3.

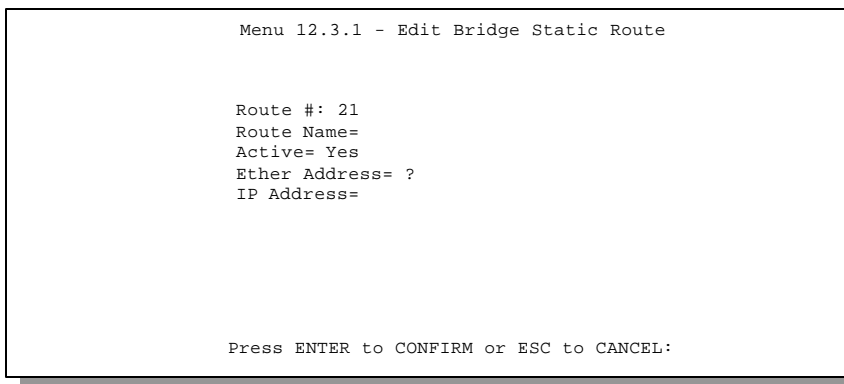


Figure 7-3 Menu 12.3.1 - Edit Bridge Static Route

The following Table 7-2 describes the Bridge Static Route Menu.

Table 7-2 Bridge Static Route Menu Fields

Field	Description
Route #	This is the index number of the route as listed in Menu 12.3 – IPX Static Route Setup.
Route Name	Enter a name for the bridge static route for identification purposes.
Active	Indicates whether the static route is active or not.
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.
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: Filter Configuration

8.1 About Filtering

Your Prestige uses filters to decide whether or not to allow passage of a packet. Data filtering is divided into incoming and outgoing filters, depending on the direction of the packet relative to a port.

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

8.2 The Filter Structure of the Prestige

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

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

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

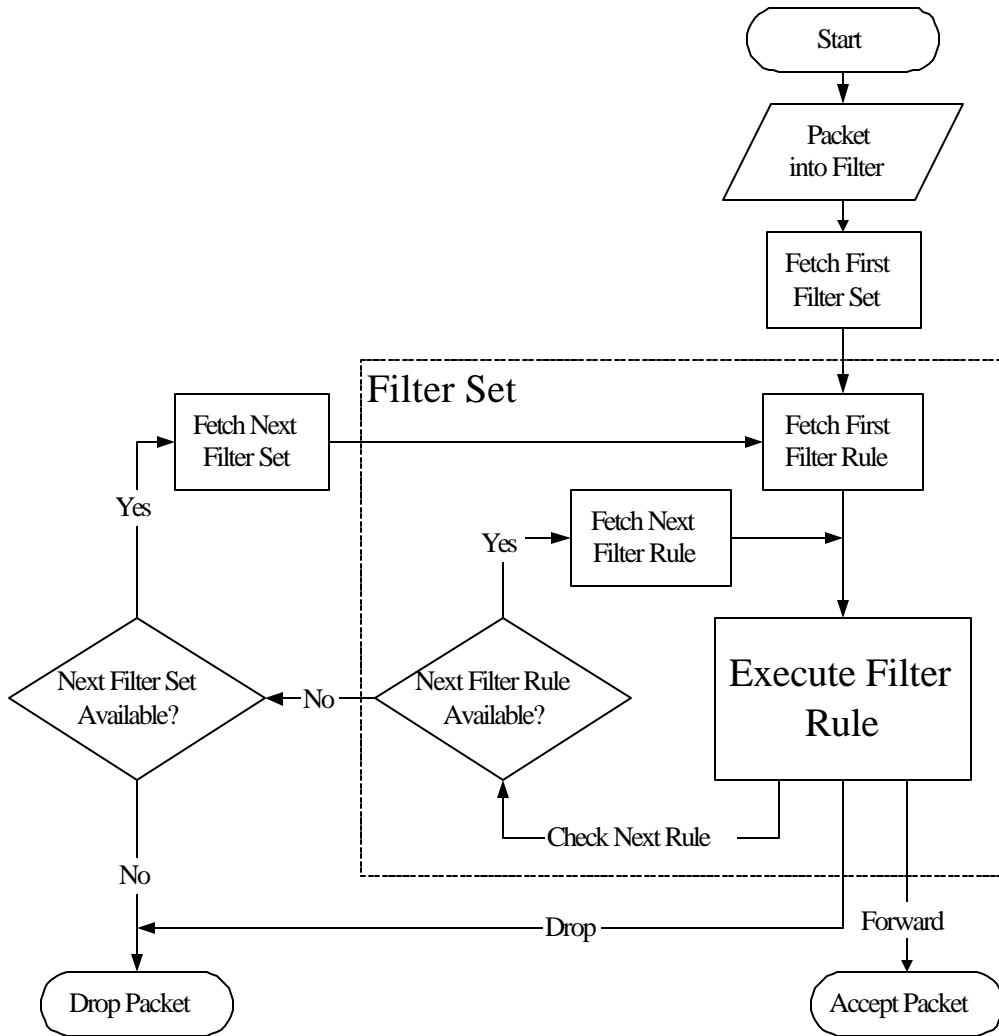


Figure 8-1 Filter Rule Process

8.3 Configuring a Filter Set

To configure a filter sets, follow the procedure below:

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

```
Menu 21 - Filter Set Configuration

Filter      Filter
Set #      Set #
-----
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 8-2 Menu 21 - Filter Set Configuration

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

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

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

```

Menu 21.1 - Filter Rules Summary

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

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

Edit Comments= NetBIOS_WAN

Press ENTER to Confirm or ESC to Cancel:

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

```

Figure 8-3 Menu 21.1 - Filter Rules Summary

8.3.1 Filter Rules Summary Menu

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

Table 8-1 Abbreviations Used in the Filter Rules Summary Menu

Abbreviations	Description	Display
#	Refers to the filter rule number (1-6).	
A	Refers to Active.	[Y] means the filter rule is active. [N] means the filter rule is inactive.
Type	Refers to the type of filter rule. This shows IP for TCP/IP, IPX and Device	[IP] for TCP/IP [IPX] for Novell's IPX protocol [Dev] for Device
Filter Rules	The filter rule parameters are displayed here (see below).	

Abbreviations	Description	Display
M	<p>Refers to More.</p> <p>[Y] means an action can not yet be taken as there are more rules to check, which are concatenated with the present rule to form a rule chain. When the rule chain is complete an action can be taken.</p> <p>[N] means you can now specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.</p> <p>If More is [Yes], then [Action Matched] and [Action Not Matched] will be [N/A].</p>	<p>[Y] means there are more rules to check.</p> <p>[N] means there are no more rules to check.</p>
m	<p>Refers to Action Matched.</p> <p>[F] means to forward the packet immediately and skip checking the remaining rules if any.</p>	<p>[F] means to forward the packet.</p> <p>[D] means to drop the packet.</p> <p>[N] means check the next rule.</p>
n	<p>Refers to Action Not Matched</p> <p>[F] means to forward the packet immediately and skip checking the remaining rules if any.</p>	<p>[F] means to forward the packet.</p> <p>[D] means to drop the packet.</p> <p>[N] means check the next rule.</p>

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 8-2 Abbreviations Used If Filter Type Is IP

Abbreviation	Description
Pr	Protocol
SA	Source Address
SP	Source Port number
DA	Destination Address
DP	Destination Port number

- Abbreviations Used If Filter Type Is IPX

Table 8-3 Abbreviations Used If Filter Type Is IPX

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

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

Table 8-4 Abbreviations Used If Filter Type Is Dev

Abbreviation	Description
Off	Offset
Len	Length

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

8.4 Configuring a Filter Rule

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

8.4.1 Filter Types and SUA

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

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 device filters are applied to the raw packets that appear on the wire. They are applied at the point where the Prestige is receiving and sending the packets; i.e. the interface. The interface can be an Ethernet, or any other hardware port. The following diagram illustrates this.

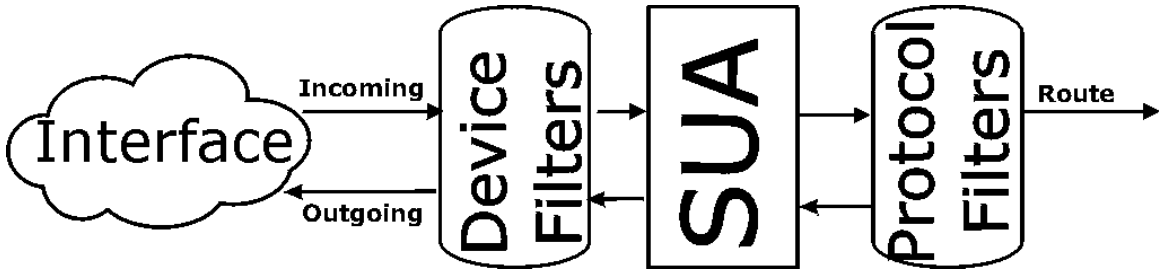


Figure 8-4 Protocol and Device Filter Sets

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

8.4.2 TCP/IP Filter Rule

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

To configure 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= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 137
                Port # Comp= Equal
Source: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 0
                Port # Comp= None

TCP Estab= No
More= No          Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

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

Figure 8-5 Menu 21.1.1 - TCP/IP Filter Rule

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

Table 8-5 TCP/IP Filter Rule Menu Fields

Field	Description	Option
Filter #	This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third filter rule of that set.	
Filter Type	Use the space bar to toggle between types of rules. Parameters displayed below each type will be different.	[Device Filter Rule] / [TCP/IP Filter Rule] / [IPX Filter Rule]
Active	This field activates/deactivates the filter rule.	[Yes]/[No]
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. This value must be between 0 and 255. Enter 0 if IP protocol is don't care.	0-255
IP Source Route	If Yes, the rule applies to packet with IP source route option; else the packet must not have source route option. The majority of IP packets do not have source route.	[Yes]/[No]
Destination: IP Addr	Enter the destination IP Address of the packet you wish to filter. This field is a 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. To filter a single host, enter 255.255.255.255 as the mask.	Subnet mask

Field	Description	Option
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 #.	[None]/[Less]/[Greater]/[Equal]/[Not Equal]
TCP Estab	This field is applicable only when IP Protocol field is 6, TCP. If yes, the rule matches only established TCP connections; else the rule matches all TCP packets.	[Yes]/[No]
More	If yes, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields. If More is [Yes], then Action Matched and Action Not Matched will be [N/A].	[Yes]/[N/A]
Log	Select the logging option from the following: <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.		

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

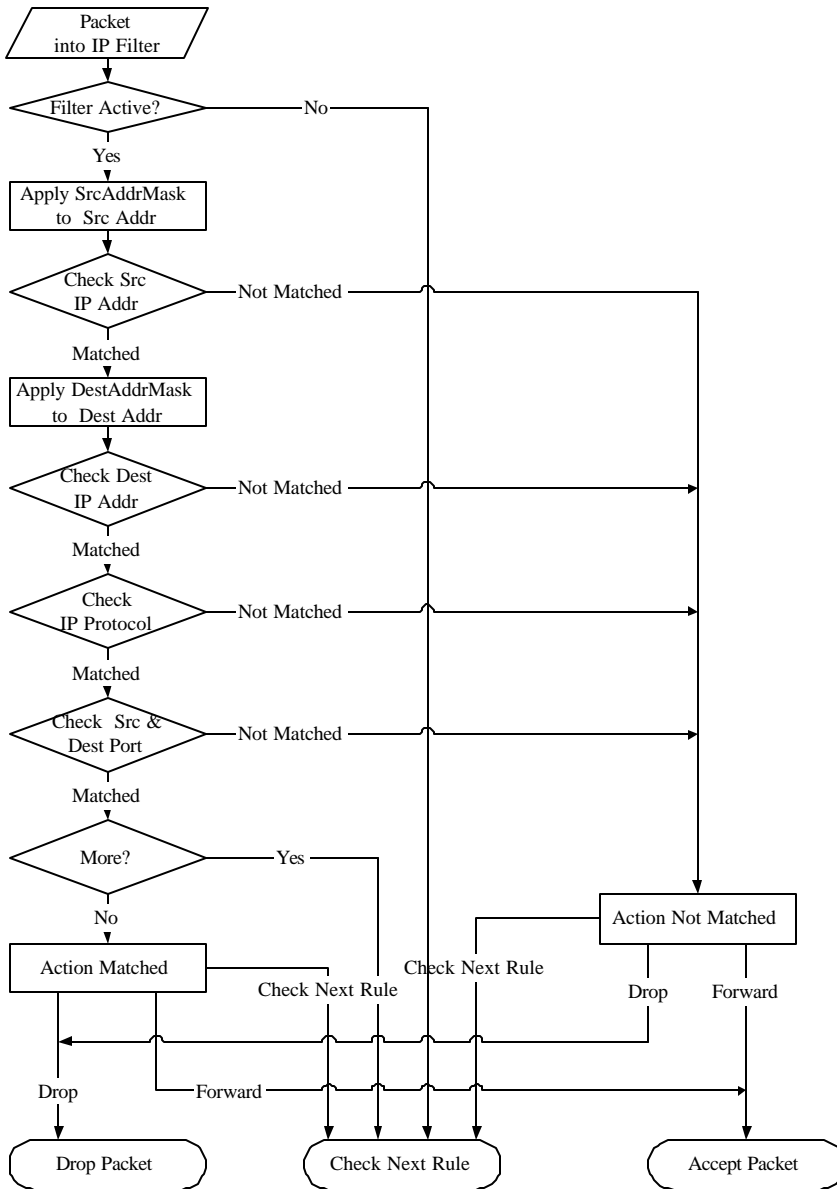


Figure 8-6 Executing an IP Filter

8.4.3 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 21.1.1 IPX Filter Rule**, as shown in the figure below.

```
Menu 21.1.1 - 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 8-7 Menu 21.1.1 - IPX Filter Rule

The table below describes the IPX Filter Rule.

Table 8-6 IPX Filter Rule Menu Fields

Field	Description	Option
Filter #	This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third filter rule of that set.	e.g., 2,3
Filter Type	Use the space bar to toggle between types of rules. Parameters displayed below each type will be different.	[Device Filter Rule] / [TCP/IP Filter Rule] / [IPX Filter Rule]
Active	Select [Yes] to turn on the filter rule.	[Yes]/[No]
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	e.g., 14
Destination Network #	Enter the destination network numbers (4-byte in hexadecimal) of the packet that you wish to filter.	e.g., 22222222
Destination Node #	Enter in the destination node number (6-byte in hexadecimal) of the packet you wish to filter.	e.g., 333333333333
Destination Socket #	Enter the destination socket number (2-byte in hexadecimal) of the packets that you wish to filter.	e.g.,4444
Destination Socket # Comp	Select the comparison you wish to apply to the destination socket in the packet against that specified above.	[None]/[Equal]/[Not Equal]/[Less]/[Greater]
Source Network #	Enter the source network numbers (4-byte in hexadecimal) of the packet that you wish to filter.	e.g., 55555555
Source Node #	Enter in the source node number (6-byte in hexadecimal) of the packet you wish to filter.	e.g., 666666666666

Field	Description	Option
Source Socket #	Enter the source socket number (2-byte in hexadecimal) of the packets that you wish to filter.	e.g.,7777
Source Socket # Comp	Select the comparison you wish to apply to the source socket in the packet against that specified above.	[None]/[Equal]/ [Not Equal]/[Less]/ [Greater]
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.	[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 21.1.1 - 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 .		

8.4.4 Device Filter Rule

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

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

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

```

Menu 21.1.1 - Device Filter Rule

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

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

Figure 8-8 Menu 21.1.2 - Device Filter Rule

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

Table 8-7 Device Filter Rule Menu Fields

Field	Description	Option
Filter #	This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third filter rule of that set.	
Filter Type	Use the space bar to toggle between types of rules. Parameters displayed below each type will be different.	[Device Filter Rule] / [TCP/IP Filter Rule] / [IPX Filter Rule]
Active	Select [Yes] to turn on the filter rule.	[Yes]/[No]
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.	Default = 0
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.	Default = 0
Mask	Enter the mask (in Hexadecimal) to apply to the data portion before comparison.	
Value	Enter the value (in Hexadecimal) to compare with the data portion.	
More	If yes, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields. If More is [Yes], then [Action Matched] and [Action Not Matched] will be [N/A].	[Yes] / [N/A]

Field	Description	Option
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 - Device Filter Rule, press [ENTER] at the message [Press Enter to Confirm] to save your configuration, or press [ESC] to cancel. This data will now be displayed on Menu 21.1 - Filter Rules Summary.

8.5 Applying a Filter

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

8.5.1 Ethernet traffic

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

```

Menu 3.1 - General Ethernet Setup

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

Press ENTER to Confirm or ESC to Cancel:

```

Figure 8-9 Filtering Ethernet Traffic

8.5.2 Remote Node Filters

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

```
Menu 11.1 - Remote Node Profile

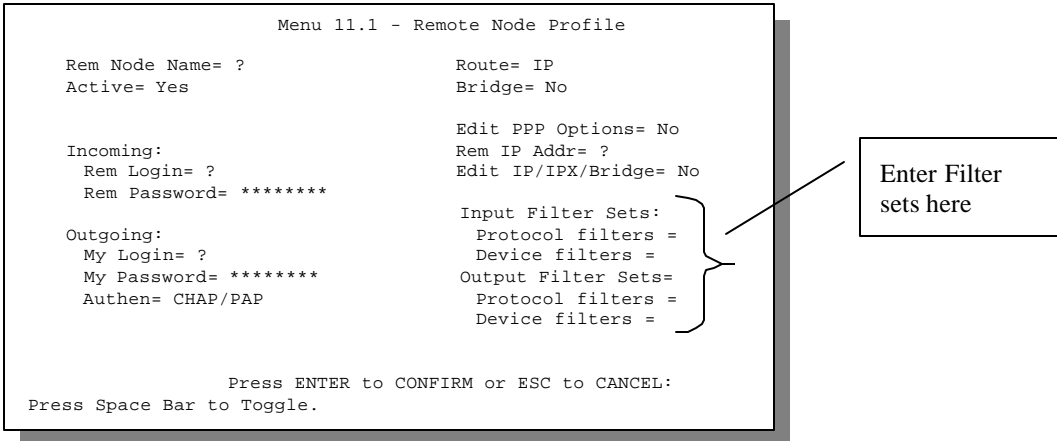
Rem Node Name= ?           Route= IP
Active= Yes                Bridge= No

                               Edit PPP Options= No
                               Rem IP Addr= ?
                               Edit IP/IPX/Bridge= No

Incoming:
  Rem Login= ?
  Rem Password= *****

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

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



Enter Filter sets here

Figure 8-10 Filtering Remote Node traffic

Chapter 9: SNMP Configuration

9.1 About SNMP

SNMP (Simple Network Management Protocol) is a protocol for network management and monitoring. Your Prestige 1100 supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige 1100 through the network. Keep in mind that SNMP is only available if TCP/IP is configured on your Prestige 1100.

9.2 SNMP Configuration

To configure SNMP, select option **22. SNMP Configuration** from the Main Menu to open Menu 22 - SNMP Configuration, as shown in Figure 9-1. 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 9-1 Menu 22 - SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 9-1 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 1100 will only respond to SNMP messages from this address. If you leave the field blank (default), your Prestige 1100 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 10: System Security

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

10.1 Changing the System Password

To change the system password, following steps below:

- Step 1.** Select option **23. System Security** in the Main Menu to open Menu 23 - System Security as shown in Figure 10-1.

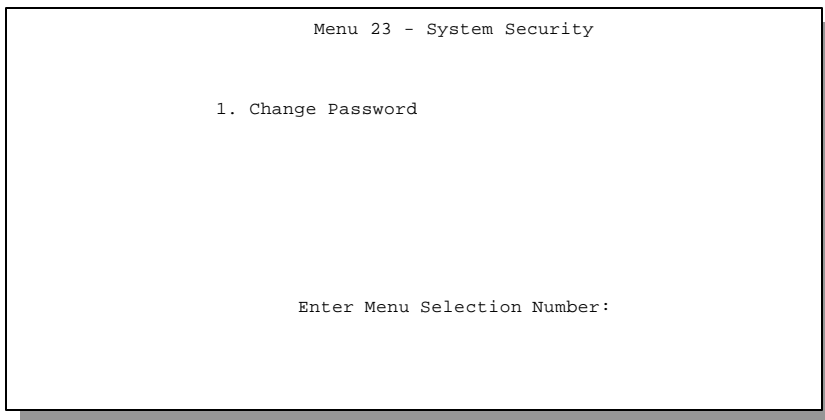


Figure 10-1 Menu 23 - System Security

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

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

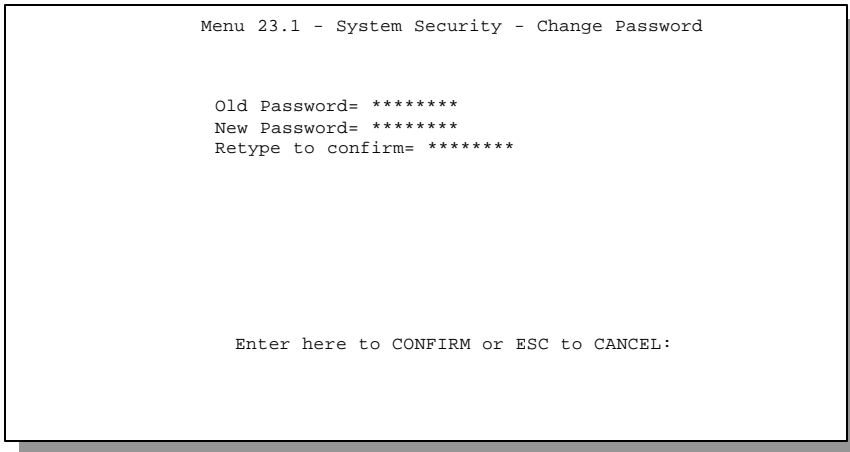


Figure 10-2 Menu 23.1 - System Security - Change Password

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

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

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

Chapter 11: Telnet Configuration and Capabilities

11.1 About Telnet Configuration

Before the Prestige 1100 is properly setup for TCP/IP, the only option for configuring it is through the console port. Once your Prestige 1100 is configured, you can use telnet to configure it remotely.

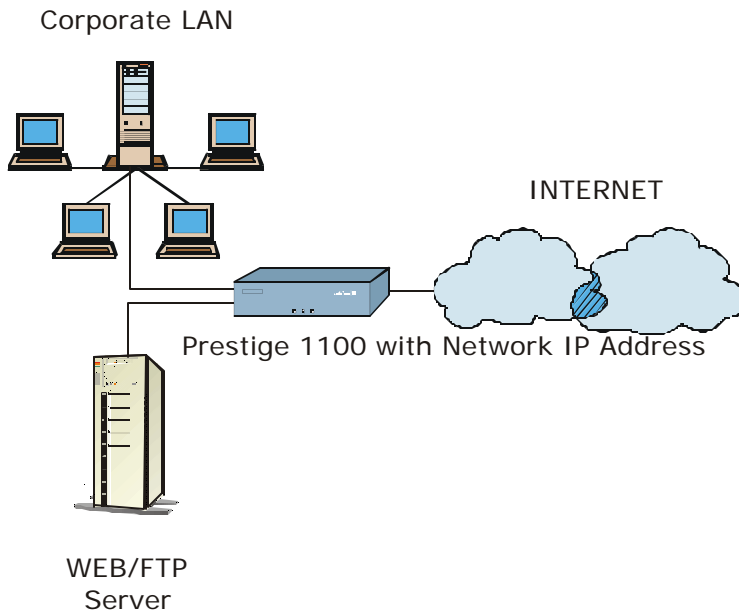


Figure 11-1 Telnet Configuration on a TCP/IP Network

If your Prestige 1100 is configured for IPX but not IP routing in Menu 1, telnet is still available provided you assign the Prestige 1100 a correct IP address and subnet mask. When IP routing is disabled, the Prestige 1100 can still function as a host.

11.2 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, telnet to the SUA's IP address will connect to the Prestige directly.

11.3 Telnet Capabilities

11.3.1 Single Administrator

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

11.3.2 System Timeout

There is a system timeout of 5 minutes (300 seconds) for either the console port or telnet. Your Prestige 1100 will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in Menu 24.1.

Chapter 12: System Maintenance

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

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

```
Menu 24 - System Maintenance

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

Enter Menu Selection Number:
```

Figure 12-1 Menu 24 - System Maintenance

12.1 System Status

The first selection, System Status gives you the status and statistics of the ports, as shown below. System Status is a tool that can be used to monitor your Prestige. Specifically, it gives you information on WAN port 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**.

The following figure shows 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

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

WAN IP Addr:

Ethernet 1:                               Ethernet 2:
Status: 100M/Half Duplex                   Status: 100M/Half Duplex
TX Pkts: 52                                 TX Pkts: 52
RX Pkts: 537                               RX Pkts: 537
Collisions: 0                              Collisions: 0

Press Command:
COMMANDS: 1- Drop Port 9- Reset Counters   ESC-Exit
```

Figure 12-2 Menu 24.1 - System Maintenance – Status

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

Table 12-1 System Maintenance - Status Menu Fields

Field	Description
Status	The status of the WAN port.
TXPkts	The number of transmitted packets on this channel.
RXPkts	The number of received packets on this channel.
Errors	The number of error packets on this channel.
Tx (Byte / s)	The transmission speed in bytes per second.
Rx (Byte / s)	The reception speed in bytes per second.
Up Time	Time this channel has been connected to the current remote node.
WAN IP Addr	Shows the IP address of the WAN port.
Ethernet 1 & 2	
Status	Shows the current transmission speed and mode of the LAN.
TX Pkts	The number of transmitted packets to LAN.
RX Pkts	The number of received packets from LAN.
Collisions	Number of collisions.
COMMANDS	
1	Press "1" to drop a port.
9	Press "9" to reset all counters.
ESC	Press [ESC] to exit this menu.

12.2 System Information

- Step 1.** Select option 24 from the Main Menu to open **Menu 24 - System Maintenance**.
- Step 2.** From Menu 24, select option 2 then select the first option from Menu 24.2 to display **Menu 24.2.1 - System Maintenance – Information**.

```

Menu 24.2.1 - System Maintenance - Information

Name: P1100
Routing: IP/IPX
ZyNOS S/W Version: V2.50a05

LAN 1:
Ethernet Address: 00:a0:c5:30:00:b0
IP Address: 202.132.154.170
IP Mask: 255.255.255.0
DHCP: None
LAN 2:
Ethernet Address: 00:a0:c5:30:00:b1
IP Address: 202.132.50.25
IP Mask: 255.255.255.248
DHCP: Server

Press ESC or RETURN to Exit:
    
```

Figure 12-3 System Maintenance – Information

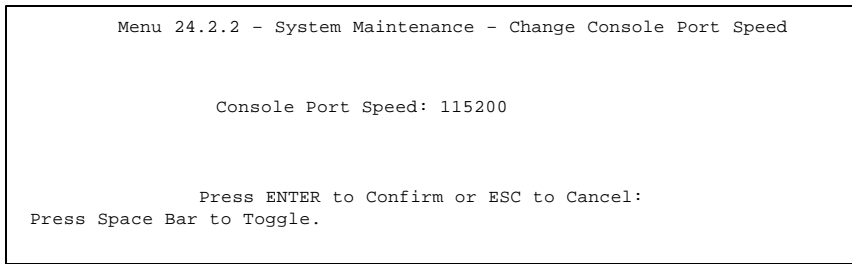
Table 12-2 Fields in System Maintenance

Field	Description
Name	Displays the system name of your Prestige. This information can be modified in Menu 1 - General Setup .
Routing	Refers to the routing protocol enabled.
ZyNOS S/W Version	Refers to the ZyXEL Network operating System software version.
LAN 1 & 2	
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.

12.2.1 Console Port Speed

- Step 1.** Select option 24 from the Main Menu to open **Menu 24 - System Maintenance**.
- Step 2.** From Menu 24, select option 2 then select the second option from Menu 24.2 to display **Menu 24.2.2 – System Maintenance – Change Console Port Speed**.

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

A screenshot of a terminal window showing the configuration menu for the console port speed. The text is as follows:

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

Console Port Speed: 115200

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

Figure 12-4 Menu 24.2.2 – System Maintenance – Change Console Port Speed

12.3 Log and Trace

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

12.3.1 Viewing Error Log

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

- Step 1.** Select option 24 from the Main Menu to open Menu 24 - System Maintenance.
- Step 2.** From Menu 24, select option 3 to open Menu 24.3 - System Maintenance - Log and Trace.
- Step 3.** Select the first option from Menu 24.3 - System Maintenance - Log and Trace to display the error log in the system.

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

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

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

Figure 12-5 Examples of Error and Information Messages

12.3.2 Syslog And Accounting

The Prestige uses the UNIX syslog facility to log system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 - System Maintenance - Syslog and Accounting**, as shown next.

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

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

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

Figure 12-6 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 12-3 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.

12.4 Diagnostic

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

```

Menu 24.4 - System Maintenance - Diagnostic

1. Ping Host
2. Reboot System
3. Command Mode

Enter Menu Selection Number:

Post IP Address= N/A

```

Figure 12-7 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 12-4 System Maintenance Menu Diagnostic

Field	Description
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.

12.5 Filename conventions

The configuration file (sometimes called the romfile or romfile-0) contains the settings in the menus such as password, DHCP Setup defaults, TCP/IP Setup defaults etc. The external (i.e., not on the Prestige) configuration filename is usually the router model name with a *.rom extension, e.g., P1100.rom. The ZyNOS firmware file (sometimes referred to as the “ras” file) is the file that contains the ZyXEL Network Operating System firmware and the external firmware file is usually called the router model name with a *.bin extension, e.g., P1100.bin. Rename the configuration filename to “rom-0” or “rom-spt” (see the next section) and the firmware filename to “ras” when transferring files to the Prestige. These are the internal (i.e., on the Prestige) filenames. Renaming the files is not necessary when you transfer files to the Prestige using the X-Modem protocol.

The following table is a summary. Please note that the internal filename refers to the filename on the Prestige and the external filename refers to the filename not on the Prestige, i.e., on your workstation, local network or ftp site and so the name (but not the extension) will vary. The AT command is the command you enter after you press “Y” when prompted in the SMT menu to go into debug mode.

Table 12-5 Filename Conventions

File type	Internal Name	Description	AT Command	External Name
Configuration File	Rom-spt	This is the router configuration filename on the Prestige when you are backing up and restoring files (menus 24.5 and 24. 6). The rom-spt file contains your Prestige configurations such as IP addresses, DHCP settings, Remote Node settings etc. as well as your personal password.		*.rom
	Rom-0	This is the router configuration filename on the Prestige when you are uploading the configuration file in menu 24.7.2. Uploading the rom-0 file replaces the entire ROM file system, including your Prestige configurations, system-related data (including the baud rate and default password), the error log and the trace log.	ATUR3	*.rom
Firmware	Ras ¹	This is the generic name for the firmware (in the main block) on the Prestige.	ATUR ¹	*.bin
	Ras-m ¹	This is the name for the firmware in the main block on the Prestige.	ATUM ¹	*.bin
	Ras-b	This is the name for the firmware in the backup block on the Prestige.	ATUB	*.bin

12.6 Back up Configuration

12.6.1 Backup using the Console Port

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

You can perform the backup either through an FTP or TFTP client program (preferred method) or through the RS-232 console port (in the event of the network being down). Backup via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the XMODEM protocol to perform the download/upload.

¹ Ras and ATUR exist for backward compatibility. Ras is equivalent to ras-m; atur is equivalent to ATUM.

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

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

Figure 12-8 Menu 24.5 –Backup Configuration using the Console Port

12.6.2 Back up using FTP

To transfer the configuration file, follow the procedure below:

- Step 1.** Launch the FTP client on your workstation.
- Step 2.** Type `open` and the IP address of your Prestige. Then type `root` and your SMT password as requested.
- Step 3.** Locate the “rom-spt” file.
- Step 4.** Type `get rom-spt` to backup the current Prestige configuration to your workstation.

For details on FTP commands, please consult the documentation of your FTP client program.

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

Press ENTER to Exit:
```

Figure 12-9 Backup Configuration using FTP

12.6.3 Back up using TFTP

Even though TFTP should work over WAN as well, it is not recommended.

To use TFTP, your workstation must have both telnet and TFTP clients.

To transfer the configuration file, follow the procedure below: Use telnet from your workstation to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.

- Step 1.** Launch the TFTP client on your workstation and connect to the Prestige.
- Step 2.** Go to SMT menu 24.5. Note that you must remain in this menu until backup is complete.
- Step 3.** Use the TFTP client to transfer files between the Prestige and the workstation. The file name for the configuration file is “rom-spt”.

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

12.7 Restore Configuration

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

12.7.1 Restore using the Console Port

You can restore the configuration either through an FTP or TFTP client program (preferred method) or through the RS-232 console port (in the event of the network being down). Restoring via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the XMODEM protocol to perform the download/upload. Please note that the system reboots automatically after the file transfer process is complete.

```

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

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

Figure 12-10 Menu 24.6 –Restore Configuration using the Console Port

12.7.2 Restore using FTP

To transfer your current workstation configuration to your Prestige, follow the procedure below:

- Step 1.** Launch the FTP client on your workstation.
- Step 2.** Type open and the IP address of your Prestige. Then type root and password as requested.
- Step 3.** Type put *backupfilename* rom-spt where “*backupfilename*” is the name of your backup configuration file on your workstation and “rom-spt” is the remote file name on the

Prestige. This restores the configuration to your Prestige.

Step 4. The system reboots automatically after the file transfer process is complete.

For details on FTP commands, please consult the documentation of your FTP client program.

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

Press ENTER to Exit:
```

Figure 12-11 Restore Configuration using FTP

12.7.3 Restore using TFTP

Even though TFTP should work over WAN as well, it is not recommended.

To use TFTP, your workstation must have both telnet and TFTP clients. To transfer the configuration file, follow the procedure below. Use telnet from your workstation to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.

Step 1. Launch the TFTP client on your workstation and connect to the Prestige.

Step 2. Go to SMT menu 24.6. Note that you must remain in this menu until file transfer is complete.

Step 3. Use the TFTP client to transfer files between the Prestige and the workstation. The remote file name on the Prestige is "rom-spt".

Step 4. The system reboots automatically after the file transfer process is complete.

Note that the telnet connection must be active before and during the TFTP transfer. For details on TFTP commands, please consult the documentation of your TFTP client program. For UNIX, use "put" to transfer from the workstation to the Prestige, and "binary" to set binary transfer mode.

12.8 Upload Firmware

Option 7 from **Menu 24 – System Maintenance** takes you to **Menu 24.7 – System Maintenance – Firmware Update** which allows you to upgrade the firmware or default configuration. You can upgrade the firmware either through an FTP or TFTP client program (preferred method) or through the RS-232 console port (in the event of the network being down). Updating the firmware via the console port under

normal conditions is not recommended since FTP or TFTP is faster. Please note that the system reboots automatically after the file transfer process is complete.

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

1. Upload ZyNOS Code
2. Upload Router Configuration File

Enter Menu Selection Number:
```

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

12.8.1 Dual Firmware Block Structure

The Prestige P1100 employs a “dual firmware block structure” where one block is called the “main block” and the other block is called the “backup block”. The benefits of this approach are:

- You can upload the current firmware into the backup block (ras-b) before you try to upload new firmware. If the new firmware has problems, you may either revert to using your old working firmware by using the “ATSW” command under Boot Extension or selectively run the old firmware in the backup block by using the “ATGB” command under Boot Extension.
- If the firmware in the main block gets corrupted for some reason, the Prestige will try to boot from the backup block automatically so service won’t get interrupted.

12.8.2 Upload Router Firmware via the Console Port

FTP or TFTP are the preferred methods for uploading router firmware to your Prestige. However in the event of your network being down, uploading router firmware is only possible with a direct connection to your Prestige via the console port. Uploading router firmware via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the XMODEM protocol to perform the download/upload.

Select 1 from Menu 24.7 – System Maintenance – Firmware Update to go to Menu 24.7.1 - System Maintenance - Upload ZyNOS Code.

- Step 1.** Enter "y" at the prompt to go into debug mode.
- Step 2.** Enter "atur" after the "Enter Debug Mode" message
- Step 3.** Wait for the "Starting XMODEM upload" message before activating the Xmodem upload on your terminal.
- Step 4.** The system reboots automatically after a successful firmware upload.

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

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

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

Figure 12-13 Menu 24.7.1 –Upload ZyNOS Code using the Console Port.

12.8.3 Upload Router Firmware using FTP

To transfer the firmware, follow the procedure below:

- Step 1.** Launch the FTP client on your workstation.
- Step 2.** Type `open` and the IP address of your Prestige. Then type `root` and your SMT password as requested.
- Step 3.** Type `put firmwarefilename ras-m` where “*firmwarefilename*” is the name of your firmware upgrade file on your workstation and “`ras-m`” is the remote file name on the Prestige. Specify “`ras-m`” as the remote filename if you want to upload firmware from your workstation into the main block or “`ras-b`” if you want to upload firmware into the backup block.
- Step 4.** The system reboots automatically after a successful firmware upload.

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

Press ENTER to Exit:
```

Figure 12-14 Menu 24.7.1. – Upload Router Firmware using FTP

12.8.4 Upload Router Firmware using TFTP

Even though TFTP should work over WAN as well, it is not recommended.

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

- Step 1.** Launch the TFTP client on your workstation and connect to the Prestige.
- Step 2.** Go to SMT menu 24.7.1. Note that you must remain in this menu until file transfer is complete.
- Step 3.** Use the TFTP client to transfer files between the Prestige and the workstation.
- Step 4.** Specify “ras-m” as the remote filename if you want to upload firmware from your workstation into the main block or “ras-b” if you want to upload firmware into the backup block of the Prestige.
- Step 5.** The system reboots automatically after a successful firmware upload.

Note that the telnet connection must be active before and during the TFTP transfer. For details on TFTP commands, please consult the documentation of your TFTP client program. For UNIX, use “put” to transfer from the workstation to the Prestige, and “binary” to set binary transfer mode.

12.9 Upload Router Configuration File

The configuration data, system-related data, the error log and the trace log are all stored in the configuration file. Please be aware that uploading the configuration file replaces all previous configurations. You can upgrade the configuration file either through an FTP or TFTP client program (preferred method) or through the RS-232 console port (in the event of the network being down). Updating the configuration file via the console port under normal conditions is not recommended since FTP or TFTP is faster. Please note that you need to reboot the system after the configuration file update process is complete. Note that if you replace the current configuration with the default configuration file, i.e.. P1100.rom, you will lose all configurations that you had before and the speed of the console port will be reset to the default of 9600 bps with 8 data bit, no parity and 1 stop bit(8n1). You will need to change your serial communication software to the default before you can connect to the Prestige again. The password will be reset to the default of 1234, as well.

12.9.1 Upload Router Configuration File using the Console Port

Select 2 from Menu 24.7 – System Maintenance – Firmware Update to go to Menu 24.7.2 –Upload Router Configuration File.

- Step 1.** Enter "y" at the prompt to go into debug mode.
- Step 2.** Enter "atur3" after the "Enter Debug Mode" message.
- Step 3.** Wait for the "Starting XMODEM upload" message before activating the Xmodem upload on your terminal.

Step 4. After successful file transfer, enter "atgo" to restart the router.

```
Menu 24.7.2 - System Maintenance - Upload Router Configuration File
FTP or TFTP are the preferred methods for uploading the router configuration
file to your Prestige since FTP or TFTP is faster.
To upload the router configuration file:
1. Enter "y" at the prompt to go into debug mode.
2. Enter "atur3" after the "Enter Debug Mode" message
3. Wait for the "Starting XMODEM upload" message before activating the
Xmodem upload on your terminal.
4. After successful file transfer, enter "atgo" to restart the router.

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

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

Figure 12-15 Menu 24.7.2 –Upload Router Configuration File.

12.9.2 Upload Router Configuration File using FTP

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

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

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

Press ENTER to Exit:
```

Figure 12-16 Menu 24.7.2 – Upload Router Configuration File using FTP

12.9.3 Upload Router Configuration File using TFTP

Even though TFTP should work over WAN as well, it is not recommended.

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

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

- Step 1.** Launch the TFTP client on your workstation and connect to the Prestige. Set the transfer mode to binary before starting data transfer.
- Step 2.** Go to SMT menu 24.7.2. Note that you must remain in this menu until file transfer is complete.
- Step 3.** Use the TFTP client to transfer files between the Prestige and the workstation.
- Step 4.** Specify “rom-0” as the remote file name on the Prestige.
- Step 5.** The system reboots automatically after the upload router configuration file process is complete.

Note that the telnet connection must be active before and during the TFTP transfer. For details on TFTP commands, please consult the documentation of your TFTP client program. For UNIX, use “put” to transfer from the workstation to the Prestige, and “binary” to set binary transfer mode.

12.9.4 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, etc.

```
=====  
Debug Command Listing  
=====  
athe  
=====  
Debug Command Listing  
=====  
AT          just answer OK  
ATHE        print help  
ATBAx       change baudrate. 1:38.4k, 2:19.2k, 3:9.6k  
4:57.6k 5:115.2k  
ATENx(,y)   set BootExtension Debug Flag (y=password)  
ATSE        show the seed of password generator  
ATTI(h,m,s) change system time to hour:min:sec or show  
current time  
ATDA(y,m,d) change system date to year/month/day or show  
current date  
ATDS        dump RAS stack  
ATDT        dump Boot Module Common Area  
ATDUX,y     dump memory contents from address x for length  
y  
ATRBx       display the 8-bit value of address x  
ATRBx       display the 8-bit value of address x  
ATRWx       display the 16-bit value of address x  
ATRLx       display the 32-bit value of address x  
ATGox       run program at addr x or boot ZyNOS  
ATGR        boot ZyNOS  
ATGT        run Hardware Test Program  
ATRTw,x,y(,z) RAM Test level w, from address x to y (z  
iterations)  
ATCB        copy from FLASH ROM to working buffer  
ATSH        dump manufacturer related data in ROM  
ATDOx,y     download from address x for length y to PC via  
XMODEM  
ATTD        download configuration to PC via XMODEM  
  
< press any key to continue >  
ATUR        upload RAS code to flash ROM  
ATUR3       upload RAS configuration file  
ATLOa,b,c,d Int/Trap Log Cmd  
ATGM        boot ZyNOS in main block  
ATGB        boot ZyNOS in backup block  
ATUM        upload RAS code to main block  
ATUB        upload RAS code to backup block  
ATSW        switch main block and backup block  
  
or
```

Figure 12-17 Boot module commands

12.10 Command Interpreter Mode

This option allows you to enter the command interpreter mode. A list of valid commands can be found by typing [help] at the command prompt. For more detailed information, check the ZyXEL Web site or send e-mail to the ZyXEL Support Group. Please note that the first release of the P1100 does not support L2TP.

```
Enter Menu Selection Number: 8

Copyright (c) 1999 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys          exit          device        ether
wan          l2tp          radius        ip
ppp          bridge        ipx           hdap
ras>
```

Figure 12-18 Command mode

Chapter 13: IP Policy Routing

13.1 Introduction

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

13.1.1 Benefits

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Quality of Service (QoS) – Organizations can differentiate traffic by setting the precedence or TOS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.

13.1.2 Routing Policy

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

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

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

13.1.3 IP Policy Routing Setup

Menu 25 shows all the policies defined

```
Menu 25 - IP Routing Policy Setup

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

Enter Policy Set Number to Configure= 0

Edit Name= N/A

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

Figure 13-1 IP Routing Policy Setup

To setup a routing policy, follow the procedures below:

- Step 1.** Enter 25 in the Main Menu to open **Menu 25 – IP Policy Routing Setup**.
- Step 2.** Enter the index of the policy set you wish to configure to open **Menu 25.1 - IP Policy Routing Summary**.

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

```
Menu 25.1 - IP Routing Policy Summary

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

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

Figure 13-2 Menu 25 - IP Routing Policy Summary

Table 13-1 IP Routing Policy Summary

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

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

```

Menu 25.1.1 - IP Routing Policy

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

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

Figure 13-3 IP Routing Policy

Table 13-2 IP Routing Policy

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

13.2 Applying an IP Policy

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

13.2.1 Ethernet IP Policies

From Menu 3 - Ethernet Setup, enter 2 to go to Menu 3.2 -General Ethernet Setup.

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

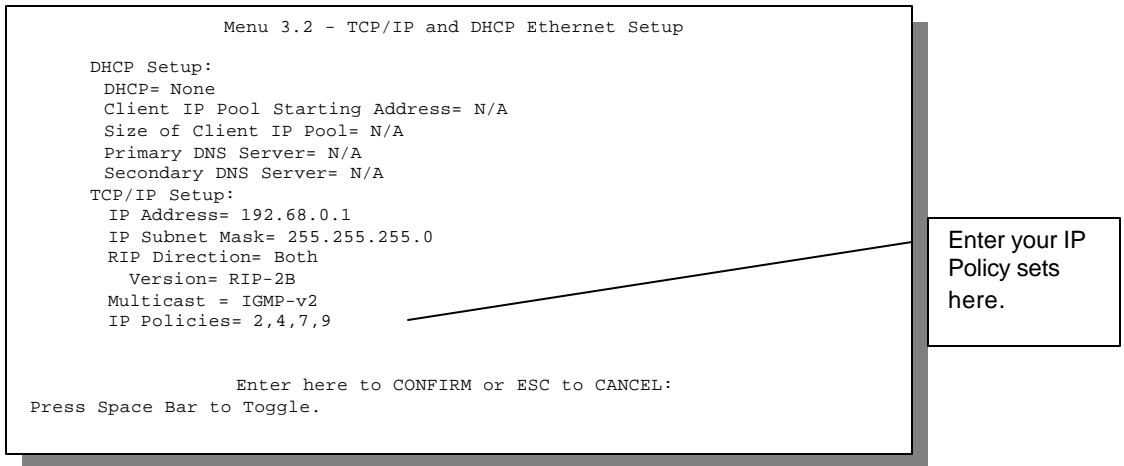


Figure 13-4 Menu 3.1.1 - General Ethernet Setup

13.2.2 Remote Node IP Routing Policies

Go to Menu 11.3 (shown next) and enter the number(s) of the IP Routing Policy set(s) as appropriate. You can cascade up to four policy sets by entering their numbers separated by commas.


```
Menu 11.3 - Remote Node Network Layer Options

IP Options:                               IPX Options:
Rem IP Addr= 0.0.0.0                       Rem LAN Net #= N/A
Rem Subnet Mask= 0.0.0.0                   My WAN Net #= N/A
My WAN Addr= 0.0.0.0                       Hop Count= N/A
Single User Account= No                    Tick Count= N/A
                                             W/D Spoofing(min)= N/A
                                             SAP/RIP Timeout(min)= N/A

Metric= 2
Private= No
RIP Direction= Both                        Bridge Options:
  Version= RIP-2B                           Ethernet Addr Timeout(min)= N/A
Multicast = IGMP-v2
IP Policies= 1,2,3,4

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

Enter your IP
Policy sets
here.

Figure 13-5 Menu 11.3 - Remote Node Network Layer Options

Chapter 14: Troubleshooting

This chapter covers the potential problems you may run into and the possible remedies. After each problem description, some instructions are provided to help you to diagnose and to solve the problem.

14.1 Problems Starting Up the Prestige 1100

Table 14-1 Troubleshooting the Start-Up of your Prestige 1100

Troubleshooting	Corrective Action	
None of the LEDs are on when you power on the Prestige 1100	<p>Check the connection between the power cord and your Prestige 1100.</p> <p>If the error persists you may have a hardware problem. In this case you should contact technical support.</p>	
Cannot access the Prestige 1100 via the console port.	1. Check to see if the Prestige 1100 is connected to your computer's serial port. Note that a null modem is required.	
	2. Check to see if the communications program is configured correctly. The communications software should be configured as follows:	VT100 terminal emulation
		9600 Baud.
No parity, 8 Data bits, 1 Stop bit.		

14.2 Problems With the WAN Port

Table 14-2 Troubleshooting a WAN Port Connection

Troubleshooting	Corrective Action
RDY LED of a WAN Port is not ON	Check if the WAN port is connected to an external WAN device.
	Check if the power of the external WAN device is turned on.

14.3 Problems with the LAN Interface

Table 14-3 Troubleshooting the LAN Interface

Troubleshooting	Corrective Action
Can't ping any station on the LAN	Check the Ethernet LED on the front panel of your Prestige 1100. If it is off, check the cables connecting your Prestige 1100 to the hub.
	Verify that the IP address and the subnet mask in Menu 3.2 are consistent between the Prestige 1100 and the workstations.

14.4 Problems Connecting to a Remote Node or ISP

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

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

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
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
STP	Shielded Twisted Pair (cable)
WAN	Wide Area Network

Index

A

Action Matched, 8-5
Applications, 4
 Internet Access, 4
 SUA, 5
 LAN-to-LAN, 6, 5-1
Authentication, 4-2, 4-3

B

Back Panel, 4
Boot Module Commands, 12-18
Bridging, 2, 6, 2-10, 4-2, 7-1
 Ether Address, 7-4
 Ethernet, 7-1
 Ethernet Addr Timeout, 7-3
 Remote Node, 7-2
 Static Route Setup, 7-4

C

CHAP, 4-2
Command Interpreter Mode, 12-19
Community, 9-1
Compression, 4-4
Connections, 2-2
 Ethernet, 2-3
 Power Cord, 2-3
 WAN Devices, 2-2
Copyright, ii
CSU/DSU, xiv, 1
Customer Support, iv

D

DHCP. *See* Dynamic Host Configuration Protocol
DNS. *See* Domain Name System
Domain Name System, 3-3
 DNS Proxy, 3-3
 Primary and Secondary DNS Server, 3-3
Dynamic Host Configuration Protocol, 3-3

E

Encapsulation, 4-4
Ethernet Setup, 2-12

F

Feature Overview
 Data Compression, 3
 Detailed Features, 1
 DHCP Support, 3
 Ethernet LANs, 2
 Full Network Management, 2
 Multiple Protocol Support, 2
 NAT Support, 2
 Quick, 1
 WAN Solutions, 1
Filename Conventions, 12-8
Filters
 About, 8-1
 Applying, 8-15
 Ethernet, 8-15
 Remote Node, 8-16
 Configuring a Filter Rule, 8-6
 Configuring a Filter Set, 8-3
 Device
 Abbreviations, 8-6
 Device Filter Rule, 8-13
 Ethernet, 2-13
 Executing a Filter Rule, 8-1
 IP
 Abbreviations, 8-5
 IPX Filter Rule, 8-11
 Logic Flow of an IP Filter, 8-10
 More, 8-5
 Rules Summary, 8-4
 Session Options, 4-3
 Structure, 8-1
 SUA, 8-6
 TCP/IP Filter Rule, 8-7
Fractional T1/E1, xiv, 1
Front Panel, 3
 LEDs, 3

G

Gateway, 5-8
General Setup, 2-9
 Menu Fields, 2-10

H

Hop Count, 6-7, 6-9

I

IANA. *See* Internet Assigned Number Authority
Initial Screen, 2-3
Interactive Applications, 13-1
Internet access, 3-1
Internet Access Configuration, 3-6
Internet Assigned Number Authority, 3-2
Internet Service Provider, 3-2
IP Address, 3-2, 3-5, 3-8, 4-3, 5-3, 5-8, 7-4
IP Multicast, 3-5
 Internet Group Management Protocol(IGMP), 3-5
IP Network Number, 3-2
IP Policies, 3-5, 5-5, 13-6
IP Policy Routing (IPPR), 13-1
 Applying an IP Policy, 13-6
 Benefits, 13-1
 Cost Savings, 13-1
 Criteria, 13-1
 Ethernet IP Policies, 13-6
 Gateway, 13-5
 Load Sharing, 13-1
 Remote Node IP Policies, 13-6
 Setup, 13-2
IP Pool, 3-3
IP Routing Policy, 13-5
IP Routing Policy Setup, 13-4
IPX, 2, 6, 4-3, 6-1
 Ethernet Setup, 6-4
 External Network Number, 6-2
 Frame Types, 6-1, 6-4
 802.2, 6-1
 802.3, 6-1
 Ethernet II, 6-1
 SNAP(Sub-Network Access Protocol), 6-1
 Internal Network Number, 6-2
 LAN-to-LAN, 6-5
 Prestige, 6-2

 Remote Node Setup, 6-6
 Seed Router, 6-3
 Static Route Setup, 6-8
IPX Network Number, 6-1, 6-7
IPX Node Number, 6-1
ISP. *See* Internet Service Provider

L

LAN, 5, 3-2, 12-3
 Receiving, 12-3
 Transmitting, 12-3
LANs & WANs, 3-11
 Prestige, 3-11
Login, 3-7, 4-2

M

MAC. *See* Media Access Control
Main Menu, 2-6
 Summary, 2-6
Media Access Control, 6-1, 7-1
Metric, 5-4, 5-8
My WAN Addr, 5-3, 5-4

N

Navigating the SMT Interface, 2-5
NetWare, 6-1
Network Address Translation, 1, 2, 8-6, A
Network Address Translator (NAT), 3-9
Network Interface Card, 2-1
NIC. *See* Network Interface Card

P

Packing List Card, xv
PAP, 4-2
Password, 2-3, 2-7, 3-7, 4-2, 9-1, 10-1
Point-to-Point Protocol, 2
Power On, 2-3
PPP, 4-3
 Editing PPP Options, 4-3
Precedence, 13-1, 13-5
Private, 5-4, 5-8

Q

Quality of Service, 13-1

R

Remote Configuration, 2

Remote Node, 4-1, 12-3

Leased Line, 4-1

TCP/IP, 5-1

Remote Node Setup, 5-2

RIP. *See* Routing Information Protocol

RJ-45, 2-3

Route IP Setup, 3-1

Routing Information Protocol, 3-2

Direction, 3-2

Version, 3-2

Routing Policy, 13-1

S

SAP/RIP Timeout, 6-7

Single User Account, 2

Single User Account, 5, 3-2, 3-7, 3-8, 3-9, 3-10, 5-4,
8-6, B

Advantages, 3-9

Configuration, 3-9

Ethernet, 3-10

SMT. *See* System Management Terminal

SNMP (Simple Network Management Protocol), 9-1

Community, 9-2

Configuration, 9-1

Traps, 9-2

Trusted Host, 9-2

Socket, 6-9

Stac, 3

Static Route Setup, 5-6

Menu Fields, 5-8

STP (Shielded Twisted Pair), 2-3

SUA. *See* Single User Account

Subnet Mask, 3-2, 3-5, 5-4, 5-8

Supporting Disk, xiv

Syntax Conventions, xiv

System Maintenance

Backup

Console Port, 12-9

FTP, 12-10

TFTP, 12-10

Console Port Speed, 12-5

Diagnostic, 12-7

Ping, 12-8

Reboot, 12-8

Log & Trace, 12-5

Viewing, 12-5

Menu 24, 12-1

Restore, 12-11

Console Port, 12-11

FTP, 12-11

TFTP, 12-12

Syslog & Accounting, 12-6

System Status, 12-2

System Management Terminal, 2-5

System Security, 2-6, 2-7, 2-8, 10-1, 10-2

Password, 10-1, 10-2

T

TCP/IP, 3-3, 12-8

Telnet, 11-1

Single Administrator, 11-2

Single User Account, 11-2

SUA, 11-2

Timeout, 11-2

Terminal Emulation, 2-1, 14-1

Tick Count, 6-7, 6-9

TOS (Type of Service), 13-1

Troubleshooting, 14-1

LAN Interface, 14-2

Remote Node, 14-2

Start up, 14-1

WAN Port, 14-2

Type of Service, 13-1, 13-4, 13-5

U

UNIX syslog, 12-6

Upload Firmware, 12-12

Console Port, 12-13

Dual Firmware Block Structure, 12-13

FTP, 12-14

TFTP, 12-15

Upload Router Configuration File, 12-15

Console Port, 12-15

FTP, 12-16

TFTP, 12-17

V

VT100, 2-1

WAN Setup, 2-11
Watchdog, 6-7

W

WAN port, 2-2

Z

ZyNOS, 12-4, 12-13, 12-14, 13-1
ZyXEL Limited Warranty, iii