

# *Prestige 480*

*Dual BRI ISDN Router*

## *User's Guide*

Version 2.42

Dec. 1999



# **Prestige 480**

## **ISDN Router**

### **Copyright**

Copyright © 02.08.1999 by ZyXEL Communications Corporation.

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

Published by ZyXEL Communications Corporation. All rights reserved.

### **Disclaimer**

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

### **Trademarks**

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



# Declaration of Conformity

We, the Manufacturer/Importer

ZyXEL Communications Services GmbH.

Thaliastrasse 125a/2/2/4

A-1160 Vienna - AUSTRIA

declare that the product

## Prestige 480

is in conformity with

(Reference to the specification under which conformity is declared)

<b>Standard</b>	<b>Standard Item</b>	<b>Version</b>
• EN 55022	Radio disturbance characteristics – Limits and method of measurement.	1994
• EN 61000-3-2	Disturbance in supply system caused by household appliances and similar electrical equipment “Harmonics”.	1995
• EN 61000-3-3	Disturbance in supply system caused by household appliances and similar electrical equipment “Voltage fluctuations”.	1995
• EN 61000-4-2	Electrostatic discharge immunity test – Basic EMC Publication	1995
• EN 61000-4-3	Radiated, radio-frequency, electromagnetic field immunity test	1996
• EN 61000-4-4	Electrical fast transient / burst immunity test - Basic EMC Publication	1995
• EN 61000-4-5	Surge immunity test	1995
• EN 61000-4-6	Immunity to conducted disturbances, induced by radio-frequency fields	1996

- EN 61000-4-8 Power Magnetic Measurement 1993
- EN61000-4-11 Voltage dips, short interruptions and voltage variations immunity tests 1994

## **ZyXEL Limited Warranty**

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

### **Note**

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

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

## Customer Support

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

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





# Table of Contents

<b>Declaration of Conformity .....</b>	<b>iv</b>
<b>Table of Contents .....</b>	<b>ix</b>
<b>List of Figures.....</b>	<b>xix</b>
<b>List of Tables.....</b>	<b>xxv</b>
<b>Preface .....</b>	<b>xxvii</b>
<b>Prestige Scenarios .....</b>	<b>xxix</b>
<b>Chapter 1.....</b>	<b>1-1</b>
<b>Getting to Know Your Router .....</b>	<b>1-1</b>
1.1 Prestige 480 ISDN Router.....	1-1
1.2 Features of Prestige 480.....	1-1
1.3 Applications for Prestige 480.....	1-5
1.3.1 Internet Access.....	1-6
1.3.2 LAN-to-LAN Connection.....	1-9
1.3.3 Remote Access Server.....	1-10
<b>Chapter 2.....</b>	<b>2-1</b>
<b>Hardware Installation &amp; Initial Setup .....</b>	<b>2-1</b>
2.1 Front Panel LEDs .....	2-1
2.2 Prestige 480 Rear Panel and Connections .....	2-2
2.3 Prestige Network Commander .....	2-3
2.4 Additional Installation Requirements .....	2-4
2.5 Housing .....	2-4
2.6 Power On Your Prestige.....	2-4
2.7 Navigating the SMT Interface.....	2-5
2.7.1 System Management Terminal Interface Summary .....	2-7

2.8	Changing the System Password.....	2-8
2.9	Resetting the Prestige .....	2-9
2.10	General Setup .....	2-12
2.11	European ISDN Setup Menus .....	2-13
2.11.1	Advanced Setup.....	2-14
2.12	NetCAPI Setup .....	2-17
2.12.1	Basics .....	2-17
2.12.2	CAPI.....	2-17
2.12.3	ISDN-DCP .....	2-17
2.12.4	RVS-COM .....	2-18
2.13	Configuring the P480 as a NetCAPI Server .....	2-18
2.13.1	Installing the CAPI driver and Communication Software .....	2-19
2.13.2	Configuring NetCAPI .....	2-19
2.14	Ethernet Setup .....	2-22
2.14.1	General Ethernet Setup.....	2-22
<b>Chapter 3</b>	.....	<b>3-1</b>
<b>Internet Access</b>	.....	<b>3-1</b>
3.1	Factory Ethernet Defaults .....	3-1
3.2	Route IP Setup.....	3-1
3.3	TCP/IP Parameters .....	3-2
3.3.1	IP Address and Subnet Mask.....	3-2
3.3.2	RIP Setup.....	3-3
3.3.3	DHCP Configuration.....	3-3
3.4	TCP/IP Ethernet Setup and DHCP .....	3-5
3.5	IP Alias .....	3-7

---

3.5.1	Basics .....	3-7
3.5.2	IP Alias Setup .....	3-8
3.6	Internet Access Configuration.....	3-11
3.7	Single User Account .....	3-14
3.7.1	Advantages of SUA .....	3-15
3.7.2	Single User Account Configuration.....	3-16
3.8	Mega Bundle or Multiple ISPs Support.....	3-17
3.8.1	Basics .....	3-17
3.8.2	ISP Remote Node and Supplementary Remote Node.....	3-18
3.9	Configuring Mega Bundle .....	3-18
3.10	Configuring Backup ISP Accounts.....	3-20
3.10.1	Configure a Backup ISP .....	3-20
3.10.2	To Switch ISP.....	3-20
<b>Chapter 4</b>	.....	<b>4-1</b>
<b>Remote Node Configuration</b>	.....	<b>4-1</b>
4.1	Remote Node Setup .....	4-1
4.1.1	Remote Node Profile .....	4-1
4.1.2	Nailed-up Connection.....	4-5
4.1.3	Outgoing Authentication Protocol.....	4-5
4.1.4	PPP Multilink.....	4-6
4.1.5	Bandwidth on Demand.....	4-6
4.1.6	Editing PPP Options.....	4-8
4.1.7	Remote Node Filter.....	4-10
<b>Chapter 5</b>	.....	<b>5-1</b>

<b>Remote Node TCP/IP Configuration .....</b>	<b>5-1</b>
5.1 LAN-to-LAN Application .....	5-1
5.2 Remote Node Setup .....	5-3
5.2.1 Static Route Setup.....	5-6
<b>Chapter 6.....</b>	<b>6-1</b>
<b>IPX Configuration .....</b>	<b>6-1</b>
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 in an IPX Environment .....	6-3
6.2.1 Prestige on LAN with Server.....	6-3
6.2.2 Prestige on LAN without Server.....	6-4
6.3 IPX Spoofing .....	6-4
6.4 IPX Ethernet Setup.....	6-4
6.5 LAN-to-LAN Application with Novell IPX.....	6-7
6.6 IPX Remote Node Setup.....	6-8
6.6.1 IPX Static Route Setup .....	6-10
<b>Chapter 7.....</b>	<b>7-1</b>
<b>Bridging Setup .....</b>	<b>7-1</b>
7.1 Bridging in General.....	7-1
7.2 Bridge Ethernet Setup .....	7-1
7.2.1 Remote Node Bridging Setup.....	7-2
7.3 Bridge Static Route Setup.....	7-3

---

<b>Chapter 8</b> .....	<b>8-1</b>
<b>Dial-in Server Configuration</b> .....	<b>8-1</b>
8.1 Remote Access Server .....	8-2
8.2 LAN-to-LAN Server Application .....	8-3
8.3 Default Dial-in Setup.....	8-4
8.3.1 Default Dial-in Filter .....	8-7
8.4 Dial-In Users Setup .....	8-7
8.4.1 Remote Access under Windows.....	8-10
8.4.2 CLID Authentication.....	8-12
8.4.3 Callback .....	8-12
8.4.4 Configuring the Prestige for Callback with CLID.....	8-14
8.5 Multiple Servers behind SUA .....	8-17
8.5.1 Configuring a Server behind SUA .....	8-18
<b>Chapter 9</b> .....	<b>9-1</b>
<b>Filter Configuration</b> .....	<b>9-1</b>
9.1 About Filtering.....	9-1
9.2 Configuring a Filter Set .....	9-3
9.2.1 Filter Rules Summary Menus.....	9-4
9.3 Configuring a Filter Rule .....	9-6
9.3.1 Filter Types and SUA .....	9-7
9.3.2 TCP/IP Filter Rule .....	9-8
9.3.3 Generic Filter Rule .....	9-12
9.3.4 IPX Filter Rule .....	9-14
9.4 Applying Filters and Factory Defaults.....	9-16
9.4.1 Ethernet traffic .....	9-16

---

9.4.2	Remote Node Filters .....	9-16
9.4.3	Default Dial-in Filter .....	9-17
<b>Chapter 10</b>	.....	<b>10-1</b>
<b>SNMP Configuration</b>	.....	<b>10-1</b>
10.1	About SNMP .....	10-1
10.2	Configuring SNMP .....	10-1
<b>Chapter 11</b>	.....	<b>11-1</b>
<b>System Security</b>	.....	<b>11-1</b>
11.1	Changing the System Password .....	11-1
11.2	Using RADIUS Authentication .....	11-3
11.2.1	Installing a RADIUS Server .....	11-3
11.2.2	RADIUS Server Configuration .....	11-5
11.2.3	The Key Field .....	11-6
11.2.4	Adding Users to the RADIUS Database.....	11-6
11.2.5	Using RADIUS Authentication for CLID .....	11-7
11.3	RADIUS Accounting .....	11-7
<b>Chapter 12</b>	.....	<b>12-1</b>
<b>Telnet Configuration and Capabilities</b>	.....	<b>12-1</b>
12.1	About Telnet Configuration .....	12-1
12.2	Telnet Under SUA .....	12-2
12.3	Telnet Capabilities .....	12-2
12.3.1	Single Administrator .....	12-2
12.3.2	System Timeout .....	12-2
<b>Chapter 13</b>	.....	<b>13-1</b>
<b>System Maintenance</b>	.....	<b>13-1</b>

---

13.1	System Status .....	13-2
13.1.1	System Information.....	13-6
13.1.2	Console Port Speed .....	13-7
13.2	Log and Trace .....	13-7
13.2.1	Viewing Error Log.....	13-7
13.2.2	Syslog And Accounting.....	13-9
13.3	Diagnostic.....	13-13
13.4	Boot Module Command .....	13-16
13.5	Command Interpreter Mode .....	13-17
13.6	Call Control .....	13-17
13.6.1	Call Control Parameters .....	13-18
13.6.2	Blacklist.....	13-19
13.6.3	Budget Management.....	13-20
13.6.4	Call History .....	13-21
13.7	Time and Date Setting .....	13-22
<b>Chapter 14</b>	.....	<b>14-1</b>
<b>Backup, Restore and Upload</b>	.....	<b>14-1</b>
14.1	Backup Configuration .....	14-1
14.1.1	Backup using the Console Port .....	14-1
14.1.2	Back up using FTP.....	14-2
14.1.3	Back up using TFTP .....	14-3
14.2	Restore Configuration.....	14-4
14.2.1	Restore using the Console Port .....	14-4
14.2.2	Restore using FTP.....	14-6

14.2.3	Restore using TFTP .....	14-6
14.3	Firmware Update .....	14-7
14.3.1	Upload through the Console Port .....	14-8
14.3.2	Upload using FTP .....	14-10
14.3.3	Upload using TFTP .....	14-13
<b>Chapter 15</b>	.....	<b>15-1</b>
<b>IP Policy Routing</b>	.....	<b>15-1</b>
15.1	Introduction .....	15-1
15.1.1	Benefits .....	15-1
15.1.2	Routing Policy .....	15-1
15.1.3	IP Routing Policy Setup.....	15-2
15.2	Applying an IP Policy .....	15-7
15.2.1	Ethernet IP Policies .....	15-7
<b>Chapter 16</b>	.....	<b>16-1</b>
<b>Troubleshooting</b>	.....	<b>16-1</b>
16.1	Problems Starting Up the Prestige .....	16-1
16.2	Problems With the ISDN Lines .....	16-3
16.3	Problems with the Ethernet Connection .....	16-4
16.4	Problems Connecting to a Remote Node or ISP .....	16-4
16.5	Problems for Remote User to Dial-in .....	16-5
<b>Information Worksheet</b>	.....	<b>A</b>
<b>Enhanced Syslog</b>	.....	<b>E</b>
<b>Acronyms and Abbreviations</b>	.....	<b>G</b>
<b>Index</b>	.....	<b>I</b>







# List of Figures

Figure 1-1 Internet Access Application .....	1-6
Figure 1-2 Internet Access Application .....	1-8
Figure 1-3 LAN-to-LAN Application.....	1-9
Figure 1-4 Remote Access Server Application.....	1-10
Figure 2-1 Front Panel .....	2-1
Figure 2-2 Prestige 480 Rear Panel and Connections.....	2-2
Figure 2-3 Power-On Display .....	2-5
Figure 2-4 Login Screen.....	2-5
Figure 2-5 SMT Main Menu.....	2-7
Figure 2-6 Menu 23 - System Security .....	2-8
Figure 2-7 Menu 23.1 - System Security - Change Password .....	2-9
Figure 2-8 Booting Up the Prestige.....	2-10
Figure 2-9 Menu 1 – General Setup.....	2-12
Figure 2-10 Menu 2 – ISDN Setup.....	2-13
Figure 2-11 Menu 2.1 – ISDN Basic Setup .....	2-13
Figure 2-12 Menu 2.1.1 - ISDN Advanced Setup.....	2-15
Figure 2-13 Loopback Test.....	2-17
Figure 2-14 Configuration Example .....	2-19
Figure 2-15 Menu 2.2 - NetCAPi Setup.....	2-20
Figure 2-16 Menu 3 - Ethernet Setup.....	2-22
Figure 2-17 General Ethernet Setup.....	2-23
Figure 3-1 General Setup .....	3-2
Figure 3-2 Menu 3.2 – TCP/IP and DHCP Ethernet Setup .....	3-5
Figure 3-3 Physical Network .....	3-7

Figure 3-4 Partitioned Logical Networks.....	3-8
Figure 3-5 IP Alias Example .....	3-8
Figure 3-6 Menu 3.2 - TCP/IP and DHCP Ethernet Setup.....	3-9
Figure 3-7 Menu 3.2.1 - IP Alias Setup.....	3-9
Figure 3-8 Menu 4 – Internet Access Setup.....	3-12
Figure 3-9 Single User Account Topology .....	3-14
Figure 3-10 Menu 4 – Internet Access Setup for Single User Account .....	3-16
Figure 4-1 Menu 11 – Remote Node Setup .....	4-2
Figure 4-2 Menu 11.1 Remote Node Profile .....	4-3
Figure 4-3 Menu 11.2 - Remote Node PPP Options.....	4-8
Figure 4-4 Menu 11.5 – Remote Node Filter .....	4-10
Figure 5-1 TCP/IP LAN-to-LAN Application .....	5-1
Figure 5-2 LAN 1 Setup.....	5-2
Figure 5-3 LAN 2 Setup.....	5-3
Figure 5-4 Menu 11.3- Remote Node TCP/IP Options.....	5-3
Figure 5-5 Sample IP Addresses for a TCPI/IP LAN-to-LAN Connection .....	5-4
Figure 5-6 Example of Static Routing Topology.....	5-6
Figure 5-7 Menu 12.1 – IP Static Route Setup.....	5-7
Figure 5-8 Edit IP Static Route Setup.....	5-7
Figure 8-1 Example of Remote Access Server Application.....	8-2
Figure 8-2 Example of a LAN-to-LAN Server Application .....	8-3
Figure 8-3 Menu 13 – Default Dial-in Setup.....	8-4
Figure 8-4 Default Dial-in Filter .....	8-7
Figure 8-5 Menu 14 - Dial-in User Setup .....	8-8
Figure 8-6 Edit Dial-in User.....	8-8
Figure 8-7 Remote Access Example .....	8-10
Figure 8-8 Configuring Menu 13 for Remote Access.....	8-11

Figure 8-9 Edit Dial-in-User for RAS.....	8-11
Figure 8-10 LAN 1 LAN-to-LAN Application .....	8-13
Figure 8-11 LAN2 LAN-to-LAN Application .....	8-13
Figure 8-12 Testing Callback with your Connection.....	8-14
Figure 8-13 Callback with CLID Configuration.....	8-15
Figure 8-14 Configuring CLID with Callback .....	8-16
Figure 8-15 Callback and CLID Connection Test.....	8-17
Figure 8-16 Multiple Server Configuration .....	8-18
Figure 9-1 Filter Rule Process.....	9-2
Figure 9-2 Menu 21 - Filter Set Configuration .....	9-3
Figure 9-3 Menu 21.1 - Filter Rules Summary .....	9-4
Figure 9-4 Menu 21.2 - Filter Rules Summary .....	9-4
Figure 9-5 Protocol and Device Filter Sets .....	9-7
Figure 9-6 Menu 21.1.1 - TCP/IP Filter Rule .....	9-8
Figure 9-7 Executing a Filter Rule .....	9-11
Figure 9-8 Menu 21.3.1 - Generic Filter Rule .....	9-12
Figure 9-9 Menu 21.1.3 - IPX Filter Rule .....	9-14
Figure 9-10 Filtering Ethernet traffic .....	9-16
Figure 9-11 Filtering Remote Node traffic.....	9-17
Figure 9-12 Default Dial-in Filter.....	9-17
Figure 10-1 Menu 22 - SNMP Configuration.....	10-2
Figure 11-1 Menu 23 - System Security.....	11-1
Figure 11-2 Menu 23.1 - System Security - Change Password .....	11-2
Figure 11-3 Menu 23.2 - System Security - External Server.....	11-5
Figure 11-4 Menu 24.3.3 – System Maintenance – Accounting Server.....	11-7
Figure 11-5 Examples of RADIUS Accounting Message.....	11-8
Figure 12-1 Telnet Configuration on a TCP/IP Network.....	12-2

Figure 13-1 Menu 24 - System Maintenance .....	13-1
Figure 13-2 Menu 24.1 - System Maintenance – Status.....	13-2
Figure 13-3 Menu 24.1 after Toggle Status .....	13-3
Figure 13-4 LAN Packet That Triggered Last Call.....	13-5
Figure 13-5 System Maintenance - Information.....	13-6
Figure 13-6 Menu 24.2.2 – System Maintenance – Change Console Port Speed.....	13-7
Figure 13-7 Examples of Error and Information Messages .....	13-9
Figure 13-8 Menu 24.3.2 - System Maintenance – UNIX Syslog and Accounting.....	13-10
Figure 13-9 Menu 24.4 - System Maintenance - Diagnostic.....	13-13
Figure 13-10 Trace Display for a Successful Manual Call.....	13-15
Figure 13-11 Trace Display for a Failed Authentication .....	13-15
Figure 13-12 Boot Module Commands.....	13-16
Figure 13-13 Command Mode.....	13-17
Figure 13-14 Menu 24.9 - System Maintenance - Call Control.....	13-18
Figure 13-15 Call Control Parameters .....	13-18
Figure 13-16 Menu 24.9.2 - Blacklist.....	13-19
Figure 13-17 Menu 24.9.3 - Budget Management .....	13-20
Figure 13-18 Call History .....	13-21
Figure 13-19 System Maintenance – Time and Date Setting .....	13-22
Figure 14-1 Menu 24.5 –Backup Configuration using the Console Port .....	14-1
Figure 14-2 Receive File .....	14-2
Figure 14-3 Successful Backup .....	14-2
Figure 14-4 TFTP Example .....	14-4
Figure 14-5 Menu 24.6 –Restore Configuration using the Console Port .....	14-5
Figure 14-6 Send File .....	14-5
Figure 14-7 Successful Restoration .....	14-6
Figure 14-8 Menu 24.7 - System Maintenance - Upload Firmware .....	14-7

Figure 14-9 Menu 24.7.1 - Uploading Router Firmware .....	14-9
Figure 14-10 Menu 24.7.2 - System Maintenance - Upload Router Configuration File .....	14-10
Figure 14-11 FTP Example .....	14-11
Figure 14-12 Edit Host.....	14-12
Figure 14-13 Username Prompt.....	14-12
Figure 14-14 Files Transfer.....	14-13
Figure 15-1 Menu 25.1.1 - IP Routing Policy .....	15-5
15-2 Menu 3.2 – TCP/IP Ethernet Setup.....	15-7





# List of Tables

Table 2-1 LED Functions.....	2-1
Table 2-2 Main Menu Commands.....	2-5
Table 2-3 Main Menu Summary .....	2-7
Table 2-4 General Setup Menu Fields.....	2-12
Table 2-5 Menu 2.1 – ISDN Basic Setup .....	2-14
Table 2-6 Menu 2.1.1 - ISDN Advanced Setup.....	2-16
Table 2-7 NetCAPI Setup Fields.....	2-20
Table 3-1 DHCP Ethernet Setup Menu Fields.....	3-6
Table 3-2 TCP/IP Ethernet Setup Menu Fields .....	3-6
Table 3-3 Internet Account Information .....	3-11
Table 3-4 Internet Access Setup Menu Fields .....	3-13
Table 3-5 Single User Account Menu Fields .....	3-16
Table 4-1 Remote Node Profile Menu Fields.....	4-3
Table 4-2 BTR v MTR for BOD .....	4-7
Table 4-3 Remote Node PPP Options Menu Fields.....	4-9
Table 5-1 TCP/IP related fields in Remote Node Profile .....	5-4
Table 5-2 TCP/IP Remote Node Configuration.....	5-5
Table 5-3 Edit IP Static Route Menu Fields.....	5-8
Table 8-1 Remote Dial-in Users/Remote Nodes Comparison Chart .....	8-1
Table 8-2 Default Dial-in Setup Fields .....	8-4
Table 8-3 Edit Dial-in User Menu Fields .....	8-9
Table 8-4 Services vs. Port number .....	8-18
Table 9-1 Abbreviations Used in the Filter Rules Summary Menu .....	9-4
Table 9-2 Abbreviations used if Filter Type is IP .....	9-6

Table 9-3 Abbreviations used if Filter Type is GEN .....	9-6
Table 9-4 TCP/IP Filter Rule Menu Fields .....	9-8
Table 9-5 Generic Filter Rule Menu Fields .....	9-13
Table 9-6 IPX Filter Rule Menu Fields .....	9-15
Table 10-1 SNMP Configuration Menu Fields .....	10-3
Table 11-1 System Security - External Server Menu Fields .....	11-6
Table 11-2 System Maintenance – Accounting Server Fields .....	11-8
Table 11-3 Accounting Attributes .....	11-9
Table 13-1 System Maintenance - Status Menu Fields .....	13-3
Table 13-2 Fields in System Maintenance .....	13-6
Table 13-3 System Maintenance Menu - UNIX Syslog Parameters .....	13-11
Table 13-4 System Maintenance Menu Diagnostic .....	13-14
Table 13-5 Call Control Parameters Fields .....	13-19
Table 13-6 Call History Fields .....	13-21
Table 13-7 Time and Date Setting Fields .....	13-22
Table 15-1 IP Routing Policy Menu Fields .....	15-5
Table 16-1 Troubleshooting the Start-Up of your Prestige .....	16-1
Table 16-2 Troubleshooting the ISDN Lines .....	16-3
Table 16-3 Troubleshooting the Ethernet Connection .....	16-4
Table 16-4 Troubleshooting a Connection to a Remote Node or ISP .....	16-4
Table 16-5 Troubleshooting for Remote Users to Dial-in .....	16-5
Table 16-6 IP Subnet Masks and the Number of Hosts .....	C

# Preface

## About Your Router

Congratulations on your purchase of the Prestige 480 dual BRI ISDN Router.

The Prestige 480 is a high-performance router that offers a complete solution for your WAN (Wide Area Network) applications such as Internet access, multi-protocol LAN-to-LAN connections, telecommuting and remote access over ISDN (Integrated Service Digital Network). In addition, your Prestige also

*Note: If you do not have the ISDN lines installed already, order it as soon as possible in order to install and configure your P480. Contact your telephone company's ISDN Ordering Center to find about the type of ISDN service most suitable for your purpose.*

Your Prestige 480 is easy to install and to configure. You can use the PNC or the SMT interface to configure your Prestige.

The PNC (Prestige Network Commander) is a C++ based utility designed to allow users to manage the Prestige via Windows. For configuring your Prestige with PNC, use PNC ISDN Series Version 2.20. All functions of the Prestige 480 are also software configurable via the SMT (System Management Terminal) Interface. The SMT is a menu-driven interface that you can access from either a VT100 compatible terminal or a terminal emulation program on a computer.

Your Prestige also adheres to SNMP (Simple Network Management Protocol) standards. SNMP is a management protocol for collecting information from devices on the network.

*Note: ZyXEL is currently accepting online product registration. Visit [www.zyxel.com](http://www.zyxel.com) and register your P480. Registered owners will receive ZyXEL newsletter and future product and update information.*

## About This User's Manual

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

It is designed to guide you through the configuration of your Prestige 480 for its various applications.

## Other Resources

For more information about the Prestige check the following sources:

- ◆ Prestige Support disk.
- ◆ Release notes for firmware upgrades and other information. These can be accessed through ZyXEL FTP server site and ZyXEL web Page.

For ZyXEL support information see the *Customer Support* section in page v.

## **Syntax Conventions**

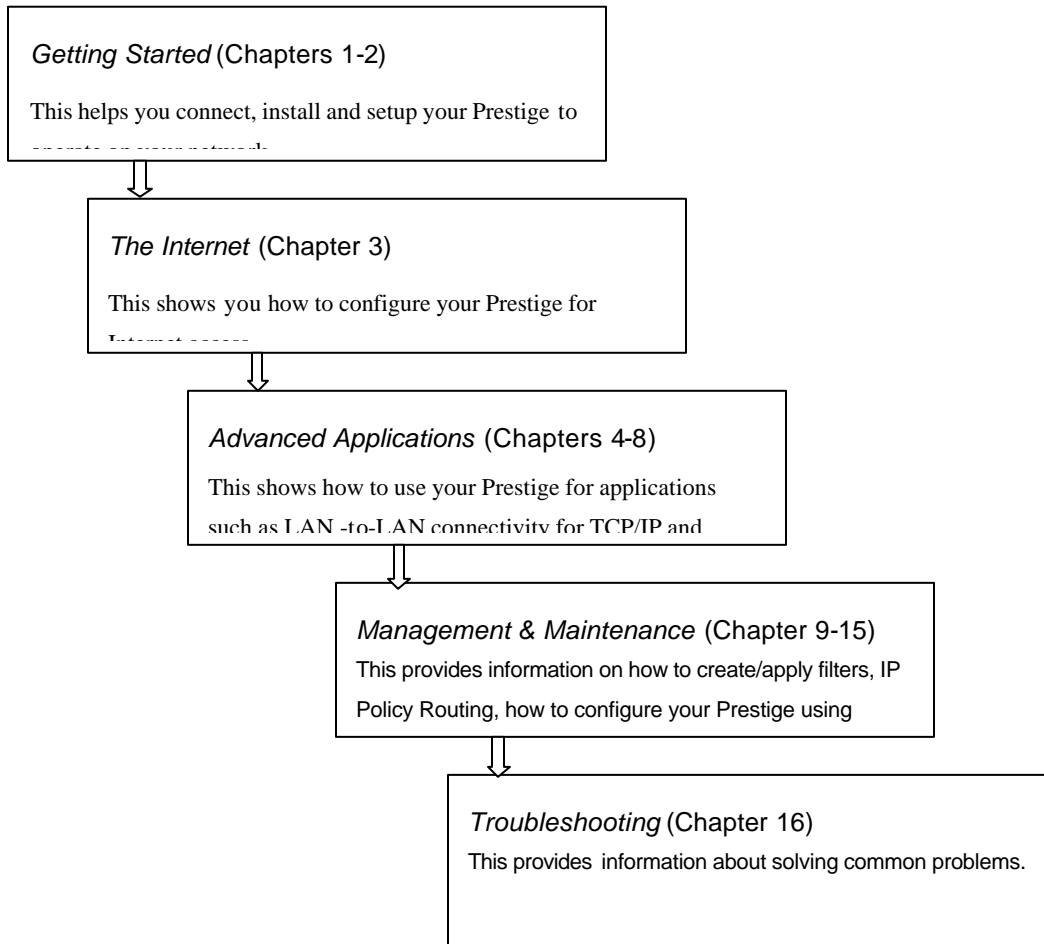
- “Enter” means for you to type one or more characters and press the carriage return. “Select” or “Choose” means for you to select one from the predefined choices.
- The SMT menu titles and labels are in **Bold Times** font. The choices of a menu item are in **Bold Arial** font. A single keystroke is in Arial font and enclosed in square brackets, for instance, [ENTER] means the Enter, or carriage return, key; [ESC] means the Escape key.
- For brevity’s sake, we will use “e.g.” as a shorthand for “for instance”, and “i.e.” as a shorthand for “that is” or “in other words” throughout this manual.
- The Prestige 480 will also be referred to as the Prestige or the P480 from now on, in this manual

# Prestige Scenarios

*For fast access to example SMT menus to show you how to configure the Prestige for various scenarios go to the following sections*

<b>SCENARIO</b>	<b>GO TO SECTION</b>
To reset your Prestige	2.9
NetCAPi	2.12
DHCP	3.4
Internet Access	3.5
To configure SUA	3.7.2
IP Alias	3.5
Mega Bundle or Multiple ISPs Support	3.8
LAN-to-LAN application	5.1
Remote Access under Windows	8.4.1
Callback	8.4.3
Callback with CLID	8.4.4
To apply filters	9.3.4

## General Structure of this Manual



# Chapter 1

## Getting to Know Your Router

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

### 1.1 Prestige 480 ISDN Router

The Prestige 480 is a dual-line multi-protocol ISDN router. The Prestige is ideal for everything from Internet browsing or receiving calls from remote dial-in users to making LAN-to-LAN connections to remote networks.

### 1.2 Features of Prestige 480

The following are the key features of the Prestige 480.

#### ***Dual ISDN Basic Rate Interface (BRI) Support***

The P480 supports two BRI, with each BRI offering two 64Kbps channels. The channels can be used independently for up to four destinations simultaneously in any incoming/outgoing combination or be bundled in a single connection to speed up data transfer.

#### ***Mega Bundle or Multiple ISPs Support***

The P480 can call a second, third or fourth ISP when the traffic exceeds a certain threshold and split the traffic between the various connections. The P480 refers to this multiple ISPs support as Mega Bundle.

#### ***IP Alias***

The P480 allows you to partition a physical network into logical networks. It support three logical networks on the same physical Ethernet segment and allows the users to access the Internet using Prestige's Single

User Account feature. The ability to partition physical network into logical network over the same Ethernet interface is referred to as IP Alias functionality.

### ***Dial-in Server***

The four B-channels and the dial-in capability make the Prestige an ideal platform as a dial-in server to provide remote access for up to four telecommuting employees.

### ***Auto-negotiating 10/100 Mbps Ethernet***

The LAN interface automatically detects if it's on a 10 or a 100 Mbps Ethernet and adjusts itself for the highest speed.

### ***Single User Account (SUA)***

The SUA™ (Single User Account) features allows multiple users on the LAN to share Internet access for the price of a single ISP account.

### ***DNS Proxy***

The DNS (Domain Name System) proxy capability eliminates the need of statically configuring the DNS servers.

### ***DHCP Support***

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

### ***Dial-On-Demand***

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

### ***Multiple Protocol Support***

- ◆ TCP/IP (Transmission Control Protocol/Internet Protocol) network layer protocol.
- ◆ IPX (Internetwork Packet eXchange) network layer protocol.
- ◆ Transparent bridging for unsupported network layer protocols.



### ***IP Policy Routing Support***

The Prestige can now override the default routing behavior and forward packets based on the policies defined by the network administrator.

### ***PPP Support***

The Prestige supports PPP (Point-to-Point Protocol) link layer protocol.

### ***PPP Multilink Support***

The Prestige can bundle up to four B-channels in a single connection using the PPP Multilink Protocol. The number of links can be either statically configured or dynamically managed based on traffic demand.

### ***Bandwidth-On-Demand***

The Prestige can dynamically allocate bandwidth by adding and dropping links according to traffic demand. The telephone number of an additional link can be obtained either with BAP (Bandwidth Allocation Protocol) or statically configured.

### ***Full Network Management***

- ◆ Windows based PNC (Prestige Network Commander).
- ◆ SNMP (Simple Network Management Protocol) support.
- ◆ SMT (System Management Terminal) access through telnet connection.

### ***PNC***

The Prestige Network Commander (PNC) is a C++ based utility designed to allow users to access the Prestige's management settings via Windows. For configuring your Prestige with PNC, use PNC ISDN Series Version 2.20.

### ***SNMP***

The Simple Network Management Protocol (SNMP) is a management protocol for collecting information from devices on the network. When TCP/IP is configured in your Prestige, the SNMP agent functionality allows a manager station to manage and monitor the Prestige through the network.

## **SMT**

The System Management Terminal (SMT) is a menu-driven interface to configure your Prestige using either console port (through RS232 cable) connection or telnet (through LAN) connection. You can access the SMT from either a VT100 compatible terminal or a terminal emulation program on a computer.

### ***Logging and Tracing***

- ◆ CDR (Call Detail Record) for assistance in analyzing and managing the telephone bill.
- ◆ Built-in message logging and packet tracing.
- ◆ UNIX syslog facility support.

### ***RADIUS Support***

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

### ***PAP and CHAP Security***

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

### ***CLID Support***

CLID (Calling Line Identification) allows the Prestige to authenticate the caller before a call is answered, thus saving the cost of a connection. The Prestige uses the caller ID in call setup message to match against the CLID in database. (Note: The telephone company must support Caller ID for CLID authentication to work on the Prestige.)

### ***Call Back***

The Callback feature allows the Prestige to disconnect a call and then call back when an authorized remote user dials into the system. This prevents intruders from accessing your network and makes accounting easier when you use the Prestige as a dial-in server.

### ***Packet Filtering***

The Prestige supports packet filtering that stops leakage of private data to the outside world and controls access to undesirable locations.

### ***Call Control***

Your Prestige provides budget management for outgoing calls and maintains a blacklist for unreachable phone numbers, thus saving you the expense of unnecessary charges.

### ***Data Compression***

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

### ***Networking Compatibility***

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

### ***Firmware Upgrade***

In addition to the direct console port connection, the Prestige supports the uploading of firmware and the configuration file using FTP (File Transfer Protocol) and TFTP (Trivial File Transfer Protocol). TFTP over the WAN is not recommended because of potential data corruption problems .

### ***Backup and Restore Configuration File***

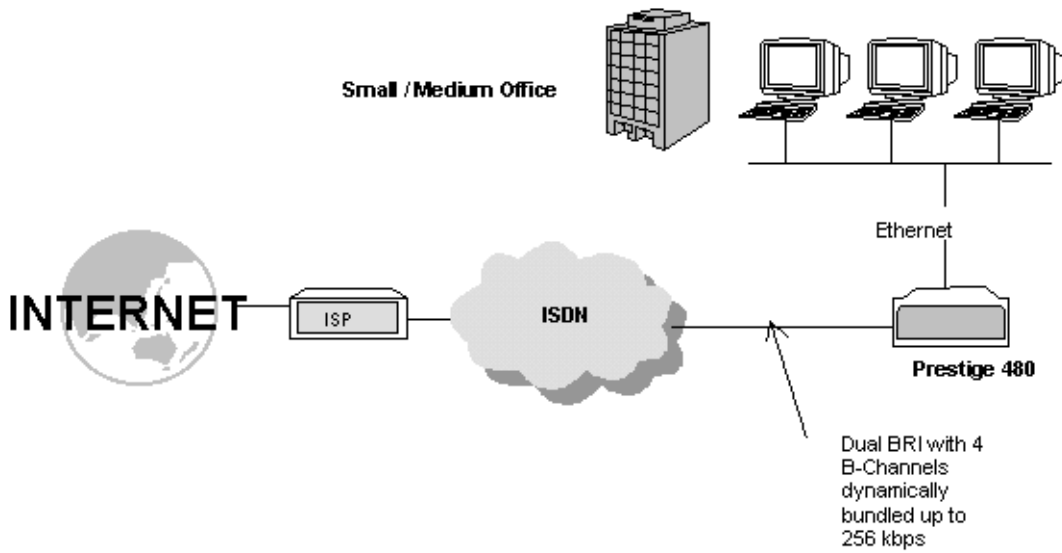
You can backup the configuration of the Prestige to your workstation and also restore the configuration from your workstation using direct console port connection, FTP and TFTP.

## **1.3 Applications for Prestige 480**

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

### 1.3.1 Internet Access

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



**Figure 1-1 Internet Access Application**

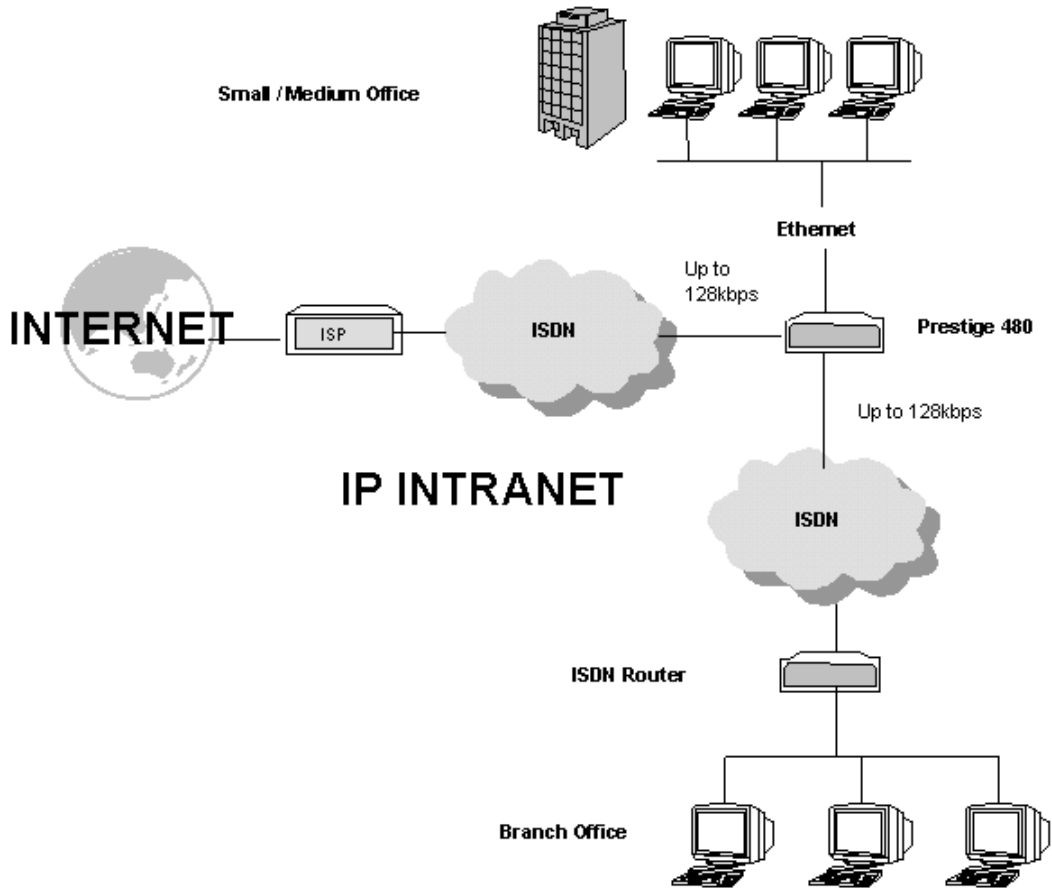
#### ***Internet Single User Account***

For a SOHO (Small Office/Home Office) environment, your Prestige offers a Single User Account (SUA) feature that allows multiple users on the LAN (Local Area Network) to access the Internet concurrently for

the cost of a single account. Single User Account address mapping can also be used for other LAN to LAN connections.

### ***Intranet Application***

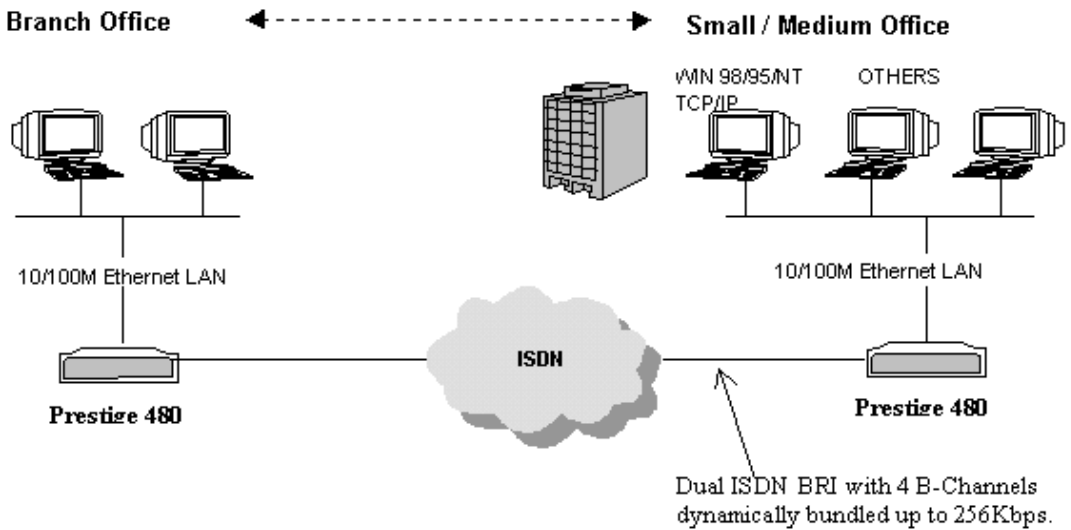
Small/Medium Office users can access the Internet via one ISDN BRI at speed up to 128Kbps even when the branch office users are connected remotely. The branch office users can access the Internet without extra ISP subscription fee. The application is shown next in Figure 1.2 Internet Access Application.



**Figure 1-2 Internet Access Application**

### 1.3.2 LAN-to-LAN Connection

You can use the Prestige to connect two geographically dispersed networks at speeds of up to 256Kbps over two ISDN BRI lines. It incorporates PPP/MP (Point-to-Point Protocol/Multilink Protocol) to bundle the B channels. The Prestige supports TCP/IP protocols. A typical LAN-to-LAN application for your Prestige is shown next.



**Figure 1-3 LAN-to-LAN Application**

### 1.3.3 Remote Access Server

Your Prestige allows remote users to dial in and gain access to your LAN. This feature enables users that have workstations with remote access capabilities, e.g., Windows 95, to dial in to access the network resources without physically being in the office. Either PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) authentication can be used to control the access from the remote users. You can also use callback for security and/or accounting purposes.

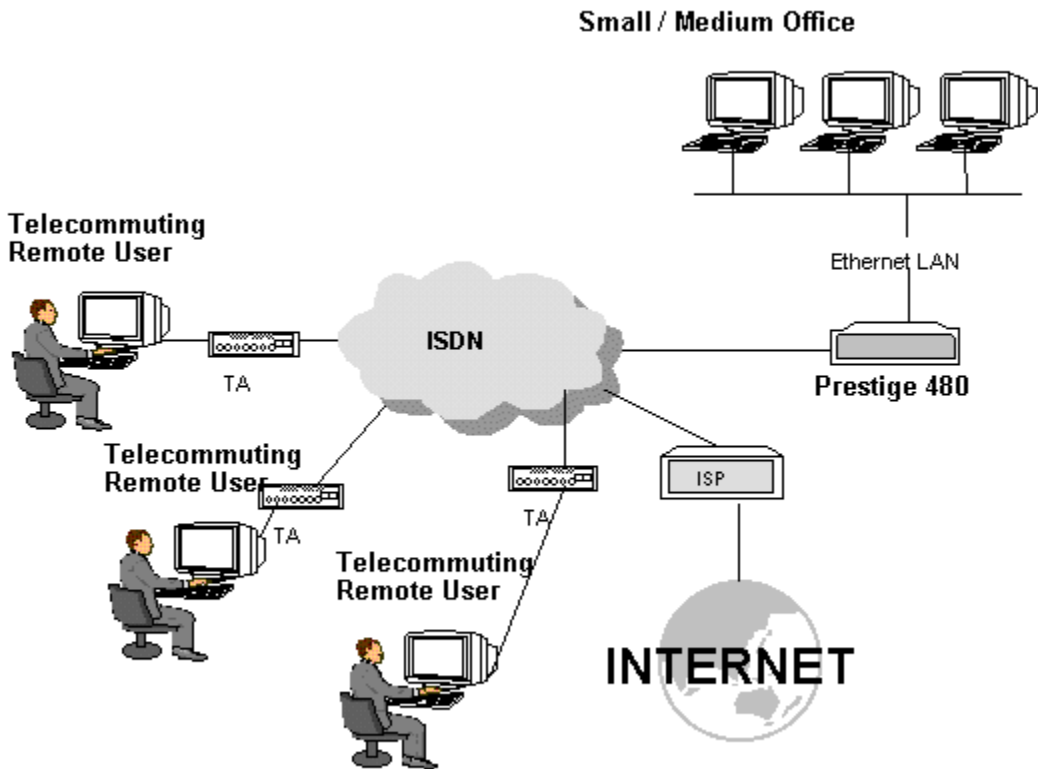


Figure 1-4 Remote Access Server Application



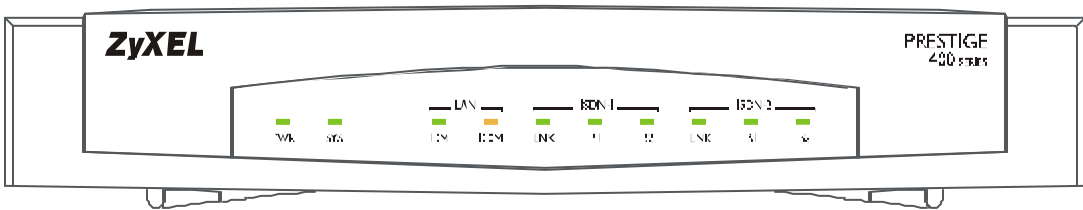
# Chapter 2

## Hardware Installation & Initial Setup

*This chapter shows you how to make the cable connections to your Prestige as well as set up your ISDN connection using the SMT.*

### 2.1 Front Panel LEDs

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

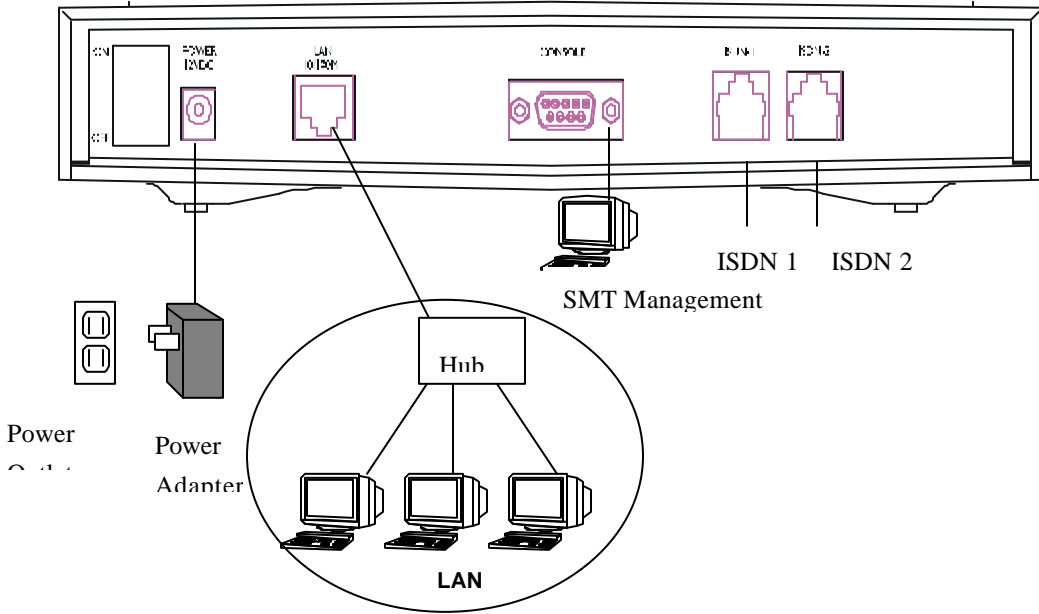


**Figure 2-1 Front Panel**

**Table 2-1 LED Functions**

Field	Description
PWR	The PWR (power) LED is on when power is applied to the Prestige.
SYS	The SYS (System) LED is on when the system is running normally, and off when the system is not ready or failed. It flashes when the system is rebooting.
LAN 10M	This green LED is on when the 10M Ethernet is connected and ready and off when the 10M Ethernet is not ready or failed. This LED flashes when the Prestige is sending or receiving packets.
100M	This orange LED is on when the 100M Ethernet is connected and ready and off when the 100M Ethernet is not ready or failed. This LED flashes when the Prestige is sending or receiving packets.

Field	Description
ISDN 1 & 2 LNK	The LNK (Link) LED is on when the Prestige is connected to an ISDN switch and the line has been successfully initialized; otherwise, it is off.
B1/B2	The B1/B2 LED is on when the corresponding B Channel is in use.



## 2.2 Prestige 480 Rear Panel and Connections

This section outlines how to connect your Prestige 480 to the LAN and to the ISDN network. The figure below shows the rear panel of your Prestige 480 and the connection diagram.

**Figure 2-2 Prestige 480 Rear Panel and Connections**

### **Step 1. Connecting the ISDN lines**

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

### **Step 2. Connecting Ethernet to your Prestige**

Use a Unshielded Twisted Pair (UTP) cable and RJ-45 connectors that look like a bigger telephone plug with eight pins to connect your Prestige to a 10/100M LAN.

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

### **Step 3. Connecting the Power Adapter to your Prestige**

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

### **Step 4. Connecting the Console Port**

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

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

## **2.3 Prestige Network Commander**

You can also setup the Prestige using the Prestige Network Commander (PNC). The PNC is a Windows-based tool that provides a quick and simple way to configure your Prestige. For more information on installing PNC insert the PNC installation disc in the relevant drive of your computer and follow the on-screen directions.

**Note:** You cannot access the PNC if you use the RS232 cable. You must use only the Ethernet cable.

## 2.4 Additional Installation Requirements

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

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

## 2.5 Housing

Your Prestige's housing has ventilation slots for cooling and clip-out legs that fit snugly into grooves for sturdy stacking with better airflow. ZyXEL recommends that you do not stack more than 4 routers for maximum stack stability and cooling.

## 2.6 Power On Your Prestige

At this point, you should have connected the console port, the ISDN BRI port, the Ethernet port and the power port to the appropriate devices or lines.

### Step 1. *Initial Screen*

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

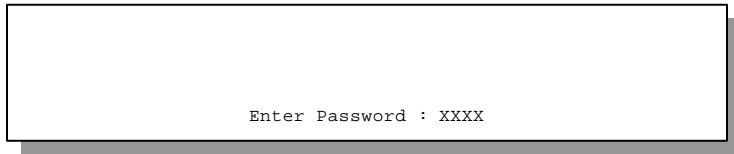
```
Copyright (c) 1994 - 1999 ZyXEL Communications Corp.  
initialize ch =0, ethernet address: 00:a0:c5:ff:00:35  
(2) DSS1:  
(2) DSS1:
```

### Figure 2-3 Power-On Display

#### Step 2. *Entering Password*

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

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



for each character you type.

### Figure 2-4 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 login screen again.

## 2.7 Navigating the SMT Interface

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

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

**Table 2-2 Main Menu Commands**

Operation	Press/<read>	Description
Move forward to another menu	[Enter]	To move forward to a sub-menu, type in the number of the desired sub-menu and press [Enter].
Move backward to a previous menu	[Esc]	Press the [Esc] key to move back to the previous menu.
Move to a submenu	Press the [Space bar] to change <b>NO</b>	Fields beginning with "Edit" have a default setting of <b>No</b> . Press the [Space bar] to change <b>No</b> to <b>Yes</b> , then press [ENTER] to go

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

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

```

Copyright (c) 1994 - 1999 ZyXEL Communications Corp.
Prestige 480 Main Menu

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

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

Advanced Management
21. Filter Set Configuration
22. SNMP Configuration
23. System Security
24. System Maintenance
25. IP Policy Routing

99. Exit

Enter Menu Selection Number:

```

Figure 2-5 SMT Main Menu

## 2.7.1 System Management Terminal Interface Summary

Table 2-3 Main Menu Summary

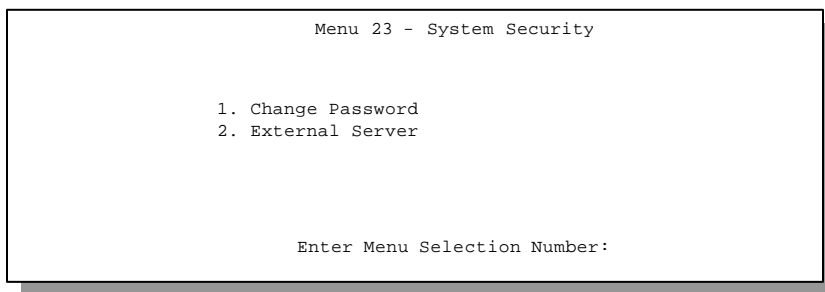
#	Menu Title	Description
1	General Setup	Use this menu to setup general information.
2	ISDN Setup	Use this menu to setup the ISDN.
3	Ethernet Setup	Use this menu to setup Ethernet.
4	Internet Access Setup	A quick and easy way to setup Internet connection.
11	Remote Node Setup	Use this menu to setup the Remote Node for LAN-to-LAN connection, including Internet connection.
12	Static Routing Setup	Use this menu to setup static route for different protocols.
13	Default Dial-in Setup	Use this menu to setup default dial-in parameters so that your Prestige can be used as a dial-in server.
14	Dial-in User Setup	Use this menu to setup dial-in users.
15	SUA Server Setup	Use this menu to specify inside servers when SUA is enabled.
21	Filter Set Configuration	Use this menu to setup filters to provide security, call control, etc.
22	SNMP Configuration	Use this menu to setup SNMP related parameters.
23	System Security	Use this menu to setup security related parameters.

24	System Maintenance	This menu provides system status, diagnostics, firmware upload, etc.
25	IP Policy Routing	This menu allows you to configure Routing Policies,
99	Exit	To exit from SMT and return to the blank screen.

## 2.8 Changing the System Password

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

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



**Figure 2-6 Menu 23 - System Security**

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



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

```
Menu 23.1 - System Security - Change Password

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

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

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

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

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

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

## 2.9 Resetting the Prestige

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

Download the "romfile.zip" file from the Internet, unzip it and save it in a folder. Turn off the Prestige and begin a Telnet session with the default console port settings.

Turn on the Prestige again. You should see the following screen.

```
Bootbase Version: V1.10 | 6/11/1999 15:04:51
RAM: Size = 8192 Kbytes
DRAM POST: Testing: 8192k OK
FLASH: intel 8M* 2

ZyNOS Version: V2.40(o.00)b02/ 7/13/1999 15:37:32

Press any key to enter debug mode within 3 seconds.
.....
Enter Debug Mode
```

### Figure 2-8 Booting Up the Prestige

When you see the message "Press Any key to enter Debug Mode within 3 seconds", press any key to enter debug mode. Follow the procedure below to upload the configuration file:

1. Enter "atur3" after the "Enter Debug Mode" message.
2. Wait for the "Starting XMODEM upload" message before activating Xmodem upload on your terminal.
3. After successful firmware upload, enter "atgo" to restart the Prestige.

The Prestige is now reinitialized with default configuration file including the default password of 1234.

**NOTE:**

The configuration filename is the router model name with a rom extension, e.g., p480.rom. The ZyNOS firmware filename is the router model name with a bin extension, e.g., p480.bin. Rename the latter filename to "ras" when uploading to the Prestige via FTP or TFTP.



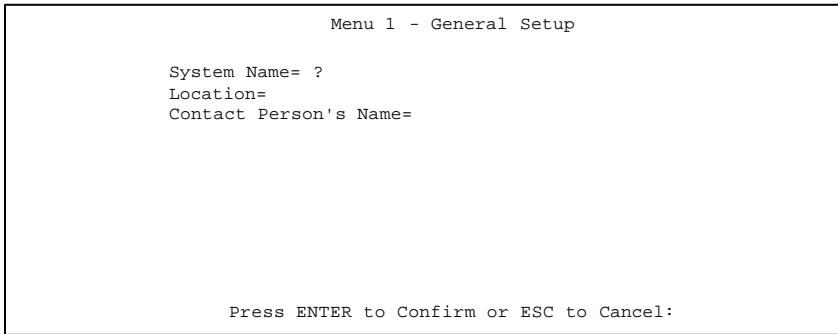
## 2.10 General Setup

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

To enter **Menu 1** and fill in the required information, follow these steps:

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

**Step 2.** The **Menu 1 - General Setup** screen appears, as shown next. Fill in the required fields marked [?] as explained in the following table.



```
Menu 1 - General Setup

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

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

Figure 2-9 Menu 1 – General Setup

**Table 2-4 General Setup Menu Fields**

Field	Description	Example
System Name	Choose a descriptive name for identification purposes. This name can be up to 8 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted. This name can be retrieved remotely via SNMP, used for CHAP authentication, and will be displayed at the prompt in the Command Mode.	P480
Location (optional)	Enter the geographic location (up to 31 characters) of your Prestige.	MyHouse
Contact Person's Name (optional)	Enter the name (up to 30 characters) of the person in charge of this Prestige.	JohnDoe

## 2.11 European ISDN Setup Menus

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

```
Menu 2 - ISDN Setup

1. ISDN Line 1 Setup
2. ISDN Line 2 Setup
3. NetCAPI Setup

Enter Menu Selection Number:
```

**Figure 2-10 Menu 2 – ISDN Setup**

From **Menu 2** select **1** or **2** to display **Menu 2.1 - ISDN Basic Setup**.

```
Menu 2.1 - ISDN Basic Setup

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

Incoming Phone Numbers:
ISDN Data      =

Edit Advanced Setup = No

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

**Figure 2-11 Menu 2.1 – ISDN Basic Setup**

**Table 2-5 Menu 2.1 – ISDN Basic Setup**

<b>Field</b>	<b>Description.</b>									
ISDN Line	Refers to ISDN line 1 or line 2 setup that you selected in <b>Menu 2 - ISDN Setup</b>									
Switch Type	This field is fixed as <b>DSS-1</b> for European switches.									
B Channel Usage	In general, this will be <b>Switch/Switch</b> (the default). If you are only using one B channel (e.g., your Prestige is sharing the ISDN BRI line with another device), then select <b>Switch/Unused</b> . If your second B channel is a leased line, select <b>Switch/Leased</b> . Press the [Space bar] to toggle through all the options. These options are  <table style="width: 100%; border: none;"> <tr> <td style="text-align: center;"><b>Switch/Switch</b></td> <td style="text-align: center;"><b>Leased/Unused</b></td> <td style="text-align: center;"><b>Switch/Unused</b></td> </tr> <tr> <td style="text-align: center;"><b>Switch/Leased</b></td> <td style="text-align: center;"><b>Unused/Leased</b></td> <td></td> </tr> <tr> <td style="text-align: center;"><b>Leased/Switch</b></td> <td style="text-align: center;"><b>Leased/Leased</b></td> <td></td> </tr> </table>	<b>Switch/Switch</b>	<b>Leased/Unused</b>	<b>Switch/Unused</b>	<b>Switch/Leased</b>	<b>Unused/Leased</b>		<b>Leased/Switch</b>	<b>Leased/Leased</b>	
<b>Switch/Switch</b>	<b>Leased/Unused</b>	<b>Switch/Unused</b>								
<b>Switch/Leased</b>	<b>Unused/Leased</b>									
<b>Leased/Switch</b>	<b>Leased/Leased</b>									
Incoming Phone Number Matching	Determines how incoming calls are routed.									
ISDN Data	Enter the telephone number assigned to ISDN data calls for the Prestige. The maximum number of digits is 25 for the telephone number.									
Edit Advanced Setup	Select <b>Yes</b> and press [Enter] to go to the advanced setup submenu. See below.									

### 2.11.1 Advanced Setup

Select **Yes** in the **Advanced Setup** field of **Menu 2.1 – ISDN Basic Setup** to display **Menu 2.1.1**.

```

Menu 2.1.1 - ISDN Advanced Setup

ISDN Line= 1
  Calling Line Indication= Enable

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

  Outgoing Calling Party Number:
    ISDN Data    =

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

**Figure 2-12 Menu 2.1.1 - ISDN Advanced Setup**

**Table 2-6 Menu 2.1.1 - ISDN Advanced Setup**

<b>Field</b>	<b>Description</b>
Calling Line Indication	The <b>Calling Line Indication</b> , or Caller ID, governs whether the other party can see your number when you call. If set to <b>Enable</b> , the Prestige sends the caller ID and the party you call can see your number; if it is set to <b>Disable</b> , the caller ID is blocked.
PABX Outside Line Prefix	A PABX (Private Automatic Branch eXchange) generally requires you to dial a number (a single digit in most cases) when you need an outside line. If your Prestige is connected to a PABX, enter this number in <b>PABX Outside Line Prefix</b> , otherwise, leave it blank. Please note that the PABX prefix is for calls initiated by the Prestige only.
PABX Number (Include S/T Bus Number)	The PABX number is used for an outside loopback test when the ISDN PABX cannot support a local loopback test. If the Prestige is connected to an ISDN PABX enter this number. Note that this number is used exclusively for loopback testing; for regular outgoing calls, the Prestige dials the phone number in the remote node. If this field is blank it indicates either that the PABX supports local loopback testing or that the Prestige is not connected to a PABX.
Outgoing Calling Party Number  ISDN Data	If this field is not blank, the Prestige will use its value as the <i>calling party number</i> for "ISDN Data" outgoing calls. Otherwise, the individual entry for "ISDN Data" in Menu 2.1 will be used as the calling party number. You only need to fill in this field if your switch or PABX requires a specific calling party number for outgoing calls; otherwise, leave it blank.

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

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



```
Setup LoopBack Test...
Dialing to 40000 ...
Sending and Receiving Data ...
Disconnecting...
```

**Figure 2-13 Loopback Test**

## **2.12 NetCAPI Setup**

### **2.12.1 Basics**

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

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

### **2.12.2 CAPI**

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

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

### **2.12.3 ISDN-DCP**

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

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

## **2.12.4 RVS-COM**

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

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

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

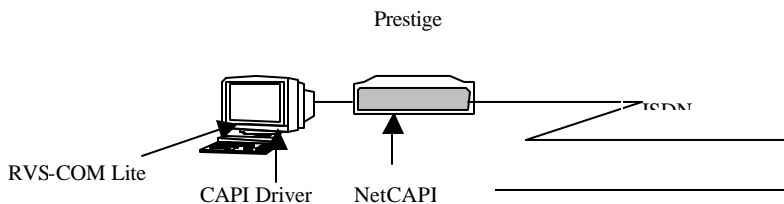
## **2.13 Configuring the P480 as a NetCAPI Server**

This section describes how to configure your Prestige to be a NetCAPI server using the SMT (System Management Terminal).

[**Note** : For configuring your Prestige with the PNC, use PNC ISDN Series version 2.20 or above.]

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

The following figure illustrates the configuration.



## Figure 2-14 Configuration Example

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

### 2.13.1 Installing the CAPI driver and Communication Software

[**Note:** Please uninstall previous versions of "RVS -CAPI" and "RVS-COM lite" before you install the new versions. You may use the Windows "START | Settings | Control Panel | Add/Remove Programs" to uninstall RVS-CAPI and RVS-COM.]

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

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

### 2.13.2 Configuring NetCAPI

**Step 1.** Go to **Menu 2.3 - NetCAPI Setup.**

```

Menu 2.3 - NetCAPI Setup

Active= Yes

Max Number of Registered Users= 1

Incoming Data Call Number Matching= MSN

Access List:

```

Start IP	End IP	Operation
192.168.1.132	192.168.1.145	Both
192.168.14.1	192.168.14.32	Imcoming

### Figure 2-15 Menu 2.2 - NetCAPI Setup

**Step 2.** Set the fields in the above menu according to the following description.

**Table 2-7 NetCAPI Setup Fields**

<b>Field</b>	<b>Description</b>
Active	This field allows you to enable or disable NetCAPI. Press the [Spacebar] to toggle between <b>Yes</b> and <b>No</b>
Max Number of Registered Users	When you want to use NetCAPI to place outgoing calls or to listen to incoming calls, you must start RVSCOM on your workstation, and RVSCOM will register itself to the Prestige. This option is the maximum number of clients that the Prestige supports at the same time. The default value is <b>4</b> .
Incoming Data Call Matching	<p>This field determines how incoming calls are routed. Press the [Spacebar] to select <b>NetCAPI</b> if you want to direct all incoming data calls to NetCAPI.</p> <p>Select <b>MSN</b> if you want to direct all incoming call to the Prestige only when the incoming phone number matches the ISDN DATA number in Menu 2. If the incoming phone number does not match the ISDN DATA number, then the call will be routed to NetCAPI.</p> <p>Select <b>Called Party Subaddress</b> if you want to direct all incoming calls to the Prestige only when the incoming call matches the subaddress of ISDN DATA in Menu 2. If the incoming call does not match the subaddress of ISDN DATA, then the call will be routed to NetCAPI.</p>
Access List	<p>This list specifies users that can use NetCAPI. This access list controls if a client is allowed to use NetCAPI. The request is rejected when</p> <ol style="list-style-type: none"><li>1. The IP address of the workstation is not between <b>Start IP</b> and <b>End IP</b> or</li><li>2. The request from the workstation is not permitted as specified in the <b>Operation</b> field.</li></ol>
Start IP	Refers to the first IP address of a group of NetCAPI clients. Each group contains contiguous IP addresses.
End IP	Refers to the last IP address in a NetCAPI client group.
Operation	<p>Press the [Spacebar] to select <b>Incoming</b> if you wish to grant incoming calls permission. Select <b>Outgoing</b> if you wish to grant outgoing calls permission. Select <b>Both</b> if you wish to grant both incoming calls and outgoing calls permissions. Select <b>None</b> if you wish to deny all calls.</p>



## 2.14 Ethernet Setup

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

```
Menu 3 - Ethernet Setup

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

Enter Menu Selection Number:
```

**Figure 2-16 Menu 3 - Ethernet Setup**

### 2.14.1 General Ethernet Setup

This menu allows you to specify the filter sets that you wish to apply to the Ethernet traffic. You seldom need to filter Ethernet traffic, however, the filter sets may be useful to block certain packets, reduce traffic

```
Menu 3.1 - General Ethernet Setup

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

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

and prevent security breaches.

### **Figure 2-17 General Ethernet Setup**

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





# 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 Factory Ethernet Defaults

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

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

These parameters should work for the majority of installations. If the parameters are satisfactory, you can skip to section 3.4 **TCP/IP Ethernet Setup and DHCP** to enter the DNS server address(es) if your ISP gives you explicit DNS server address(es). If you wish to change the factory defaults or to learn more about TCP/IP, please read on.

### 3.2 Route IP Setup

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

```
Menu 1 - General Setup

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

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

## Figure 3-1 General Setup

To edit **Menu 1**, enter 1 in the Main Menu to select **General Setup** and press [Enter].

### 3.3 TCP/IP Parameters

#### 3.3.1 IP Address and Subnet Mask

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

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

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

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

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

### 3.3.2 RIP Setup

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

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

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

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

### 3.3.3 DHCP Configuration

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (workstations) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The Prestige has built-in DHCP **Server** capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. Your Prestige can also be configured as a **Relay**. When configured as a relay, the Prestige relays the requests and responses between the clients and the real DHCP server.

#### ***IP Pool Setup***

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

## **DNS Server Address**

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

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

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

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

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

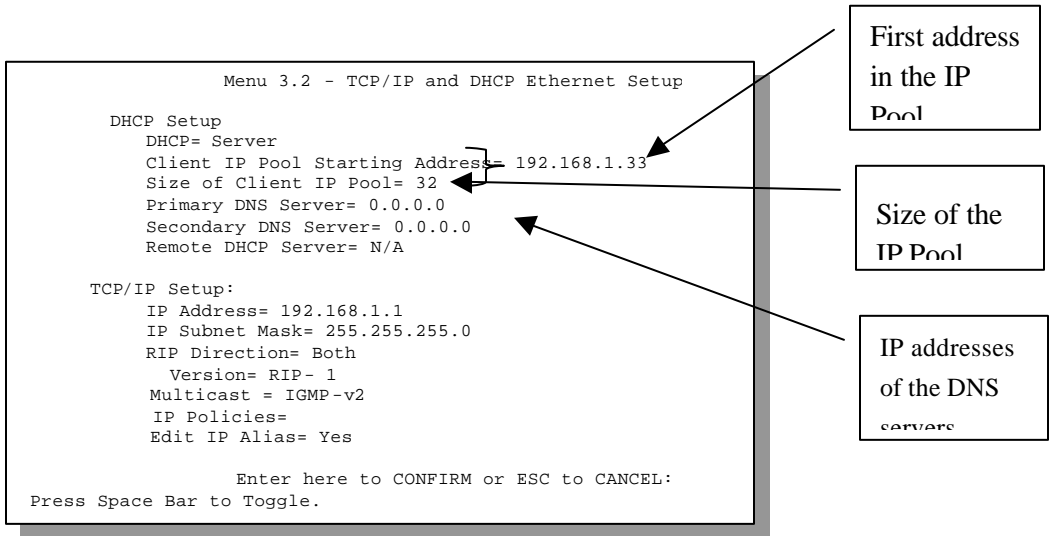
## **Relay Server Address**

When the DHCP is set to **Relay**, the Prestige will request IP addresses from a real DHCP server and relay the address to the workstation making the request.

## 3.4 TCP/IP Ethernet Setup and DHCP

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

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



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

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

**Table 3-1 DHCP Ethernet Setup Menu Fields**

Field	Description	Example
DHCP	This field enables/disables the DHCP server. If it is set to <b>Server</b> , your Prestige will act as a DHCP server. If set to <b>None</b> , the DHCP server will be disabled. If set to <b>Relay</b> , the Prestige acts as a surrogate DHCP server and relays requests and responses between the remote server and the clients. When DHCP is used, the following four items need to be set:	<b>None Server (default) Relay</b>
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size, or count, of the IP address pool.	32
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	
Remote DHCP Server	If <b>Relay</b> is selected in the above <b>DHCP=</b> field, then enter the IP address of the actual, remote DHCP server here.	

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

**Table 3-2 TCP/IP Ethernet Setup Menu Fields**

Field	Description	Example
IP Address	Enter the IP address of your Prestige in dotted decimal notation	192.168.1.1
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige	255.255.255.0
RIP Direction	Press the space bar to select the RIP direction from <b>Both/None/In Only/Out Only</b> .	<b>Both</b> (default)
Version	Press the space bar to select the RIP version from <b>RIP-1/RIP-2B/RIP-2M</b> .	<b>RIP-1</b> (default)
Multicast	Turn on/off IGMP support and select the version from <b>IGMP-v2/IGMP-v1/None</b> .	<b>IGMP-v2</b>
IP Policies	You can apply up to four IP Policy sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4,7,12.	
Edit IP Alias	Choose <b>Yes</b> to enter <b>Menu 3.2.1</b> for configuring second and	<b>Yes</b>

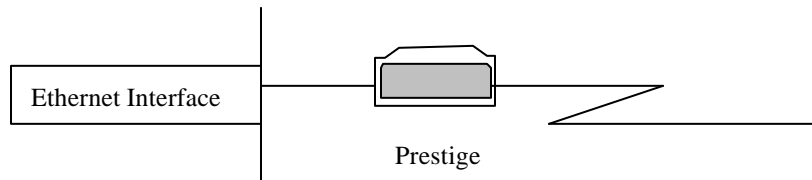
Field	Description	Example
	third IP Alias.	

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.

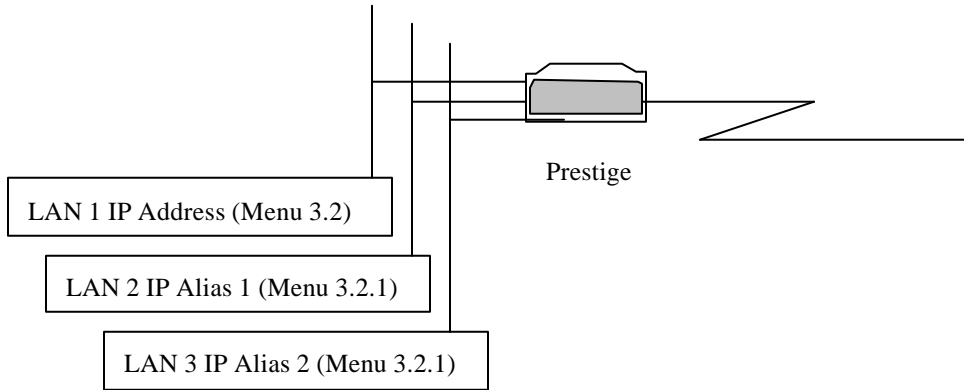
## 3.5 IP Alias

### 3.5.1 Basics

The P480 supports three logical LAN interface via its single physical Ethernet interface. The Prestige is the gateway for all the LAN networks. You can also route packets from one network to another. The IP alias feature allows your Prestige to have extra IP addresses that may be in completely different subnets than the first IP address. The ability to partition physical network into logical network over the same Ethernet interface is referred to as IP Alias functionality.

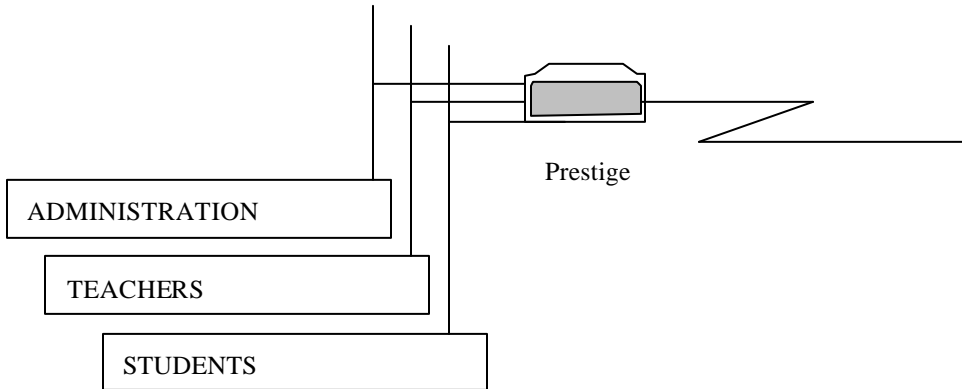


**Figure 3-3 Physical Network**



**Figure 3-4 Partitioned Logical Networks**

For example, in a school you can partition the single physical network into administration network, teachers network and students network as shown next.



**Figure 3-5 IP Alias Example**

### 3.5.2 IP Alias Setup



You must use **Menu 3.2** to configure the first network and move the cursor to **Edit IP Alias** field and toggle the space bar to choose **Yes** and press [Enter] to configure the second and third network.

```
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=
  Edit IP Alias= Yes

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

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

Pressing [Enter] opens **Menu 3.2.1 - IP Alias Setup**, as shown next.

```
Menu 3.2.1 - IP Alias Setup

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

**Figure 3-7 Menu 3.2.1 - IP Alias Setup**

Follow the instructions in the following table to configure IP Alias parameters.

### IP Alias Setup Menu Fields

Field	Description	Example
IP Alias	Choose <b>Yes</b> to configure the LAN network for the Prestige.	<b>Yes</b>
IP Address	Enter the IP address of your Prestige in dotted decimal notation	<b>192.168.2.1</b>
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige	<b>255.255.255.0</b>
RIP Direction	Press the space bar to select the RIP direction from <b>Both/In Only/Out Only</b> .	<b>Both</b>
Version	Press the space bar to select the RIP version from <b>RIP-1/RIP-2B/RIP-2M</b> .	<b>RIP-1</b>
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the Prestige.	
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Prestige.	
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.		

## 3.6 Internet Access Configuration

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

**Table 3-3 Internet Account Information**

Internet Account Information	Write your account information here
IP Address of the ISP's Gateway (Optional)	—
Telephone Number(s) of your ISP	—
Login Name	—
Password for ISP authentication	—
DNS server address(es) for your workstation	—

From the Main Menu, enter option **Internet Access Setup** to go to **Menu 4 - Internet Access Setup**, as displayed next. The table following the figure contains instructions on how to configure your Prestige for

```

Menu 4 - Internet Access Setup

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

Telco Options:
Transfer Type= 64K

Multilink= Off
Idle Timeout= 100

Press ENTER to CONFIRM or ESC to CANCEL:

```

Enter the phone number of your ISP

Enter your login and password

Internet access.

**Figure 3-8 Menu 4 – Internet Access Setup**

**Table 3-4 Internet Access Setup Menu Fields**

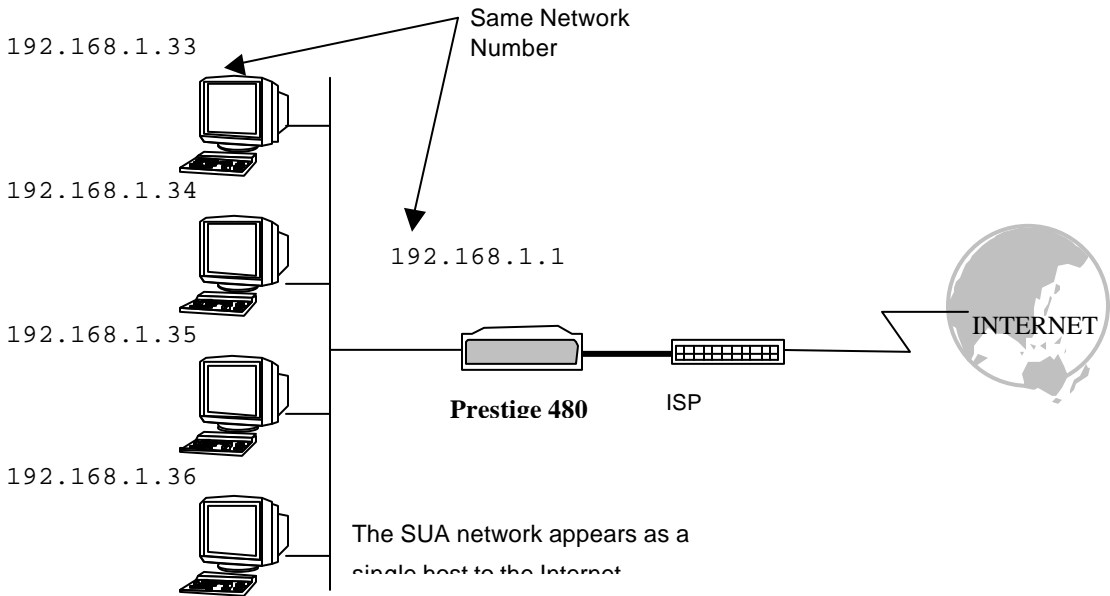
<b>Field</b>	<b>Description</b>
ISP's Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.
Pri Phone and Sec Phone Number	Both the Primary and the Secondary Phone number refer to the number that the Prestige dials to connect to the ISP.
My Login Name	Enter the login name given to you by your ISP.
My Password	Enter the password associated with the login name above.
Single User Account	Please see the following section for a more detailed discussion on the Single User Account feature. The default is <b>Yes</b> .
IP Address	If your ISP did <i>not</i> assign you a static IP address, enter [0.0.0.0] here; otherwise, enter that IP address here.
Telco options      Transfer Type	This field specifies the type of connection between the Prestige and this remote node. Select <b>64K</b> , or <b>Leased</b> .
Multilink	The Prestige uses the PPP Multilane Protocol to bundle multiple links in a single connection to boost the effective throughput between two nodes. This option is only available if the transfer type is <b>64K</b> . See <b>Menu 11.2</b> for more details.
Idle Timeout	This value specifies the number of idle seconds that elapses before the remote node is automatically disconnected. Idle seconds is the period of time when no data is transmitted from your Prestige. Administrative packets such as RIP are not counted as data. The default is <b>100</b> seconds. <i>This option only applies when the Prestige initiates the call.</i>

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

### 3.7 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 3-9 Single User Account Topology**

The Single User Account feature may also be used on connections to remote networks other than the ISP. For example, this feature can be used to simplify the allocation of IP addresses when connecting branch offices to the corporate network.

The IP address for the SUA can be either fixed or dynamically assigned when a call is connected. In addition, you can designate servers using **Menu 15**, e.g., a web server and a telnet server, on your local network and make them accessible to the outside world. For more information on setting up servers see the section **Multiple Servers behind SUA** in the chapter **Dial-in Server Configuration**.

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)*.

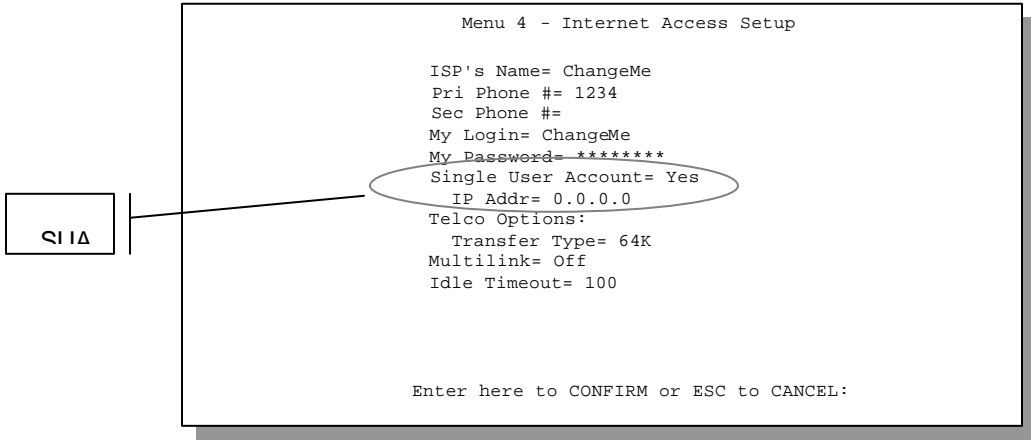
### **3.7.1 Advantages of SUA**

In summary:

- SUA is a cost-effective solution for small offices with less than 64 hosts to access the Internet or other remote TCP/IP networks.
- SUA supports servers to be accessible to the outside world.
- SUA can provide firewall protection if you do not specify a server. All incoming inquiries will be filtered out by your Prestige.
- UDP and TCP packets can be routed. In addition, partial ICMP, including echo and trace route, is supported.

### 3.7.2 Single User Account Configuration

The steps for configuring your Prestige for Single User Account are identical to the conventional Internet access with the exception that you need to fill in two extra fields in **Menu 4 - Internet Access Setup**, as shown next.



**Figure 3-10 Menu 4 – Internet Access Setup for Single User Account**

To enable the SUA feature in Menu 4, move the cursor to the **Single User Account** field and select **Yes** (or **No** to disable SUA). Then follow the instructions on how to configure the SUA fields.

**Table 3-5 Single User Account Menu Fields**

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



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

## **3.8 Mega Bundle or Multiple ISPs Support**

### **3.8.1 Basics**

If ISPs do not support multilink bundle of more than 2 links, it would be impossible for a user to dedicate all 4 channels available in a P 480 to Internet access. To differentiate P 480 from other similarly equipped products, it is desirable to be able to support bundle of 4 links where P 480 calls a second ISP when the traffic exceeds a certain threshold and split the traffic between the two connections. The Prestige refers to this multiple ISPs support as Mega Bundle.

Mega Bundle design is as listed below.

1. *One remote node* is designated as the main ISP and *another* the supplementary ISP. The Prestige dials the first and second link on the main ISP using the existing mechanism.
2. If a supplementary remote node is specified, BOD behaves as if the maximum number of channels is 4 and the adding and dropping of channels are governed by the main remote node's multilink parameters alone.
3. When the traffic triggers the third link (as determined by BOD), the Prestige calls the supplementary ISP. Since the new connection is a separate PPP session, it will have a different IP address and thus a new interface.
4. Because of NAT, if an IP connection is already assigned to a particular interface, then it must remain on that interface. For new connections, the round-robin method is used to assign a connection to either the main or the supplementary ISP. Non-IP traffic is simply distributed evenly on a packet-by-packet basis.
5. Once the Prestige determines which interface a connection uses, the MP channel assignment within each bundle remains the same as the existing method.

## 3.8.2 ISP Remote Node and Supplementary Remote Node

The previous ZyNOS versions supported only one ISP account. That remote node is called as the “ISP remote node”. Now in ZyNOS v2.42, you can setup other ISP accounts and this is called as “supplementary remote node”.

You can have several “Supplementary remote node”, but only one “ISP remote node”. These remote nodes can work at the same time. “Supplementary remote” is almost the same as “ISP remote node” except that “supplementary remote node” will not appear in the routing table as default route.

## 3.9 Configuring Mega Bundle

**Step 1.** Configure an ISP remote node.

1. Setup ISP in **Menu 4**.
2. Set **Multilink= BOD** or **Multilink= Always** in **Menu 4**
3. In **Menu 11**, edit the ISP remote node.

```
Menu 11.2 - Remote Node PPP Options

Encapsulation= Standard PPP
Compression= No
BACP= Enable
Mega Bundle= None

Multiple Link Options:
  BOD Calculation= Transmit or Receive
  Min. Channels= 1
  Max. Channels= 1
```

4. Set **Edit PPP Options= Yes** and then press [Enter]. You will enter **Menu 11.2**

5. In **Menu 11.2**, set **Max. Channels= 3** or **Max. Channels= 4**

6. Save the configuration.

**Step 2.** Configure a supplementary remote node.

1. Setup a remote node in **Menu 11**.

2. Set **Edit PPP Options= Yes** and then press [Enter]. You will enter **Menu 11.2**

3. Set **Mega Bundle= Supplementary**. Return to **Menu 11.1**.

4. Set **Rem IP Addr = 1.2.3.4**. The value can be arbitrary IP address except **0.0.0.0** and **1.1.1.1**.

5. Set **Edit IP/IPX/Bridge= Yes** and then press [Enter]. You will enter **Menu 11.3**.

6. Set **Rem Subnet Mask= 0.0.0.0**

7. Save the configuration.

Check the configuration in **Menu 11**. If the supplementary remote node is configured, you can see it in **Menu 11**. The following is a reference screen. Node 2 is a supplementary remote node.

```
Menu 11 - Remote Node Setup

1. ChangeMe (ISP, SUA)
2. Hinet (SUP)
3. _____
4. _____
5. _____
6. _____
7. _____
```

## 3.10 Configuring Backup ISP Accounts

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

### 3.10.1 Configure a Backup ISP

To configure a backup ISP Account, follow these steps:

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

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

### 3.10.2 To Switch ISP

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

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

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



# Chapter 4

## Remote Node Configuration

*This chapter covers the parameters that are protocol independent. The protocol-dependent configuration (TCP/IP) is covered in the next chapter.*

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

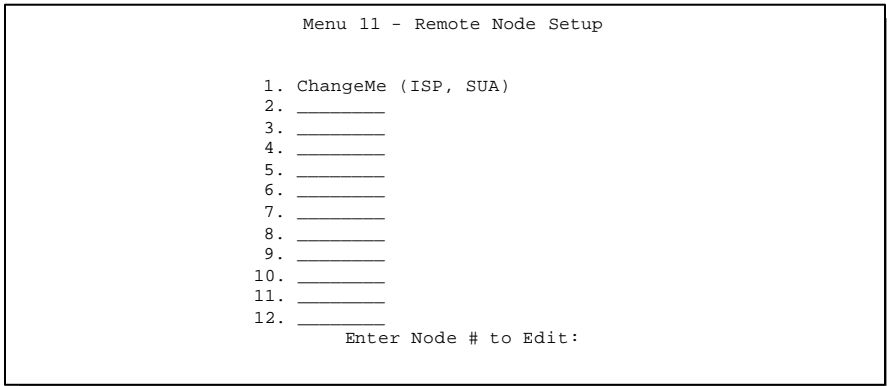
### 4.1 Remote Node Setup

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

#### 4.1.1 Remote Node Profile

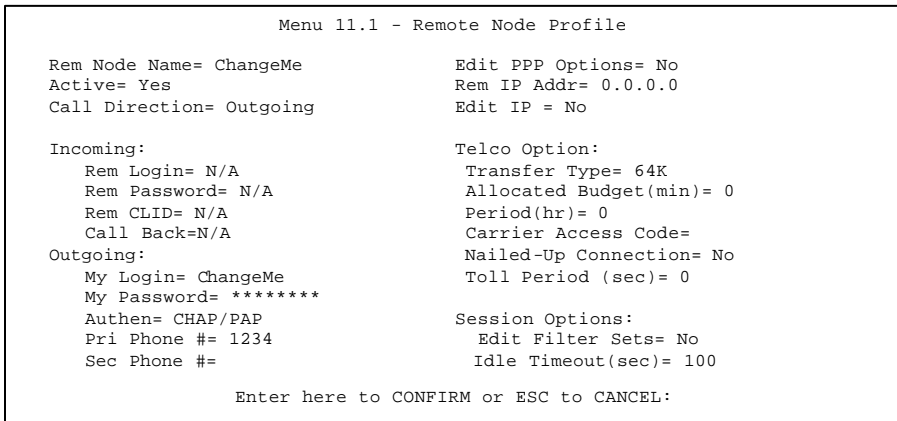
To configure a remote node, follow these steps:

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



**Figure 4-1 Menu 11 – Remote Node Setup**

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





## Figure 4-2 Menu 11.1 Remote Node Profile

### Table 4-1 Remote Node Profile Menu Fields

Field	Description	Options
Rem Node Name	This is a required field [?]. Enter a descriptive name for the remote node, for example, Corp.  This field can be up to eight characters. This name must be unique from any other remote node name or remote dial-in user name.	
Active	Press the space bar to toggle between <b>Yes</b> and <b>No</b> . Inactive nodes are displayed with a minus sign (-) at the beginning of the name in Menu 11.	Press space bar to toggle <b>Yes/No</b>
Call Direction	If this parameter is set to <b>Both</b> , your Prestige can both place and receive calls to/from this remote node.  If set to <b>Incoming</b> , your Prestige will not place a call to this remote node.  If set to <b>Outgoing</b> , your Prestige will drop any incoming calls from this remote node.  Several other fields in this menu depend on this parameter. For example, in order to enable <b>Callback</b> , the <b>Call Direction</b> must be <b>Both</b> .	<b>Both</b>  <b>Incoming</b>  <b>Outgoing</b>
Incoming: Rem Node Login Name	Enter the login name that this remote node will use when it calls your Prestige.  The login name in this field combined with the Rem Node Password will be used to authenticate this node.	
Incoming: Rem Node Password	Enter the password used when this remote node calls your Prestige.	
Incoming: Rem CLID	This field is applicable only if <b>Call Direction</b> is either <b>Both</b> or <b>Incoming</b> . Otherwise, a <b>N/A</b> appears in the field.  This is the Calling Line ID (the telephone number of the calling party) of this remote node.  If you enable the CLID Authen field in Menu 13 – Default Dial In, your Prestige will check the CLID in the incoming call against the CLIDs in the database. If no match is found and CLID Authen is Required, the call will be dropped.	
Incoming: Callback	This field is applicable only if <b>Call Direction</b> is <b>Both</b> . Otherwise, a <b>N/A</b> appears in the field.	<b>Enable</b> <b>Disable</b>

	<p>This field determines whether or not your Prestige will call back after receiving a call from this remote node.</p> <p>If this option is enabled, your Prestige will disconnect the initial call from this node and call it back at the Outgoing Primary Phone Number (see below).</p>	
Outgoing: My Login Name	<p>This is a required field [?] if <b>Call Direction</b> is either <b>Both</b> or <b>Outgoing</b>. Enter the login name for your Prestige when it calls this remote node.</p>	
Outgoing: My Password	<p>This is a required field [?] if <b>Call Direction</b> is either <b>Both</b> or <b>Outgoing</b>. Enter the password for your Prestige when it calls this remote node.</p>	
Outgoing: Authen	<p>This field sets the authentication protocol used for outgoing calls. Options for this field are:</p> <p><b>CHAP/PAP</b> - Your Prestige will accept either CHAP or PAP when requested by this remote node.</p> <p><b>CHAP</b> - accept CHAP only.</p> <p><b>PAP</b> - accept PAP only.</p>	<p><b>CHAP/ PAP</b></p> <p><b>CHAP</b></p> <p><b>PAP</b></p>
Outgoing: Pri(ary) Sec(ondary) Phone Numbers	<p>Your Prestige always calls this remote node using the Primary Phone number first for a dial-up line.</p> <p>If the Primary Phone number is busy or does not answer, your Prestige will dial the Secondary Phone number if available.</p> <p>Some areas require dialing the pound sign # before the phone number for local calls. A # symbol may be included at the beginning of the phone numbers as required.</p>	
Edit PPP Options	<p>To edit the PPP options for this remote node, move the cursor to this field, use the space bar to select <b>Yes</b> and press [Enter]. This will bring you to Menu 11.2 - Remote Node PPP Options. For more information on configuring PPP options, see the section <i>Editing PPP Options</i>.</p>	<p>Press space bar to toggle <b>Yes</b> then press [Enter]</p>
Rem IP Addr	<p>Enter the IP address of the remote gateway.</p>	
Telco Options: Allocated Budget (min)	<p>This field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 for no budget control.</p>	<p>Default = 0</p>
Period (hr)	<p>This field sets the time interval to reset the above outgoing call budget control.</p>	
Transfer Type	<p>This field specifies the type of connection between the Prestige</p>	<p><b>64k/</b></p>

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

### 4.1.2 Nailed-up Connection

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

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

### 4.1.3 Outgoing Authentication Protocol

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

successful authentication, please make sure that you specify the correct authentication protocol when connecting to such an implementation.

#### **4.1.4 PPP Multilink**

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

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

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

#### **4.1.5 Bandwidth on Demand**

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

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

Table 4-2 BTR v MTR for BOD

BTR & MTR Setting	No. of channel(s) used	Max No. of channel(s) used	Bandwidth on demand
BTR = 64, MTR = 64	1	1	Off
BTR = 64, MTR = 128	1	2	On
BTR = 128, MTR = 128	2	2	Off
BTR = 256, MTR = 256	4	4	On

The **Min. Channels** and **Max. Channels** allows you to force the Prestige to use a minimum and maximum number of channels.

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

When the **Max. Channels** is set to 3 or 4 and the threshold set in the **Target Utility** is reached for the second channel a third and fourth channel is opened. The **Bandwidth increment for Additional Channels** specifies the line utilization range at which you want the Prestige to add or subtract the third and fourth channel.

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

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

You can do the BOD configuration using **Menu 11.2 - Remote Node PPP Options**.

## 4.1.6 Editing PPP Options

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

```
Menu 11.2 - Remote Node PPP Options

Encapsulation= Standard PPP
Compression= No
BACP= Enable

Multiple Link Options:
  BOD Calculation= Transmit or Receive
  Min. Channels= 1
  Max. Channels= 1
  Target Utility for 2nd Channel(Kbps)= 32-48
  Bandwidth increment for Additional Channels(Kbps)= 64
  Add Persist(sec)= 5
  Subtract Persist(sec)= 5

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

**Figure 4-3 Menu 11.2 - Remote Node PPP Options**

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

**Table 4-3 Remote Node PPP Options Menu Fields**

<b>Field</b>	<b>Description</b>	<b>Option</b>
Encapsulation	Select the CISCO PPP only when this remote node is a Cisco machine; otherwise, select the Standard PPP.	<b>Standard PPP</b>  <b>CISCO PPP</b>
Compression	You can turn on or off Stac Compression. The default for this field is <b>Yes</b> .	<b>Yes/No</b>  (Default = <b>Yes</b> )
BACP	Allows you to enable or disable the Bandwidth Allocation Control Protocol (BACP).  The default for this field is <b>Enable</b> .	<b>Enable/Disable</b>  Default = <b>Enable</b>
Multiple Link Options:		
BOD Calculation	Select the direction of the traffic you wish to use in determining when to add or subtract a link. The default for this field is <b>Transmit or Receive</b> .	Default = <b>Transmit or Receive</b>
Min. Channel	Allows you to set the minimum number of channels the Prestige uses.	<b>1-4</b>
Max. Channels	Allows you to set the maximum number of channels the Prestige uses.	<b>1-4</b>
Target Utility (kbps)	Enter the two thresholds separated by a [-] for subtracting and adding the second port.	Default=32-48
Bandwidth Increment	Allows you set bandwidth increment for the additional channels, once the threshold is reached additional channels are opened if the Min. Channels is greater than one.	Default = <b>64</b> Kbps <b>0-64</b>
Add Persist	This parameter specifies the number of seconds where traffic is above the adding threshold before the Prestige will bring up an additional link.	Default = 5 sec
Subtract Persist	This parameter specifies the number of seconds where traffic is below the subtraction threshold before your Prestige drops a link.	Default = 5 sec
Once you have completed filling in <b>Menu 11.2 - Remote Node PPP Options</b> , press [Enter] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] at any time to cancel.		

### 4.1.7 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in **Menu 11.1**, then press the space bar to toggle and set the value to **YES**. Press [ENTER] to open **Menu 11.5 – Remote Node Filter**.

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

Note that spaces are accepted in this field. For more information on defining the filters, *see Chapter 9*. The Prestige comes with a prepackaged filter set, NetBIOS\_WAN, that blocks NetBIOS packets. You can include this in the call filter sets if you wish to prevent NetBIOS packets from triggering calls to a remote node.

```
Menu 11.5 - Remote Node Filter

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

**Figure 4-4 Menu 11.5 – Remote Node Filter**



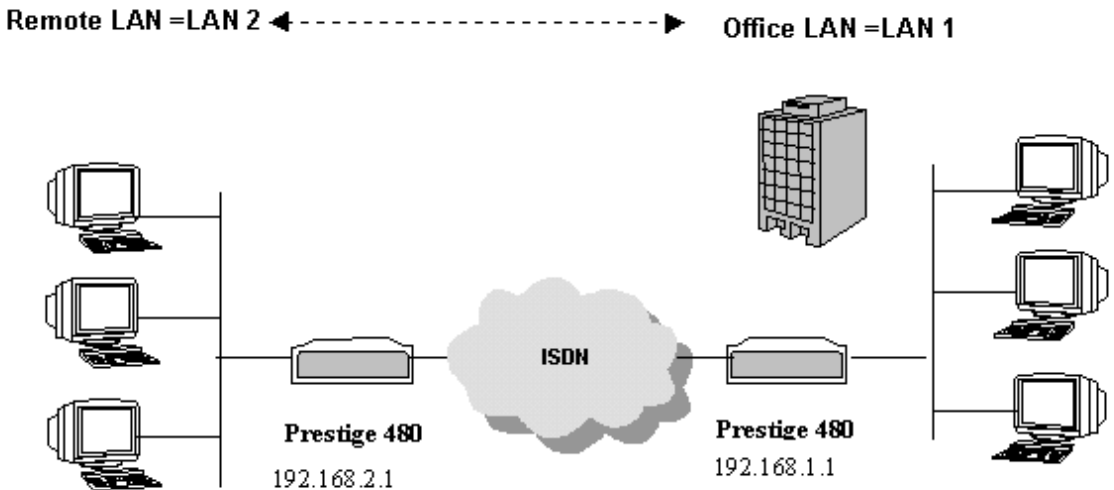
# Chapter 5

## Remote Node TCP/IP Configuration

*This chapter shows you an example of LAN-to-LAN application and explains 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 (remote LAN) to the headquarters (office LAN), as depicted in the following diagram.



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

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

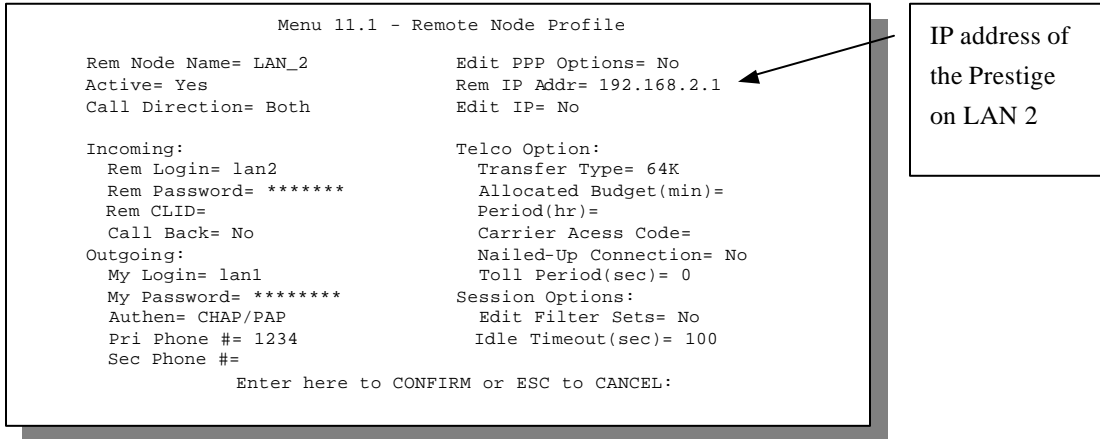
### LAN 1 Setup

```
Menu 11.1 - Remote Node Profile

Rem Node Name= LAN_2          Edit PPP Options= No
Active= Yes                   Rem IP Addr= 192.168.2.1
Call Direction= Both         Edit IP= No

Incoming:
  Rem Login= lan2             Telco Option:
  Rem Password= *****      Transfer Type= 64K
  Rem CLID=                   Allocated Budget(min)=
  Call Back= No               Period(hr)=
                                Carrier Access Code=
Outgoing:                     Nailed-Up Connection= No
  My Login= lan1              Toll Period(sec)= 0
  My Password= *****       Session Options:
  Authen= CHAP/PAP            Edit Filter Sets= No
  Pri Phone #= 1234           Idle Timeout(sec)= 100
  Sec Phone #=

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



IP address of the Prestige on LAN 2

Figure 5-2 LAN 1 Setup

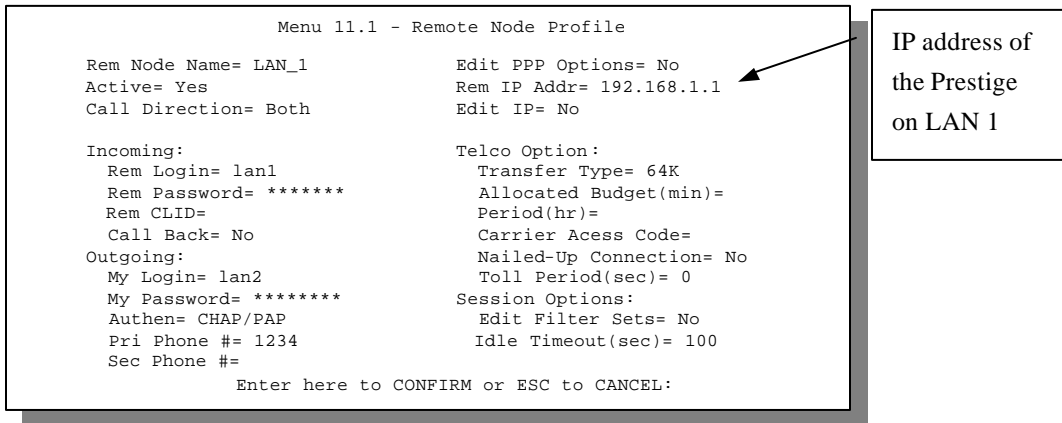
### LAN 2 Setup

```
Menu 11.1 - Remote Node Profile

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

Incoming:
  Rem Login= lan1             Telco Option:
  Rem Password= *****      Transfer Type= 64K
  Rem CLID=                   Allocated Budget(min)=
  Call Back= No               Period(hr)=
                                Carrier Access Code=
Outgoing:                     Nailed-Up Connection= No
  My Login= lan2              Toll Period(sec)= 0
  My Password= *****       Session Options:
  Authen= CHAP/PAP            Edit Filter Sets= No
  Pri Phone #= 1234           Idle Timeout(sec)= 100
  Sec Phone #=

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



IP address of the Prestige on LAN 1

Figure 5-3 LAN 2 Setup

## 5.2 Remote Node Setup

Follow the procedure in *Chapter 4 - Remote Node Configuration* to configure the protocol-independent parameters in Menu 11 - Remote Node Profile. For the TCP/IP parameters, follow the instructions below. If you are configuring your Prestige to receive incoming calls, you also need to set the default dial-in parameters in Menu 13.

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

Move the cursor to the **Edit IP** field in **Menu 11.1**, then press the space bar to toggle and set the value to **Yes**. Press [Enter] to open Menu 11.3 - Network Layer Options.

```
Menu 11.3 - Remote Node Network Layer Options

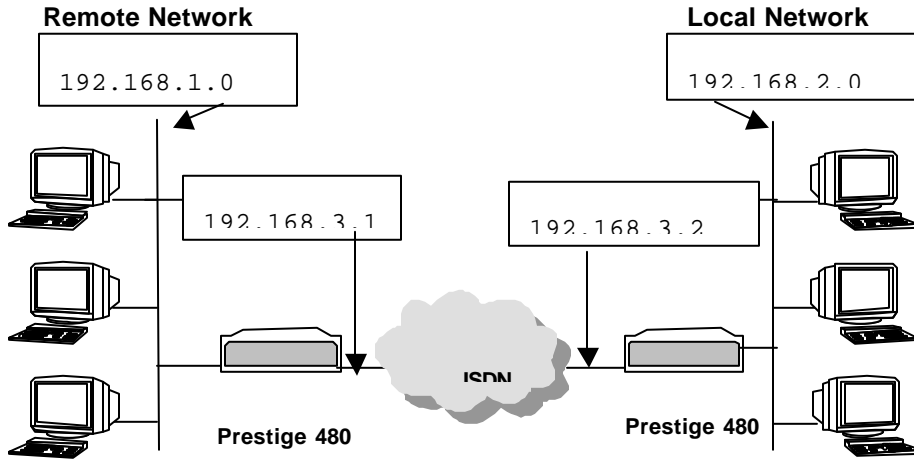
Rem IP Addr: 0.0.0.0
Rem Subnet Mask= 0.0.0.0
My WAN Addr= 0.0.0.0
Single User Account= No

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

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

Figure 5-4 Menu 11.3- Remote Node TCP/IP Options

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



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

To configure the TCP/IP parameters of a remote node, first configure the two fields in Menu 11-1 Remote Node Profile, as shown in the table below. For more details on the IP Option fields, refer to *Chapter 3 – Internet Access Application*.

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

Field	Description	Option
Rem IP Address	Enter the IP address of the remote gateway in Remote Node Profile.	
Edit IP	Press the space bar to select <b>Yes</b> and press [Enter] to go to Menu 11.3 - Remote Node Network Layer Options Menu.	<b>Yes</b> (Yes/No)

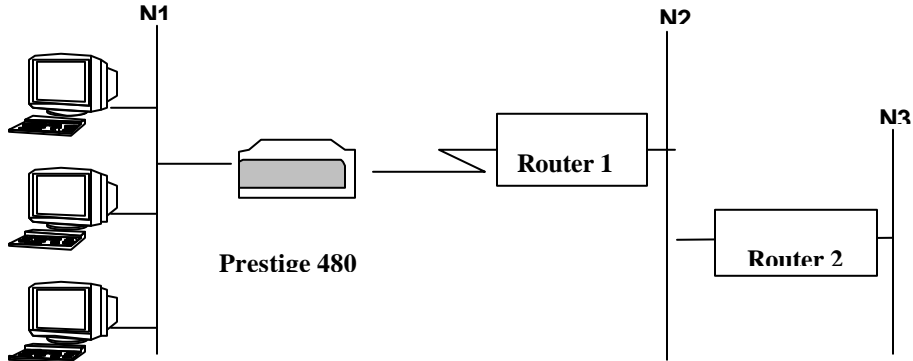
The next table shows the TCP/IP related fields in **Menu 11.3 - Remote Node Network Layer Options**.

**Table 5-2 TCP/IP Remote Node Configuration**

Rem IP Address	This will show the IP address you entered for this remote node in the previous menu.	
Rem IP Subnet Mask	Enter the subnet mask for the remote network.	
My WAN Addr	Some implementations, especially the UNIX derivatives, require the ISDN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the ISDN port of your Prestige.  Note that this is the address assigned to your local Prestige, not the remote router.	
Single User Account	Set this field to <b>Yes</b> to enable the Single User Account feature for your Prestige. Use the space bar to toggle between <b>Yes</b> and <b>No</b> . See <i>Chapter 3 - Internet Access Application</i> for more information on the Single User Account feature.	<b>Yes/No</b>
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	<b>1 to 15</b>
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to <b>Yes</b> , this route is kept private and not included in RIP broadcast. If <b>No</b> , the route to this remote node will be propagated to other hosts through RIP broadcasts.	<b>Yes/No</b>
RIP	Press the space bar to select the <b>RIP direction</b> from <b>Both/ None/In Only/Out Only</b> .	(Default= <b>Both</b> )
Version=	Press the space bar to select the RIP version from <b>RIP-1/RIP-2B/RIP-2M</b> .	<b>RIP-1</b> (default)
Once you have completed filling in the Network Layer Options Menu, press [Enter] to return to Menu 11. Press [Enter] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] at any time to cancel.		

## 5.2.1 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.

**Figure 5-6 Example of Static Routing Topology**

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

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

```
Menu 12 - IP Static Route Setup
1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____

Enter selection number:
```

**Figure 5-7 Menu 12.1 – IP Static Route Setup**

```
Menu 12.1 - Edit IP Static Route

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

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

**Figure 5-8 Edit IP Static Route Setup**

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

**Table 5-3 Edit IP Static Route Menu Fields**

<b>Field</b>	<b>Description</b>
Route Name	Enter a descriptive name for this route. This is for identification purposes only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the subnet mask for this destination. Follow the discussion on IP subnet mask in this chapter.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Prestige that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Prestige; over WAN, the gateway must be the IP address of one of the remote nodes.
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to <b>Yes</b> , this route is kept private and not included in RIP broadcast. If <b>No</b> , the route to this remote node will be propagated to other hosts through RIP broadcasts.



# Chapter 6

## IPX Configuration

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

### 6.1 IPX Network Environment

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

#### 6.1.1 Network and Node Number

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

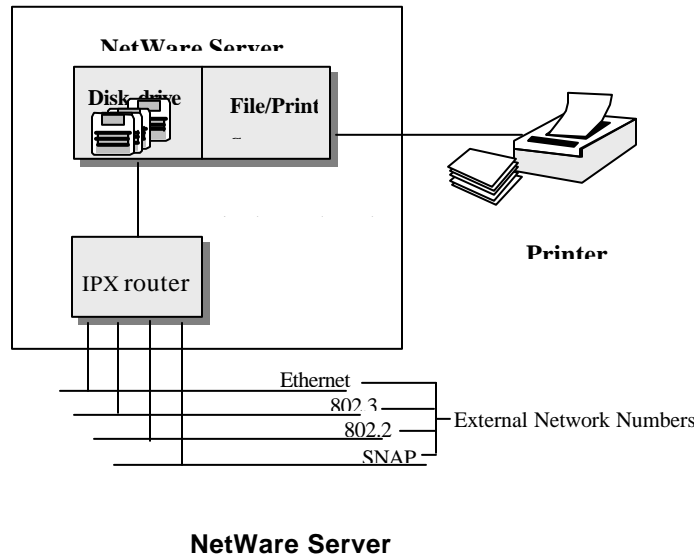
An IPX client obtains its network number from a server that has the network numbers statically configured. If there are multiple servers on a network, only one server need to have the network numbers configured, and all other stations (clients and servers) can obtain the network numbers from it. The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

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

#### 6.1.2 Frame Types

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

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



### **6.1.3 External Network Number**

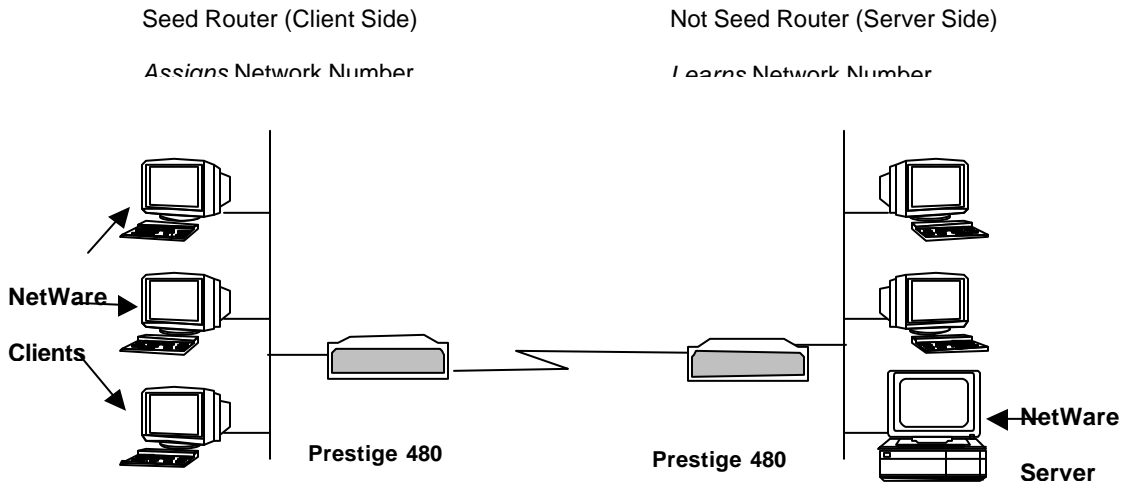
Each of the four logical networks (based on frame type) has its own external network number.

### **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 network, either internal or external.

## 6.2 Prestige in an IPX Environment

There are two scenarios in which your Prestige is deployed, depending on whether there is a NetWare server on the LAN or not, as depicted in the following diagram.



**Prestige in an IPX Environment**

### 6.2.1 Prestige on LAN with Server

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

## 6.2.2 Prestige on LAN without Server

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

## 6.3 IPX Spoofing

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

The built-in call filters are defined as follows:

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

## 6.4 IPX Ethernet Setup

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

```
Menu 3.3 - Novell IPX Ethernet Setup

Seed Router= No

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

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

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

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

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

### **Menu 3.3 - Novell IPX Ethernet Setup**

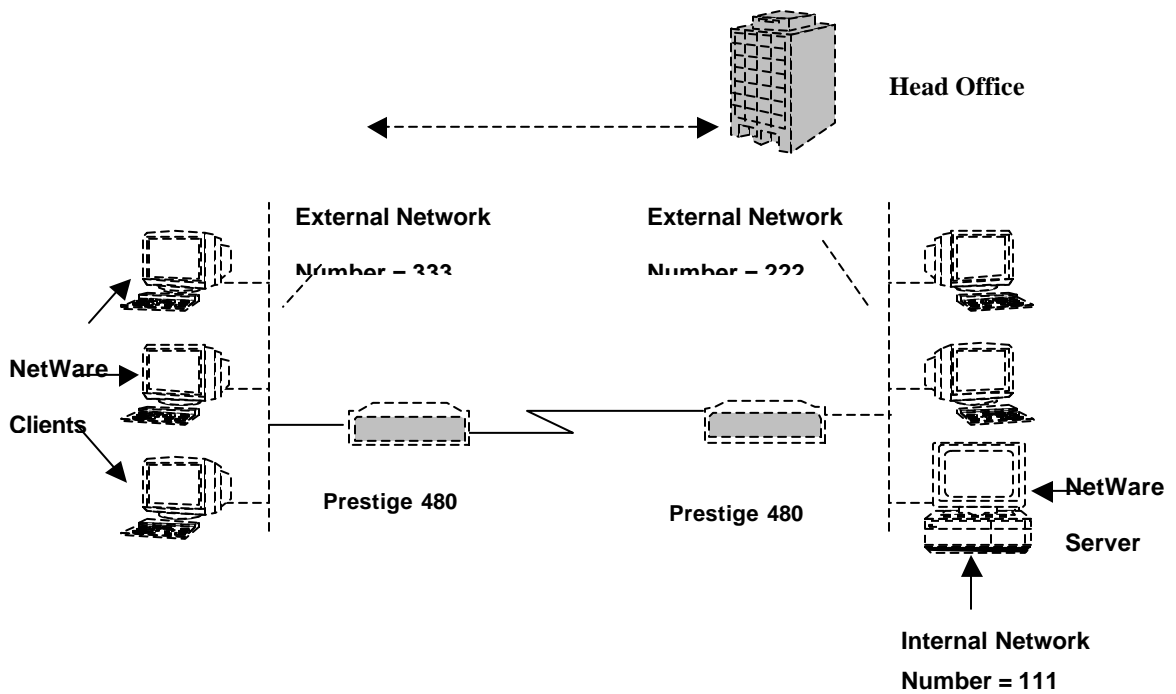
The following table describes the Novell IPX Ethernet Setup Menu.

**Novell IPX Ethernet Setup Fields**

<b>Field</b>	<b>Description</b>	<b>Options</b>
Seed Router	Determine if your Prestige is to act as a seed router.	<b>Yes/No</b>
Frame Type	Enable/Disable the individual frame type. Remember to enable only the ones that are actually used on your network.	<b>802.2</b> <b>802.3</b> <b>Ethernet II</b> <b>SNAP</b>
IPX Network #	If your Prestige is a seed router, enter a unique network number for each frame type enabled.	
Press [Enter] at the message [Press ENTER to Confirm ...] to save your configuration, or press [Esc] at any time to cancel.		

## 6.5 LAN-to-LAN Application with Novell IPX

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



LAN-to-LAN Application with Novell IPX

## 6.6 IPX Remote Node Setup

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

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

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

```
Menu 11.3 - Remote Node Network Layer Options

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

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

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

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

### Menu 11.3 - Remote Node Novell IPX Options



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

### Remote Node Novell IPX Options

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

Once you have completed filling in the Network Layer Options Menu, press [Enter] to return to Menu 11.1. Then press [Enter] at the message [Press ENTER to Confirm] to save your configuration, press [Esc] to cancel.

## 6.6.1 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 next.

```
Menu 12.2.1 - Edit IPX Static Route

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

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

### Menu 12.2 - Edit IPX Static Route

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

### **Edit IPX Static Route Menu Fields**

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



# Chapter 7

## Bridging Setup

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

### 7.1 Bridging in General

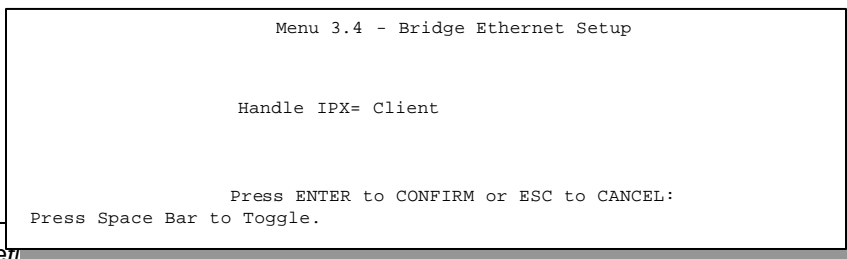
Bridging bases the forwarding decision on the MAC (Media Access Control), or hardware address, while routing does it on the network layer (IP or IPX) address. Bridging allows the Prestige to transport packets of network layer protocols that the Prestige does not route, e.g., SNA, from one network to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

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

### 7.2 Bridge Ethernet Setup

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

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



### Menu 3.5 - Bridge Ethernet Setup

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

**Bridge Ethernet Setup Menu - Handle IPX Field Configuration**

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

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

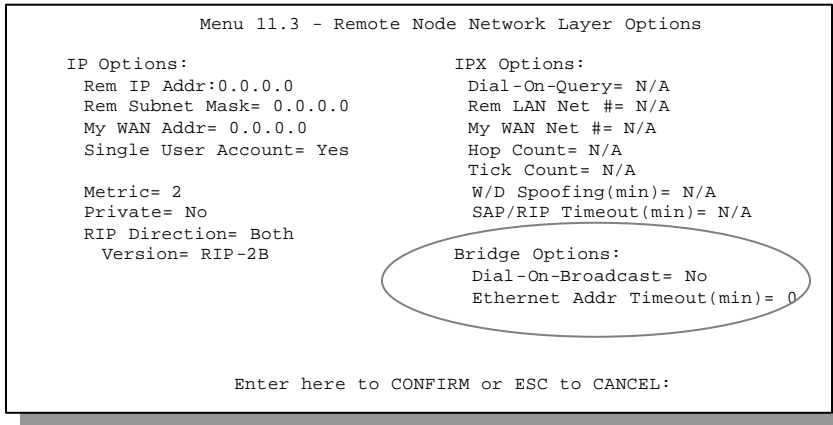
#### 7.2.1 Remote Node Bridging Setup

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

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

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

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



[Enter] to open **Menu 11.3 - Network Layer Options**.

### Menu 11.3 - Remote Node Bridging Options

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

#### Remote Node Network Layers Menu Bridge Options

Field	Description
Bridge	Make sure this field is set to <b>Yes</b> .
Edit IP/IPX/Bridge	Press the space bar to change it to <b>Yes</b> and press [Enter] to go to the Network Layer Options Menu.
Dial-On-Broadcast	This field is necessary for your Prestige on the caller side LAN. When set to <b>Yes</b> , any broadcasts coming from the LAN will trigger your Prestige to make a call to this remote node. If it is set to <b>No</b> , your Prestige will not make the outgoing call.
Ethernet Addr	In this field, enter the time (number of minutes) that you wish your Prestige to

Timeout (min)	retain the Ethernet Addr information in its internal tables while the line is down. If this information is retained, your Prestige will not have to recompile the tables when the line is brought back up.
Once you have completed filling in the Network Layer Options Menu, press [Enter] to return to Menu 11.1. Then press [Enter] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] to cancel.	

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

Enter selection number:
```

### 7.3 Bridge Static Route Setup

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

#### Menu 12.3 - Bridge Static Route Setup

```
Menu 12.3.1 - Edit Bridge Static Route

Route #: 1
Route Name= ?
Active= No
Ether Address= ?
IP Subnet Mask=
Gateway IP = 1

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



**Menu 12.3.1 - Edit Static Route**

The following table describes the Bridge Static Route Menu.

**Bridge Static Route Menu Fields**

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

## Chapter 8

# Dial-in Server Configuration

*This chapter shows you how to configure your Prestige to receive calls from remote dial-in users, e.g., telecommuters, as well as remote nodes.*

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

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

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

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

Due to memory constraints, your Prestige can only store a finite number of users locally. If there are more remote dial-in users than what Prestige can support locally, you can use an external RADIUS server to provide authentication service. For details on using a RADIUS server, see the *Using RADIUS Authentication* section in *Chapter 12 - System Security*.

## 8.1 Remote Access Server

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

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

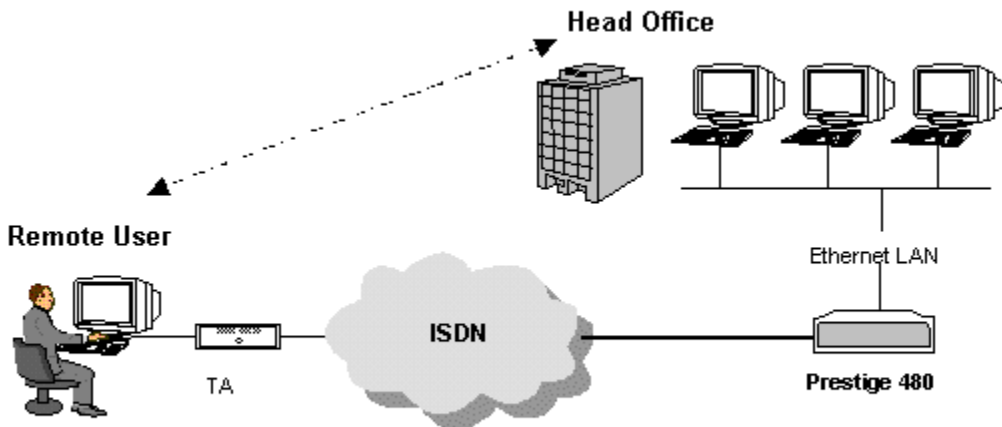


Figure 8-1 Example of Remote Access Server Application

## 8.2 LAN-to-LAN Server Application

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

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

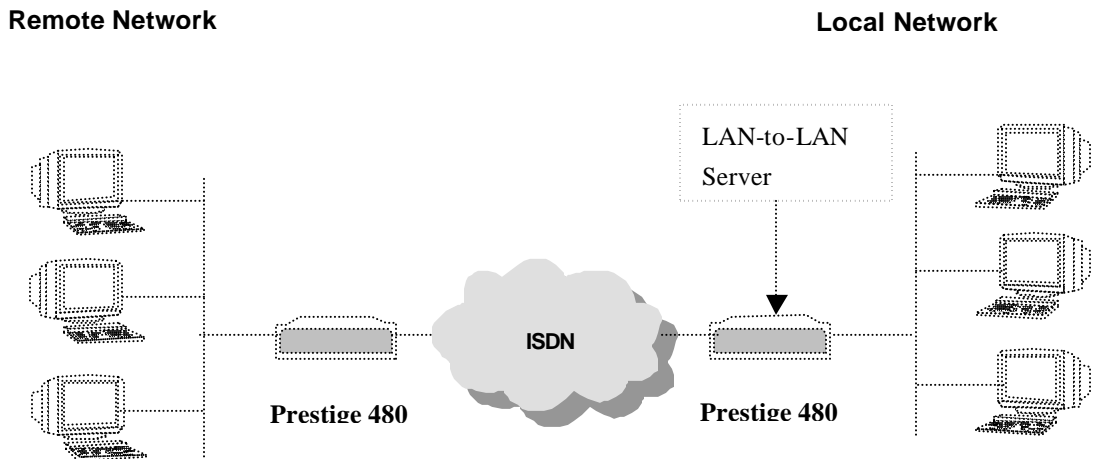


Figure 8-2 Example of a LAN-to-LAN Server Application

## 8.3 Default Dial-in Setup

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

```
Menu 13 - Default Dial-in Setup

Telco Options:
  CLID Authen= None

PPP Options:
  Recv Authen= CHAP/PAP
  Compression= Yes
  Mutual Authen= No
  O/G Login= 3
  O/G Password= ****
  Multiple Link Options:
    Max Trans Rate= 256

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

IP Address Supplied By:
  Dial-in User= Yes
  IP Pool= No
  IP Start Addr= 192.168.129.1
  IP Count(1,4)= 2

Session Options:
  Edit Filter Sets= No

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

node.

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

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

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

**Table 8-2 Default Dial-in Setup Fields**

Field	Description	Option
-------	-------------	--------

Telco Options: CLID Authen	<p>This field sets the CLID authentication parameter for all incoming calls. There are three options for this field:</p> <ul style="list-style-type: none"> <li>● <b>None</b> - No CLID is required.</li> <li>● <b>Required</b> – CLID must be available, or the Prestige will not answer the call.</li> <li>● <b>Preferred</b> - If the CLID is available then CLID will be used; otherwise, authentication is performed in PPP negotiation.</li> </ul>	<p><b>None</b> <b>Required</b> <b>Preferred</b></p>
PPP Options:		
Recv. Authen	<p>This field sets the authentication protocol for incoming calls. For security reason, setting authentication to none is strongly discouraged. Options for this field are:</p> <ul style="list-style-type: none"> <li>● <b>CHAP/PAP</b> - Your Prestige will try CHAP first, but PAP will be used if CHAP is not available.</li> <li>● <b>CHAP</b> – Use CHAP only.</li> <li>● <b>PAP</b> – Use PAP only.</li> <li>● <b>None</b> – Your Prestige tries to acquire CHAP/PAP first, but no authentication is required if CHAP/PAP is not available.</li> </ul>	<p><b>CHAP/PAP</b> <b>CHAP</b> <b>PAP</b> <b>None</b></p>
Compression	<p>You can turn on or off Stac Compression. The default for this field is <b>Yes</b>.</p>	<p><b>Yes/No</b></p>
Mutual Authen	<p>Some vendors, e.g., Cisco, require mutual authentication, i.e., the node that initiates the call will request a user name and password from the far end that it is dialing to. If the remote node requires mutual authentication, set this field to <b>Yes</b>.</p>	<p><b>Yes/No</b></p>
O/G Login	<p>Enter in the login name to be used to respond to the peer's authentication request.</p>	
O/G Password	<p>Enter in the outgoing password to be used to respond to the peer's authentication request.</p>	
Multiple Link Options:		
Max Trans Rate	<p>Enter the maximum data transfer rate between your Prestige and the remote dial-in user. 64 - At most, one B channel is used. 128 - A maximum of two channels can be used.. When the Prestige calls back to the remote dial-in user, the maximum data transfer rate is always 64.</p>	<p><b>64</b> <b>128</b> <b>192</b> <b>256</b></p>

Callback Budget Management:		
Allocated Budget (min)	This field sets the budget callback time for all the remote dial-in users. The default for this field is <b>0</b> for no budget control.	Default = <b>0</b>
Period (hr)	This field sets the time interval to reset the above callback budget control.	
IP Address Supplied By: Dial-in User	If set to <b>Yes</b> , the Prestige will allow a remote host to specify its own IP address.  If set to <b>No</b> , the remote host must use the IP address assigned by your Prestige from the IP pool, configured below. This is to prevent the remote host from using an invalid IP address and potentially disrupting the whole network.	(Default = <b>Yes</b> ) <b>Yes/No</b>
IP Pool	This field tells your Prestige to provide the remote host with an IP address from the pool. This field is required if <b>IP Address Supplied By: Dial-in User</b> is set to <b>No</b> . You can configure this field even if Dial-in User is set to <b>Yes</b> , in which case your Prestige will accept the IP address if the remote peer specifies one; otherwise, an IP address is assigned from the pool.	<b>Yes/No</b> (Default = <b>No</b> )
IP Pool: IP Start Addr	This field is applicable only if you selected <b>Yes</b> in the Dial-In IP Address Supplied By: IP Pool field.  The IP pool contains contiguous IP addresses and this field specifies the first one in the pool.	
IP Count (1,4)	In this field, enter the number ( <b>1</b> or <b>4</b> ), of addresses in the IP Pool. For example, if the starting address is 192.168.135.5 and the count is 4, then the pool will have 192.68.135.5 and 192.68.135.8	<b>1, 4</b>
Session Options: Edit Filter Sets	Press <b>Yes</b> , then [Enter] to edit the filter sets. Keep in mind that the filter set(s) will only apply to remote dial-in users but not the remote nodes.  Note that spaces and [-] symbol, are accepted in this field. For more information on customizing your filter sets, see <i>Chapter 9 - Filter Configuration</i> . The default is blank, i.e., no filters.	
Once you have completed filling in Menu 13 - Default Dial-in Setup, press [Enter] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] at any time to cancel.		



### 8.3.1 Default Dial-in Filter

Move cursor to the field **Edit Filter Sets** in **Menu 13**, press space bar to toggle and set the value to **Yes** and then press [Enter] to open **Menu 13.1 – Default Dial-in Filter**.

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

Spaces are accepted in this field. For more information on defining the filters, *see Chapter 9*.

```
Menu 13.1 - Default Dial-in Filter

Input Filter Sets:
  protocol filters=
  - . - -
```

**Figure 8-4 Default Dial-in Filter**

## 8.4 Dial-In Users Setup

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

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

```
Menu 14 - Dial-in User Setup

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

Enter Menu Selection Number:
```

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

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

```
Menu 14.1 - Edit Dial-in User

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

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

**Figure 8-6 Edit Dial-in User**

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

**Table 8-3 Edit Dial-in User Menu Fields**

Field	Description	Option
User Name	This is a required field. This will be used as the login name for authentication. Choose a descriptive word for login, for example, [JohnDoe].	
Active	You can disallow dial-in access to this user by setting this field to <b>No</b> . Inactive users are displayed with a [-] (minus sign) at the beginning of the name in Menu 14.	<b>Yes/No</b>
Password	Enter the password for the remote dial-in user.	
Callback	This field determines if your Prestige will allow call back to this user upon dial-in. If this option is enabled, your Prestige will call back to the user if requested. In such a case, your Prestige will disconnect the initial call from this user and dial back to the specified callback number (see below). <ul style="list-style-type: none"> <li>● <b>No</b> - The default is no callback.</li> <li>● <b>Optional</b> - The user can choose to disable callback.</li> <li>● <b>Mandatory</b> - The user can not disable callback.</li> </ul>	Default= <b>No</b>  <b>No</b> <b>Optional</b> <b>Mandatory</b>
Phone # Supplied by Caller	This option allows the user to specify the call back telephone number on a call-by-call basis. This is useful when your Prestige returns a call back to a mobile user at different numbers, e.g., a sales rep. in a hotel. <ul style="list-style-type: none"> <li>● If the setting is <b>Yes</b>, the user can specify and send to the Prestige the callback number of his/her choice.</li> <li>● The default is <b>No</b>, i.e., your Prestige always calls back to the fixed callback number.</li> </ul>	Default= <b>No</b>  <b>Yes</b> <b>No</b>
Callback Phone #	If <b>Phone # Supplied by Caller</b> is <b>No</b> , then this is a required field. Otherwise, a <b>N/A</b> will appear in the field. Enter the telephone number to which your Prestige will call back.	
Rem CLID	If you enable CLID Authen field in Menu 13, then you need to specify the telephone number from which this user calls. Your Prestige will check the CLID in the incoming call against the CLIDs in the database. If they do not match and CLID Authen is Required, your Prestige will not answer the call.	

<p>Idle Time-out</p>	<p>Enter the idle time (in seconds). This time-out determines how long the dial-in user can be idle before your Prestige disconnects the call when the Prestige is calling back.</p> <p>Idle time is defined as the period of time where there is no data traffic between the dial-in user and your Prestige. The default is 300 seconds (5 minutes).</p>	<p>Default=300 seconds</p>
<p>Once you have completed filling in <b>Menu 14.1 - Edit Dial-in User</b>, press [Enter] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] at any time to cancel.</p>		

### 8.4.1 Remote Access under Windows

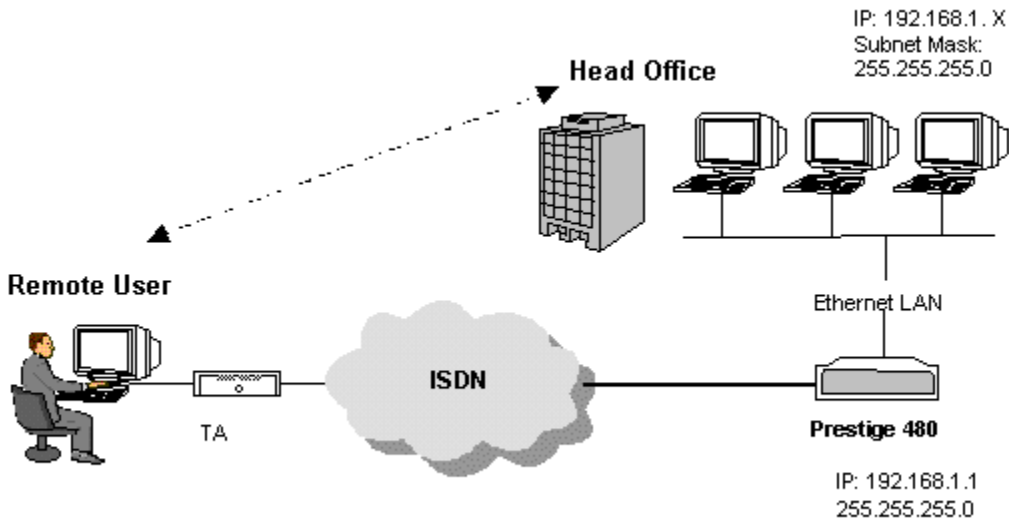


Figure 8-7 Remote Access Example

## Configuring your Prestige

```
Menu 13 - Default Dial-in Setup

Telco Options:
  CLID Authen= None
IP Address Supplied By:
  Dial-in User= Yes
  IP Pool= Yes
  IP Start Addr= 192.168.250.250
  IP Count(1,4)= 2
PPP Options:
  Recv Authen= PAP
  Compression= Yes
  Mutual Authen= No
  PAP Login= N/A
  PAP Password= N/A
Multiple Link Options:
  Max Trans Rate= 256
Session Options:
  Edit Filter Sets= No
Callback Budget Management:
  Allocated Budget(min)=
  Period(hr)=

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

IP Pool for RAS Clients

This must be PAP for Windows

Figure 8-8 Configuring Menu 13 for Remote Access

```
Menu 14.1 - Edit Dial-in User

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

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

The User name and Password must be the same as in Dial-Up Networking in Windows.

Figure 8-9 Edit Dial-in-User for RAS

**Note:** The caller always controls Idle Timeout, so the Idle Timeout field does not apply when there is callback.

## **8.4.2 CLID Authentication**

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

## **8.4.3 Callback**

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

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

### ***Configuring the Prestige for Callback***

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

#### **LAN 1**

```
Menu 11.1 - Remote Node Profile

Rem Node Name= LAN_2          Edit PPP Options= No
Active= Yes                  Rem IP Addr= 192.168.2.1
Call Direction= Both         Edit IP= No

Incoming:                    Telco Option:
  Rem Login= lan2            Transfer Type= 64K
  Rem Password= *****    Allocated Budget(min)=
  Rem CLID=                 Period(hr)=
  Call Back= No             Carrier Access Code=
Outgoing:                   Nailed-Up Connection= N/A
  My Login= lan1            Toll Period (Sec)= 0
  My Password= *****    Session Options:
  Authen= CHAP/PAP         Edit Filter Sets= No
  Pri Phone #= 1234        Idle Timeout(sec)= 100
  Sec Phone #=

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

Set Call Direction and Call Back to Both and No respectively.

Figure 8-10 LAN 1 LAN-to-LAN Application

LAN 2

```
Menu 11.1 - Remote Node Profile

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

Incoming:                    Telco Option:
  Rem Login= lan1            Transfer Type= 64K
  Rem Password= *****    Allocated Budget(min)=
  Rem CLID=                 Period(hr)=
  Call Back= Yes            Carrier Access Code=
Outgoing:                   Nailed-Up Connection= N/A
  My Login= lan2            Toll Period (Sec)= 0
  My Password= *****    Session Options:
  Authen= CHAP/PAP         Edit Filter Sets= No
  Pri Phone #= 5678        Idle Timeout(sec)= 100
  Sec Phone #=

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

Set Call Direction and Call Back to Both and Yes respectively.

Figure 8-11 LAN2 LAN-to-LAN Application

## Testing Callback with your Connection

Go to Menu 24.4.5 of the Prestige on LAN 1 and enter the numbers that correspond to the menu in the above LAN 1.

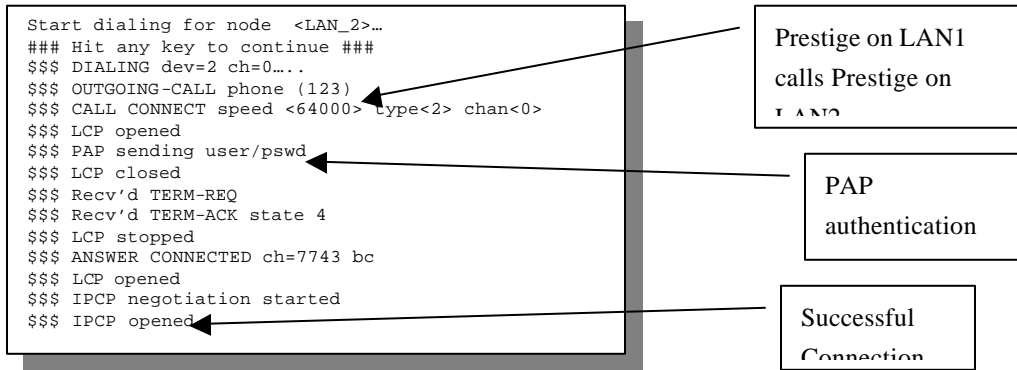


Figure 8-12 Testing Callback with your Connection

## 8.4.4 Configuring the Prestige for Callback with CLID

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

### Prestige on LAN 2



```
Menu 11.1 - Remote Node Profile

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

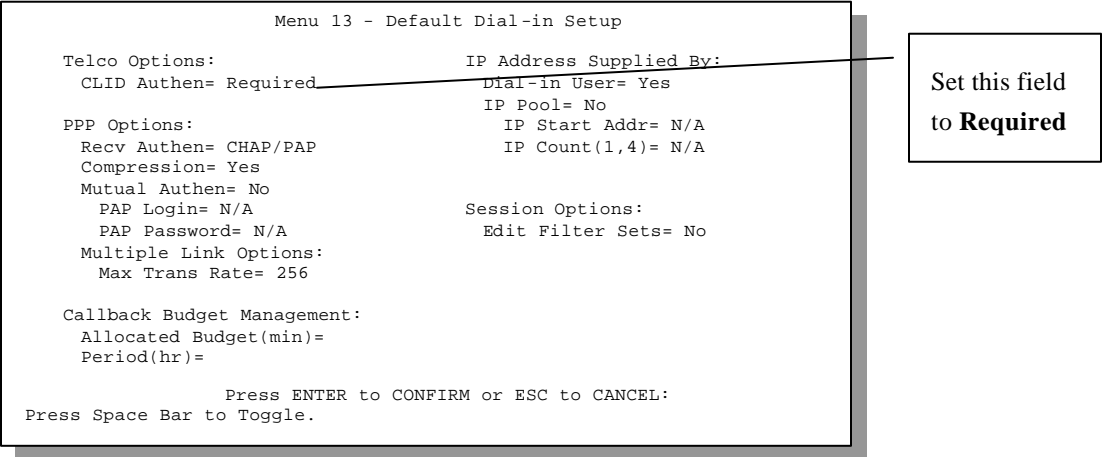
Incoming:                      Telco Option:
  Rem Login= lan1              Transfer Type= 64K
  Rem Password= *****      Allocated Budget(min)=
  Rem CLID= 1234              Period(hr)=
  Call Back= Yes              Carrier Access Code=
Outgoing:                      Nailed-Up Connection= N/A
  My Login= lan2              Toll Period (Sec)= 0
  My Password= *****      Session Options:
  Authen= CHAP/PAP           Edit Filter Sets= No
  Pri Phone #= 5678          Idle Timeout(sec)= 100
  Sec Phone #=

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

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

**Figure 8-13 Callback with CLID Configuration**

## Menu 13



The screenshot shows the configuration menu for the Prestige 480 Dual BRI ISDN Router. The title is "Menu 13 - Default Dial-in Setup". The menu is divided into several sections: Telco Options, PPP Options, Multiple Link Options, Callback Budget Management, and Session Options. A callout box on the right side of the screen, with a line pointing to the "CLID Authen= Required" field, contains the text "Set this field to Required".

```
Menu 13 - Default Dial-in Setup

Telco Options:                               IP Address Supplied By:
  CLID Authen= Required                       Dial-In User= Yes
                                              IP Pool= No
                                              IP Start Addr= N/A
                                              IP Count(1,4)= N/A

PPP Options:
  Recv Authen= CHAP/PAP                       Session Options:
  Compression= Yes                             Edit Filter Sets= No
  Mutual Authen= No
  PAP Login= N/A
  PAP Password= N/A

Multiple Link Options:
  Max Trans Rate= 256

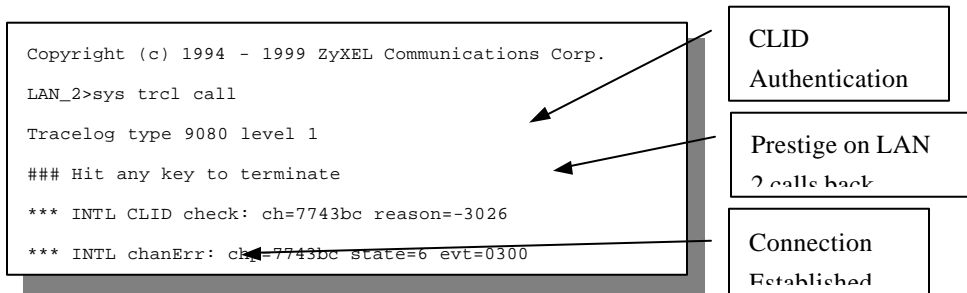
Callback Budget Management:
  Allocated Budget(min)=
  Period(hr)=

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

**Figure 8-14 Configuring CLID with Callback**

### ***Testing your Connection with Callback and CLID***

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



**Figure 8-15 Callback and CLID Connection Test**

## 8.5 Multiple Servers behind SUA

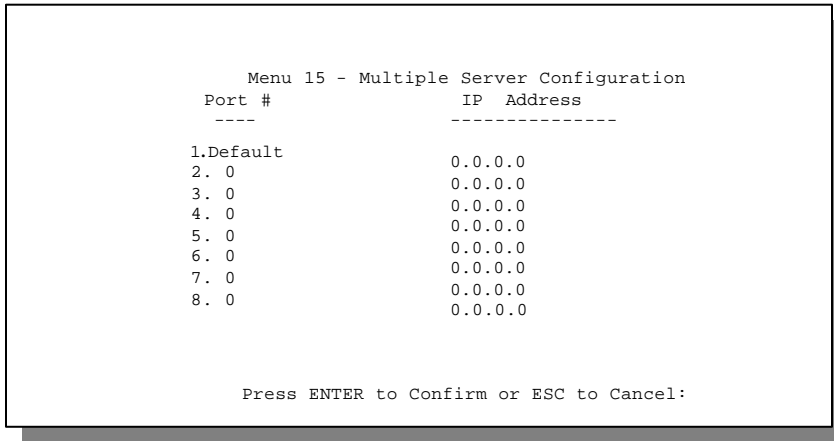
If you wish, you can make inside servers for different services, e.g., web or FTP, visible to the outside users, even though SUA makes your whole inside network appear as a single machine to the outside world. A service is identified by the port number, e.g., web service is on port 80 and FTP on port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

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

Please note that a server can support more than one service, e.g., a server can provide both FTP and DNS service, while another provides only web service. Also, since you need to specify the IP address of a server in the Prestige, a server must have a fixed IP address and not be a DHCP client whose IP address potentially changes each time it is powered on.

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

To make a server visible to the outside world, specify the port number of the service and the inside IP address of the server in **Menu 15, Multiple Server Configuration**. For more information on configuring supporting applications behind SUA refer to the ZyNOS Support Note documentation in your PNC disc.



## 8.5.1 Configuring a Server behind SUA

Follow the steps below to configure a server behind SUA:

1. Enter 15 in the main menu to go to **Menu 15, Multiple Server Configuration**.
2. Enter an index number in menu 15 to go to **Menu 15.1, SUA Server Configuration**.
3. Enter the service port number in the Port # field and the inside IP address of the server in the IP Address field.
4. Press [Enter] at the “Press ENTER to confirm ...” prompt to save your configuration after you define all the servers or press **ESC** at any time to cancel.

**Figure 8-16 Multiple Server Configuration**

The most often used port numbers are:

**Table 8-4 Services vs. Port number**

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



# Chapter 9

## Filter Configuration

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

### 9.1 About Filtering

Your Prestige uses filters to decide whether or not to allow passage of a packet. Data filters are further 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

#### **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.

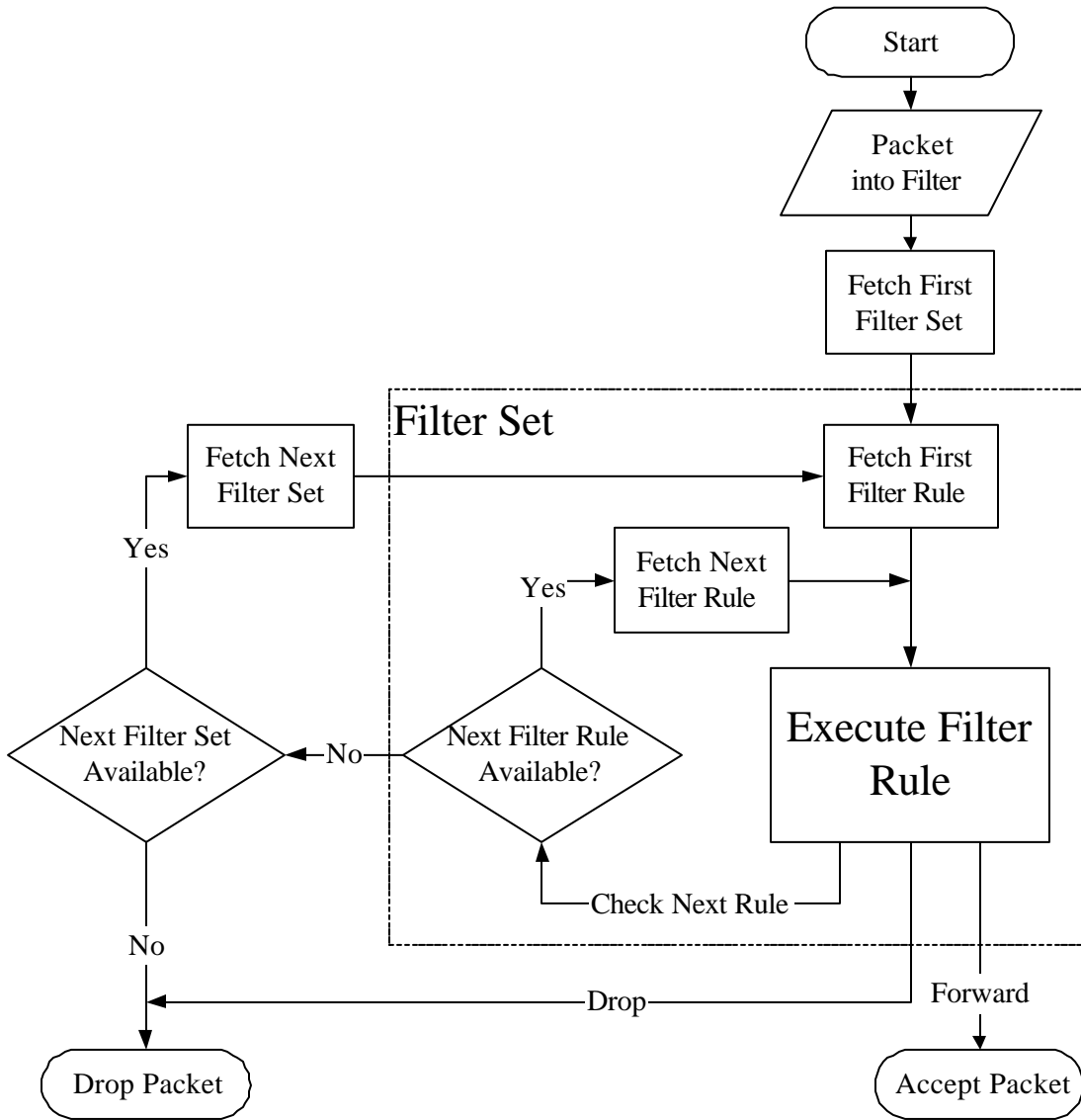


Figure 9-1 Filter Rule Process



## 9.2 Configuring a Filter Set

To configure a filter sets, follow the procedure below:

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

### Figure 9-2 Menu 21 - Filter Set Configuration

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

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

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

```
Menu 21 - Filter Set Configuration

Filter Set #      Comments      Filter Set #      Comments
-----
1                1                7                _____
2                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:
```

```

Menu 21.1 - Filter Rules Summary

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

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

```

**Figure 9-3 Menu 21.1 - Filter Rules Summary**

```

Menu 21.2 - Filter Rules Summary

# A Type                               Filter Rules                               M m n
-----
1 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53   N D F
2 N
3 N
4 N
5 N
6 N

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

```

**Figure 9-4 Menu 21.2 - Filter Rules Summary**

## 9.2.1 Filter Rules Summary Menus

The preceding screens show summaries of the existing rules in the filter set. The following tables contain a brief description of the abbreviations used in Menu 21.1 and Menu 21.2.

**Table 9-1 Abbreviations Used in the Filter Rules Summary Menu**

Abbreviations	Description	Display
#	Refers to the filter rule number (1-6).	
A	Refers to Active.	[Y] means the filter rule is active.

		[N] means the filter rule is inactive.
Type	Refers to the type of filter rule. This shows GEN for Generic and IP for TCP/IP.	[GEN] for Generic. [IP] for TCP/IP.
Filter Rules	The filter rule parameters will be displayed here (see below).	
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 <b>Yes</b>, then <b>Action Matched</b> and <b>Action Not Matched</b> will be <b>N/A</b>.</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.</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.</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 9-2 Abbreviations used if Filter Type is IP**

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

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

**Table 9-3 Abbreviations used if Filter Type is GEN**

Abbreviation	Description
Off	Offset
Len	Length

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

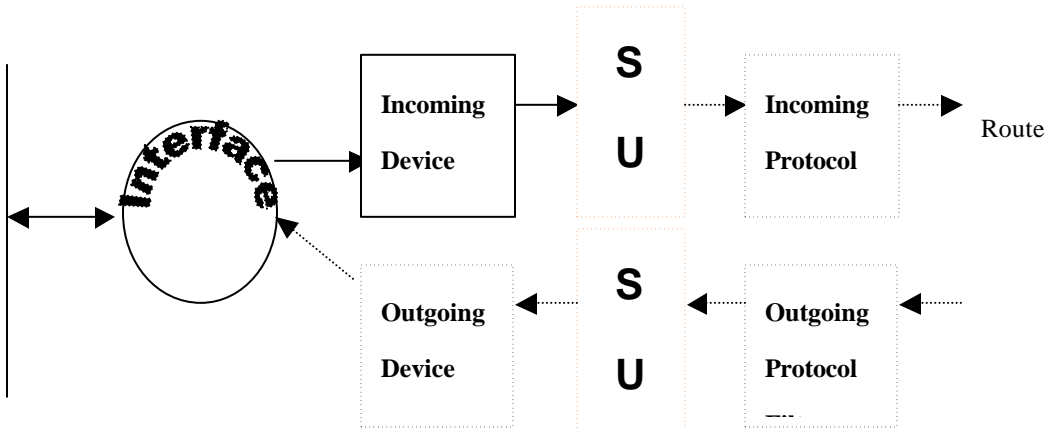
## 9.3 Configuring a Filter Rule

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

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

### 9.3.1 Filter Types and SUA

There are two categories of filter rules, Device Filter (Generic) rules and Protocol Filter (TCP/IP) rules. Device Filter rules act on the raw data from/to LAN and WAN. Protocol Filter rules act on the IP packets. Generic and TCP/IP filter rules are discussed in more detail in the next section. When NAT/SUA (Network Address Translation/Single User Account) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the Prestige applies the **protocol filters** to the “native” IP address and port number before NAT/SUA for outgoing packets and after NAT/SUA for incoming packets. On the other hand, the generic, or device filters are applied to the raw packets that appear on the wire. They are applied at the point when the Prestige is receiving and sending the packets; i.e. the interface. The interface can be Ethernet, or any other hardware port. The following diagram illustrates this.



**Figure 9-5 Protocol and Device Filter Sets**

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

### 9.3.2 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 next.

```
Menu 21.1.1 - TCP/IP Filter Rule

Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
               IP Mask= 0.0.0.0
               Port # = 137
               Port # Comp= Equal
Source: IP Addr= 0.0.0.0
         IP Mask= 0.0.0.0
         Port # = 0
         Port # Comp= None

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

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

**Figure 9-6 Menu 21.1.1 - TCP/IP Filter Rule**

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

**Table 9-4 TCP/IP Filter Rule Menu Fields**

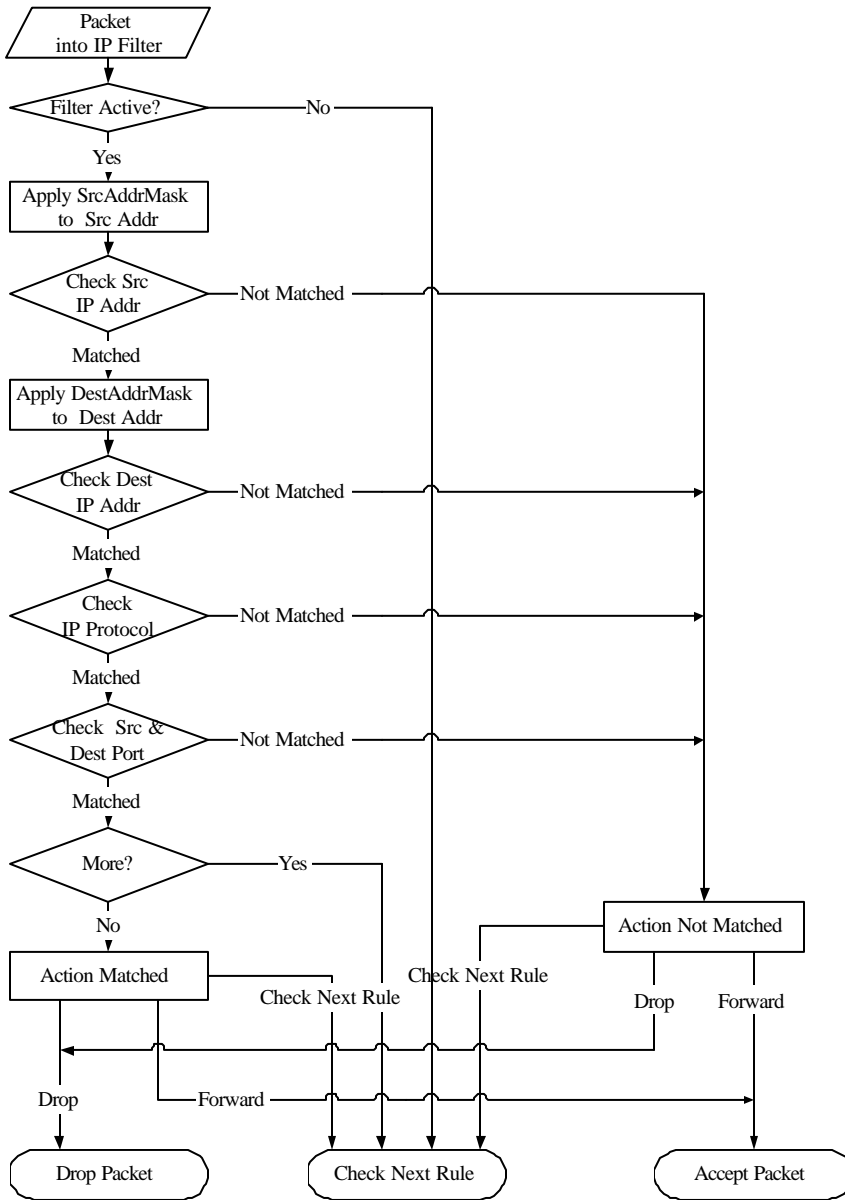
Field	Description	Option
Active	This field activates/deactivates the filter rule.	Yes/No
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. This value must be between 0 and 255	0-255
IP Source Route	If Yes, the rule applies to packet with IP source route option; else the packet must not have source route option.	Yes/No

	The majority of IP packets do not have source route.	
Destination: IP Addr	Enter the destination IP Address of the packet you wish to filter. This field is a don't-care if it is 0.0.0.0.	IP address
Destination: IP Mask	Enter the IP subnet mask to apply to the Destination: IP Addr.	Subnet mask
Destination: Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is a don't-care if it is 0.	0-65535
Destination: Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in Destination: Port #.	<b>None/Less/Greater/Equal/Not Equal]</b>
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 #.	<b>None/Less/Greater/Equal/Not Equal</b>
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.	<b>Yes/No</b>
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 <b>Yes</b> , then Action Matched and Action Not Matched will be <b>No</b> .	<b>Yes / No</b>
Log	Select the logging option from the following: <ul style="list-style-type: none"> <li>● <b>None</b> – No packets will be logged.</li> <li>● <b>Action Matched</b> - Only packets that match the rule parameters will be logged.</li> <li>● <b>Action Not Matched</b> - Only packets that do not match the rule parameters will be logged.</li> <li>● <b>Both</b> – All packets will be logged.</li> </ul>	<b>None Action Matched Action Not Matched Both</b>
Action Matched	Select the action for a matching packet.	<b>Check Next Rule Forward Drop</b>
Action Not Matched	Select the action for a packet not matching the rule.	<b>Check Next Rule Forward</b>

		<b>Drop</b>
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 9-7 Executing a Filter Rule**

### 9.3.3 Generic Filter Rule

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

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

To configure a generic rule, select **Generic Filter Rule** in the Filter Type field **Menu 21.3.1** and press [ENTER] to open Generic Filter Rule Menu, as shown below.

```
Menu 21.3.1 - Generic Filter Rule

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

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

**Figure 9-8 Menu 21.3.1 - Generic Filter Rule**

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

**Table 9-5 Generic 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 rule of that set.	
Filter Type	Use the space bar to toggle between both types of rules. Parameters displayed below each type will be different.	<b>Generic Filter Rule/TCP/IP Filter Rule</b>
Active	Select <b>Yes</b> to turn on the filter rule.	<b>Yes/No</b>
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 <b>Yes</b> , then Action Matched and Action Not Matched will be <b>No</b> .	<b>Yes / No</b>
Log	Select the logging option from the following: <b>None</b> – No packets will be logged. <b>Action Matched</b> - Only packets that match the rule parameters will be logged. <b>Action Not Matched</b> - Only packets that do not match the rule parameters will be logged. <b>Both</b> – All packets will be logged.	<b>None</b> <b>Action Matched</b> <b>Action Not Matched</b> <b>Both</b>
Action Matched	Select the action for a matching packet.	<b>Check Next Rule</b> <b>Forward</b> <b>Drop</b>
Action Not Matched	Select the action for a packet not matching the rule.	<b>Check Next Rule</b> <b>Forward</b> <b>Drop</b>
Once you have completed filling in Menu 21.1.2 - generic Filter Rule, press [Enter] at the message [Press Enter to Confirm] to save your configuration, or press [Esc] to cancel. This data will now be displayed on Menu 21.1 - Filter Rules Summary.		

### 9.3.4 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 rule, select **IPX Filter Rule** from the **Filter Type** field and press [Enter] to open **Menu 21.1.3 IPX Filter Rule**, as shown in the figure below.

```
Menu 21.1.3 - IPX Filter Rule

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

Operation= N/A
More= No           Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

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

**Figure 9-9 Menu 21.1.3 - IPX Filter Rule**

The table below describes the IPX Filter Rule.

**Table 9-6 IPX Filter Rule Menu Fields**

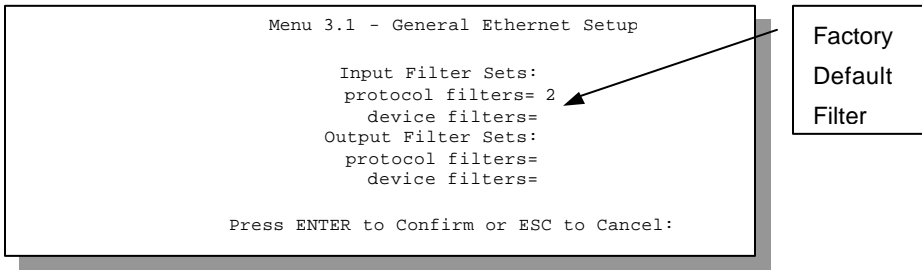
Field	Description
IPX Packet Type	Enter the IPX packet type (1-byte in hexadecimal) you wish to filter.  The popular types are (in hexadecimal): 01 - RIP 04 - SAP 05 - SPX (Sequenced Packet eXchange) 11 - NCP (NetWare Core Protocol) 14 - Novell NetBIOS
Destination/Source Network #	Enter the destination/source network numbers (4-byte in hexadecimal) of the packet that you wish to filter.
Destination/Source Node #	Enter in the destination/source node number (6-byte in hexadecimal) of the packet you wish to filter.
Destination/Source Socket #	Enter the destination/source socket number (2-byte in hexadecimal) of the packets that you wish to filter.
Destination/Source Socket # Comp	Select the comparison you wish to apply to the destination/source socket in the packet against that specified above.
Operation	This field is applicable only if one of the Socket # fields is 0452 or 0453 indicating SAP and RIP packets. There are seven options for this field that specify the type of the packet. <ul style="list-style-type: none"> <li>● None.</li> <li>● RIP Request.</li> <li>● RIP Response.</li> <li>● SAP Request.</li> <li>● SAP Response.</li> <li>● SAP Get Nearest Server Request.</li> <li>● SAP Get Nearest Server Response</li> </ul>
Once you have completed filling in <b>Menu 21.1.3 - IPX Filter Rule</b> , 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 <b>Menu 21.1 - Filter Rules Summary</b> .	

## 9.4 Applying Filters and Factory Defaults

This section shows you where to apply the filter(s) after you design it (them). Two sets of factory default filter rules have been configured in Menu 21 to prevent NetBIOS traffic from triggering calls (see Figure 8-7 **Menu 21 - Filter Set Configuration**).

### 9.4.1 Ethernet traffic

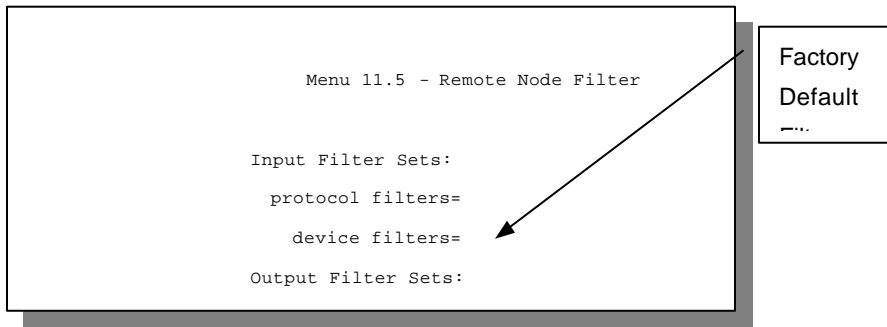
You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reducing traffic and preventing security breaches. Go to Menu 3.1 (shown below) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter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



**Figure 9-10 Filtering Ethernet traffic**

### 9.4.2 Remote Node Filters

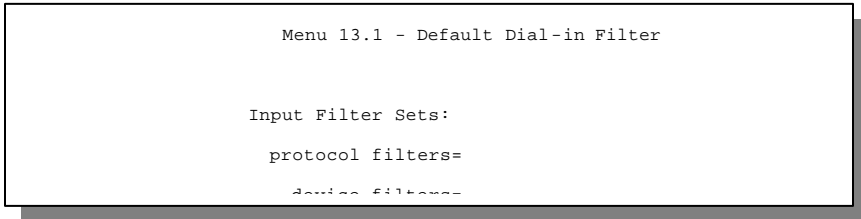
Go to Menu 11.5 (shown below) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas. The factory default filter set, NetBIOS\_WAN, is inserted in **protocol filters** field under **Call Filter Sets** in Menu 11.5 to block local NetBIOS traffic from triggering calls to the ISP.



**Figure 9-11 Filtering Remote Node traffic**

### 9.4.3 Default Dial-in Filter

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



**Figure 9-12 Default Dial-in Filter**





# Chapter 10

## SNMP Configuration

*This chapter explains how to configure SNMP.*

### 10.1 About SNMP

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

### 10.2 Configuring SNMP

To configure SNMP, select option **SNMP Configuration** from the Main Menu to open Menu 22 SNMP Configuration, as shown in the next figure. 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 10-1 Menu 22 - SNMP Configuration**

The following table describes the SNMP configuration parameters.

**Table 10-1 SNMP Configuration Menu Fields**

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



# Chapter 11

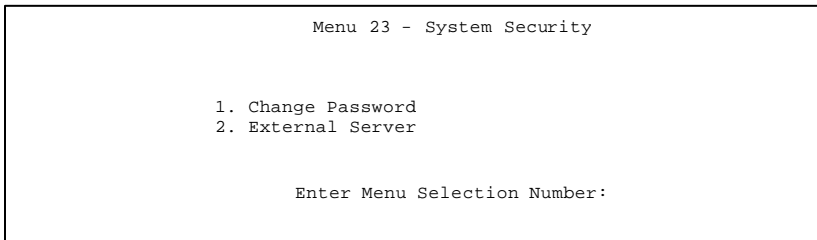
## System Security

*This chapter helps you to change the system password and to configure an external authentication server.*

### 11.1 Changing the System Password

To change the system password, follow the steps shown next:

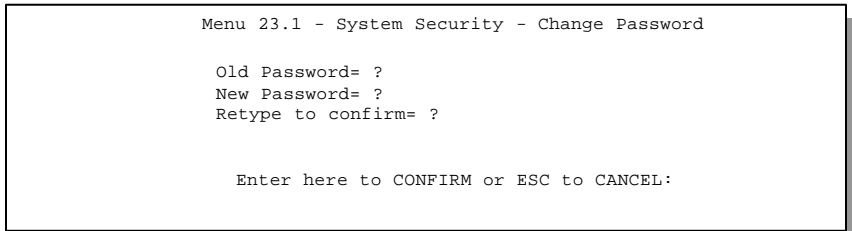
- Step 1.** Select option **System Security** in the Main Menu to open **Menu 23 – System Security** as shown next.



**Figure 11-1 Menu 23 - System Security**

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

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



**Figure 11-2 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 a (X) for each character you type.

## 11.2 Using RADIUS Authentication

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

### 11.2.1 Installing a RADIUS Server

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

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

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

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

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

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

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



## 11.2.2 RADIUS Server Configuration

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

```
Menu 23.2 - System Security - External Server

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

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

**Figure 11-3 Menu 23.2 - System Security - External Server**

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

**Table 11-1 System Security - External Server Menu Fields**

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

### 11.2.3 The Key Field

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

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

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

### 11.2.4 Adding Users to the RADIUS Database

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

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

## 11.2.5 Using RADIUS Authentication for CLID

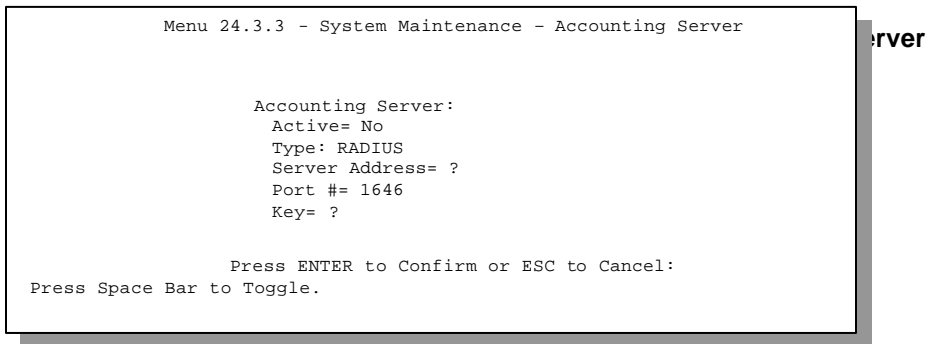
To use RADIUS for CLID authentication, create a user record in the `users` file where the user name (the first field) is the telephone number, and the password (the second field) is always `Zyxel-CLID` (case-sensitive). The regular user name is put in a `User-Name` field. The following is an example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

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

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

## 11.3 RADIUS Accounting

RADIUS accounting logs information about dial-in connections. The RADIUS accounting server may be located on the same host as the RADIUS authentication server, or on a separate host. RADIUS accounting can be configured in **Menu 24.3.3 – System Maintenance – Accounting Server** as shown next.



The fields in Menu 24.3.3 are listed in the following table.

**Table 11-2 System Maintenance – Accounting Server Fields**

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

Once the accounting server is enabled and the RADIUS external server authenticates users, the Prestige sends messages to the external server. Some examples are shown next.

```
Fri Aug 13 11:22:03 1999
    Acct-Status-Type = Start
    Acct-Session-Id = "23850000000002"
    User-Name = "ras"
    NAS-Port = 131072
    NAS-Port-DNIS = "5553100"
    Caller-Id = "5552100"
```

**Figure 11-5 Examples of RADIUS Accounting Message**

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

**Note:** Accounting attributes may vary depending on the external server.

**Table 11-3 Accounting Attributes**

<b>Field</b>	<b>Description</b>
Acct-Status-Type	Account Status Type has four values: Accounting On, Accounting Off, Start and Stop. An Accounting On record is created when the Prestige starts the RADIUS Accounting service. An Accounting Off record is created when the Prestige ends the service. A Start record is created when a user session begins. A Stop record is recorded when the session ends.
Acct-Session-Id	Account Session Id is a unique number assigned to each Start and Stop record to make it easy to match the Start and Stop records in a detail file, and to eliminate duplicate records. Note that in the above example this value matches in the Start and Stop record, indicating that these records correspond to the same session.
User-Name	Specifies the user name.
NAS-Port	Refers to the Network Access Server (NAS) port used in the connection.
NAS-Port-DNIS	Refers to the called party's directory number.
Caller Id	Refers to the dial-in-user's Caller ID.



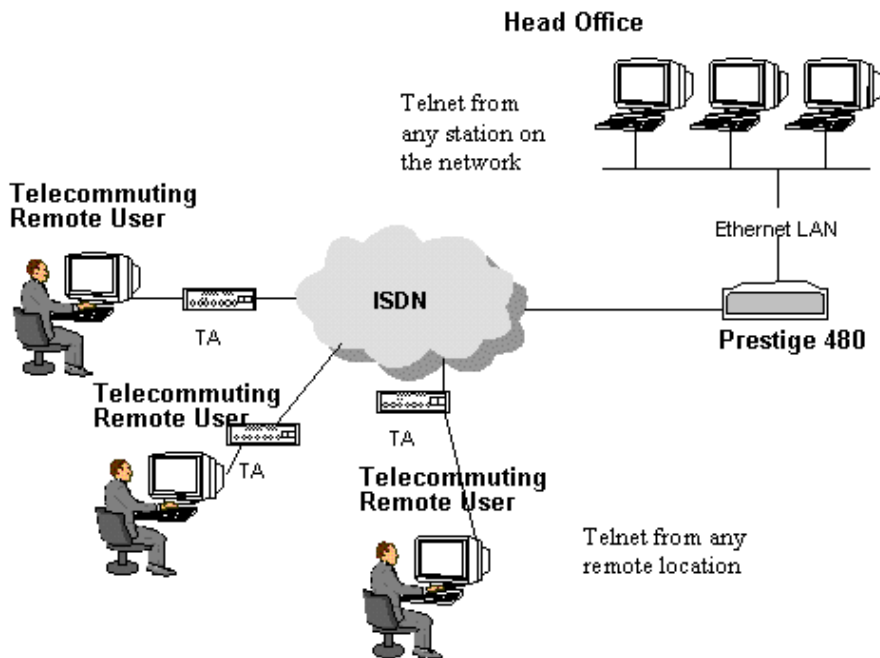
# Chapter 12

## Telnet Configuration and Capabilities

*This chapter discusses using telnet to remotely configure your Prestige.*

### 12.1 About Telnet Configuration

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



**Figure 12-1 Telnet Configuration on a TCP/IP Network**

## **12.2 Telnet Under SUA**

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

## **12.3 Telnet Capabilities**

### **12.3.1 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.

### **12.3.2 System Timeout**

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



# Chapter 13

## 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 next.

```
Menu 24 - System Maintenance

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

Enter Menu Selection Number:
```

**Figure 13-1 Menu 24 - System Maintenance**

## 13.1 System Status

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

To get to the System Status, select number **24** to go to **Menu 24 - System Maintenance**. From this menu, select number **1, System Status**. There are eight commands in **Menu 24.1 - System Maintenance - Status**. Entering **1** disconnects the B1 channel call of ISDN line 1; **2** disconnects the B2 channel call of ISDN line 1; **3** disconnects the B1 channel call of ISDN line 2; **4** disconnects the B2 channel call of ISDN

```
Menu 24.1 - System Maintenance - Status                                09:59:41
                                                                    Thu. JAN. 11, 2001

ISDN  Chan   Status   Speed   TxPkts  RxPkts  Errors  CLU    ALU    Up Time
--   --     --      --      --      --      --      --     --     --
--   --     Down    0Kbps   0        0        0        0%    0%    0:00:00
--   --     Down    0Kpbs   0        0        0        0%    0%    0:00:00
--   --     Down    0Kbps   0        0        0        0%    0%    0.00.00
--   --     Down    0Kbps   0        0        0        0%    0%    0.00.00

Ethernet:      Status           TxPkts           RxPkts           Collisions
              Down                0                 0                 0
LAN Packet Which Triggered Last Call:

Total Outcall Time:      0:00:00      CPU Load = 3.62%

Press Command:
COMMANDS: 1-Drop ISDN_1 B1 2-Drop ISDN_1 B2 3-Drop ISDN_2 B1 4-Drop ISDN_2 B2
          5-Reset Counters 6-Drop All      9-Toggle Status  ESC-Exit
```

line 2; **5** resets the counters, **6** drops both B1 and B2 channels of both ISDN lines; **9** toggles the status and **ESC** takes you back to the previous screen.

**Figure 13-2 Menu 24.1 - System Maintenance – Status**

If you enter **9** in the **Press Command** field you will see the following menu:

```

Menu 24.1 - System Maintenance - Status                                09:59:41
                                                                    Fri. May. 28, 1999

ISDN  Chan  Status  Speed  TxPkts  RxPkts  Errors  CLU  ALU  Up Time
--  --  --  --  --  --  --  --  --  --
--  --  Down  0kbps  0       0       0       0%  0%  0:00:00
--  --  Down  0kbps  0       0       0       0%  0%  0:00:00
--  --  Down  0kbps  0       0       0       0%  0%  0:00:00
--  --  Down  0kbps  0       0       0       0%  0%  0:00:00

ISDN  Chan  Own IP  Own CLID  Peer IP  Peer CLID
--  --  --  --  --  --
--  --  --  --  --  --
--  --  --  --  --  --
--  --  --  --  --  --

Total Outcall Time:      0:00:00      CPU Load = 7.92%

Press Command:
COMMANDS: 1-Drop ISDN_1 B1 2-Drop ISDN_1 B2 3-Drop ISDN_2 B1 4-Drop ISDN_2 B2
          5-Reset Counters 6-Drop All      9-Toggle Status  ESC-Exit
    
```

**Figure 13-3 Menu 24.1 after Toggle Status**

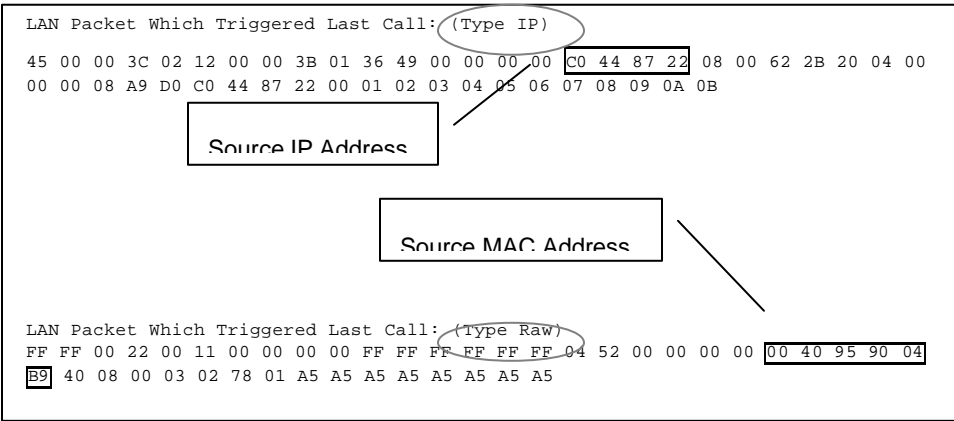
The following table describes the fields present in **Menu 24.1 - System Maintenance - Status**. It should be noted that these fields are READ-ONLY and are meant to be used for diagnostic purposes.

**Table 13-1 System Maintenance - Status Menu Fields**

Field	Description
ISDN	Shows which ISDN line(s) is in use.
Chan	Shows statistics for <b>B1</b> and <b>B2</b> channels respectively. This is the information displayed for each channel:
Status	Shows the status of the ISDN Channel.  <b>LCP UP</b> indicates that PPP negotiation is taking place. If the negotiation is successful the ISDN Channel is connected to a <b>Remote Node</b> , otherwise the connection is <b>Down</b> . <b>Idle</b> , <b>Dial</b> and <b>Answering</b> refer to the status of the ISDN channel.

Speed	Shows the current connecting speed.
TxPkts	Shows the number of transmitted packets on this channel.
RxPkts	Shows the number of received packets on this channel.
Errors	Shows the number of error packets on this channel.
CLU	(Current Line Utilization) percentage of current bandwidth used on this channel
ALU	(Average Line Utilization) a 5-second moving average of channel usage for this channel.
Up Time	Shows the time this channel has been connected to the current remote node
Ethernet	(Ethernet connection).
Status	Shows the current transmission speed and mode of the LAN.
TxPkts	Shows the number of transmitted packets to the LAN.
RxPkts	Shows the number of received packets from the LAN.
Collisions	Shows the number of collisions.
LAN Packet Which Triggered Last Call	Shows the first 48 octets of the LAN packet that triggered the last outgoing call.
Total Outcall Time	Shows the total outgoing call time for both <b>B1</b> and <b>B2</b> channels since the system has been powered up.
CPU Load	Specifies the percentage of CPU utilization.
Press Command: COMMANDS	
1	Drops the B1 channel of ISDN line 1.
2	Drops the B2 channel of ISDN line 1.
3	Drops the B1 channel of ISDN line 2.
4	Drops the B2 channel of ISDN line 2.
5	Resets counters means that all statistics, except <b>Uptime</b> are reset to zero.
6	Drop All means all ISDN line channels are dropped.
9	Toggles status means you can see alternative information such as the Prestige IP address and CLID as well as the peer's IP address and CLID (see next figure).
ESC	Exits this menu and takes you back to the previous menu.

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



**Figure 13-4 LAN Packet That Triggered Last Call**

### 13.1.1 System Information

```
Menu 24.2.1 - System Maintenance - Information

Name:
Routing: IP
ZyNOS S/W Version: V2.40(0.00)b02 | 7/13/1999
Country Code: 255

LAN

Ethernet Address:00:a0:c5:ff:00:35
IP Address: 192.168.1.1
IP Mask: 255.255.255.0
DHCP: Server

Press ESC or RETURN to Exit:
```

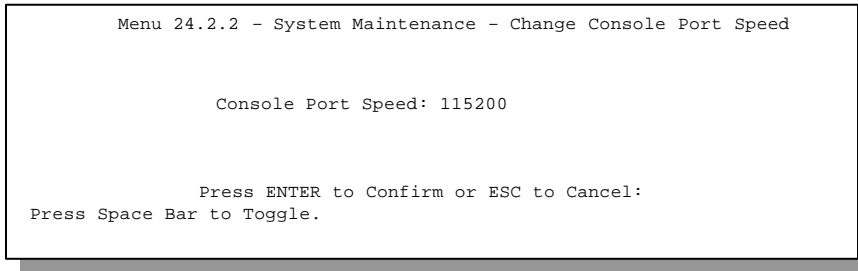
**Figure 13-5 System Maintenance - Information**

**Table 13-2 Fields in System Maintenance**

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

### 13.1.2 Console Port Speed

You can change the console port speed through **Menu 24.2.2 – Console Port Speed**. Your Prestige supports 9600 , 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 next.



**Figure 13-6 Menu 24.2.2 – System Maintenance – Change Console Port Speed**

## 13.2 Log and Trace

There are three 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. The third is RADIUS Accounting which is stored in an external server. For more information on RADIUS Accounting please refer to the chapter *System Security*.

### 13.2.1 Viewing Error Log

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

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

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



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

```
43 947822680 PP11 INFO LAN promiscuous mode <0>
44 947822680 PINI INFO main: init completed
45 947822703 PINI INFO SMT Session Begin
46 947822964 PINI INFO SMT Session End
47 947822970 PINI INFO SMT Session Begin
48 947824146 PINI INFO SMT Session End
49 947824405 PINI INFO SMT Session Begin
50 947824724 PINI INFO SMT Session End
51 947825491 PINI INFO SMT Session Begin
52 947826152 PINI INFO SMT Session End
53 947826224 PINI INFO SMT Session Begin
54 947826537 PINI INFO SMT Session End
55 947826798 PINI INFO SMT Session Begin
56 947827332 PINI INFO SMT Session End
57 947828939 PINI INFO SMT Session Begin
58 947829255 PINI INFO SMT Session End
59 947829921 PINI INFO SMT Session Begin

Clear Error Log (y/n):
```

**Figure 13-7 Examples of Error and Information Messages**

## 13.2.2 Syslog And Accounting

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

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

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

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

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

**Figure 13-8 Menu 24.3.2 - System Maintenance – UNIX Syslog and Accounting**

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

**Table 13-3 System Maintenance Menu - UNIX 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.
Types:	
CDR	Call Detail Record (CDR) logs all data phone line activity if set to <b>Yes</b> .
Packet triggered	The first 48 bytes or octets and protocol type of the triggering packet is sent to the UNIX syslog server when this field is set to <b>Yes</b> .
Filter log	No filters are logged when this field is set to <b>No</b> . Filters with the individual filter <b>Log Filter</b> field set to <b>Yes</b> are logged when this field is set to <b>Yes</b> .
PPP log	PPP events are logged when this field is set to <b>Yes</b> .

Your Prestige sends four types of syslog messages. Please see Enhanced Syslog in the Appendix for the message format. Some examples of these syslog messages are shown next:

## 1. CDR

```
Jul 19 11:19:27 192.168.102.2 ZyXEL Communications Corp.: board 0 line 0 channel 0, call 1,
C01 Outgoing Call dev=2 ch=0 40002
```

```
Jul 19 11:19:32 192.168.102.2 ZyXEL Communications Corp.: board 0 line 0 channel 0, call 1,
C02 OutCall Connected 64000 40002
```

```
Jul 19 11:20:06 192.168.102.2 ZyXEL Communications Corp.: board 0 line 0 channel 0, call 1,
C02 Call Terminated
```

## **2. Packet triggered**

Jul 19 11:28:39 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1, Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f7071727374

Jul 19 11:28:56 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1, Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4

Jul 19 11:29:06 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1, Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000

## **3. Filter log**

Jul 19 14:43:55 192.168.102.2 ZyXEL Communications Corp.: IP[Src=202.132.154.123 Dst=255.255.255.255 UDP spo=0208 dpo=0208]}S03>R01mF

Jul 19 14:44:00 192.168.102.2 ZyXEL Communications Corp.: IP[Src=192.168.102.20 Dst=202.132.154.1 UDP spo=05d4 dpo=0035]}S03>R01mF

Jul 19 14:44:04 192.168.102.2 ZyXEL Communications Corp.: IP[Src=192.168.102.20 Dst=202.132.154.1 UDP spo=05d4 dpo=0035]}S03>R01mF

## **4. PPP log**

Jul 19 11:42:44 192.168.102.2 ZyXEL Communications Corp.: ppp:LCP Closing

Jul 19 11:42:49 192.168.102.2 ZyXEL Communications Corp.: ppp:IPCP Closing

Jul 19 11:42:54 192.168.102.2 ZyXEL Communications Corp.: ppp:CCP Closing

## 13.3 Diagnostic

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

```
Menu 24.4 - System Maintenance - Diagnostic

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

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

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

as shown next.

**Figure 13-9 Menu 24.4 - System Maintenance - Diagnostic**

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

- Step 1.** From the Main Menu, select option 24 to open **Menu 24 - System Maintenance**.
- Step 2.** From this menu, select option 4. Diagnostic. This 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 13-4 System Maintenance Menu Diagnostic**

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

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

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

**Figure 13-10 Trace Display for a Successful Manual Call**

This figure shows a trace example where authentication failed.

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

**Figure 13-11 Trace Display for a Failed Authentication**

## 13.4 Boot Module Command

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

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
ATRWx	display the 16-bit value of address x
ATRLx	display the 32-bit value of address x
ATGO(x)	run program at addr x or boot router
ATGR	boot router
ATGT	run Hardware Test Program
ATRTw,x,y(,z)	RAM test level w, from address x to y (z iterations)
ATSH	dump manufacturer related data in ROM
ATDOx,y	download from address x for length y to PC via XMODEM
ATTD	download router configuration to PC via XMODEM
ATUR	upload router firmware to flash ROM
ATUR3	upload router configuration file to router
ATXSx	xmodem select: x=0: CRC mode(default); x=1: checksum mode

**Figure 13-12 Boot Module Commands**



## 13.5 Command Interpreter Mode

This option allows you to enter the command interpreter mode(CI). A list of valid commands can be found by typing [help] at the command prompt. For more detailed information, check your PNC installation disc or

```
Enter Menu Selection Number: 8

Copyright (c) 1994 - 1999 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys          exit          ether          isdn
ip
```

visit the ZyXEL Web site or send e-mail to the ZyXEL Support Group.

**Figure 13-13 Command Mode**

## 13.6 Call Control

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

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

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

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

phone number is put in the blacklist. You will have to enable the number manually before the Prestige will dial that number again.

Call history chronicles preceding incoming and outgoing calls.

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

```
Menu 24.9 - System Maintenance - Call Control

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

Enter Menu Selection Number:
```

**Figure 13-14 Menu 24.9 - System Maintenance - Call Control**

### **13.6.1 Call Control Parameters**

```
Menu 24.9.1 - Call Control Parameters

Dialer Timeout:
Digital Call(sec)= 60

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

**Figure 13-15 Call Control Parameters**

**Table 13-5 Call Control Parameters Fields**

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

## 13.6.2 Blacklist

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

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

```
Menu 24.9.2 - Blacklist

Phone Number
1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.

Remove Selection(1-14):
```

**Figure 13-16 Menu 24.9.2 - Blacklist**

### 13.6.3 Budget Management

**Menu 24.9.3 Budget Management** shows the budget management statistics for outgoing calls.

```
Menu 24.9.3 - Budget Management

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

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

**Figure 13-17 Menu 24.9.3 - Budget Management**

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

### 13.6.4 Call History

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

```
Menu 24.9.4 - Call History

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

Enter Entry to Delete(0 to exit):
```

**Figure 13-18 Call History**

**Table 13-6 Call History Fields**

Field	Description
Phone Number	This is the telephone number of past incoming and outgoing calls.
Dir	This shows whether the call was incoming or outgoing.
Rate	This is the transfer rate of the call.
#call	This is the number of calls made to or received from that telephone number.
Max	This is the length of time of the longest telephone call.
Min	This is the length of time of the shortest telephone call.
Total	This is the total length of time of all the telephone calls to/from that telephone number.

## 13.7 Time and Date Setting

**Menu 24.10** allows you to update the time and date settings of your Prestige 480.

```
Menu 24.10 - System Maintenance - Time and Date Setting

Current Time:                02 : 31 : 31
New Time (hh:mm:ss):        2  : 31 : 31

Current Date:                01 / 17 / 2001
New Date (mm-dd-yyyy):      1  / 17 / 2001

Daylight Savings= Disable

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

**Figure 13-19 System Maintenance – Time and Date Setting**

**Table 13-7 Time and Date Setting Fields**

Field	Description
New Time	Enter the new time in hour, minute and second format.
New Date	Enter the new date in month, date and year format.
Daylight Savings	Enable <b>Daylight Savings</b> if daylight savings is in effect in your country.
Once you have filled in the new time and date , press <b>[Enter]</b> to save the setting and press <b>[Esc]</b> to return to <b>Menu 24</b> .	







# Chapter 14

## Backup, Restore and Upload

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

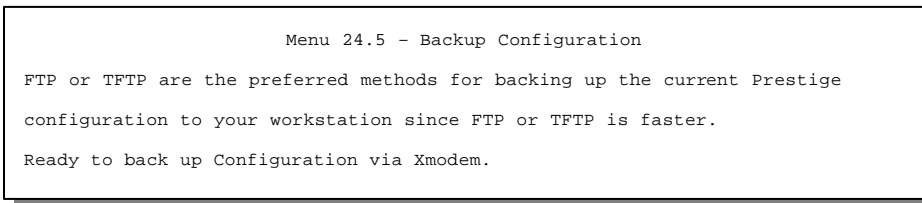
Please note that terms “download” and “upload” are relative to the workstation. Download means to transfer from another machine to the workstation, while upload means from your workstation to another machine.

### 14.1 Backup Configuration

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

#### 14.1.1 Backup using the Console Port

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.

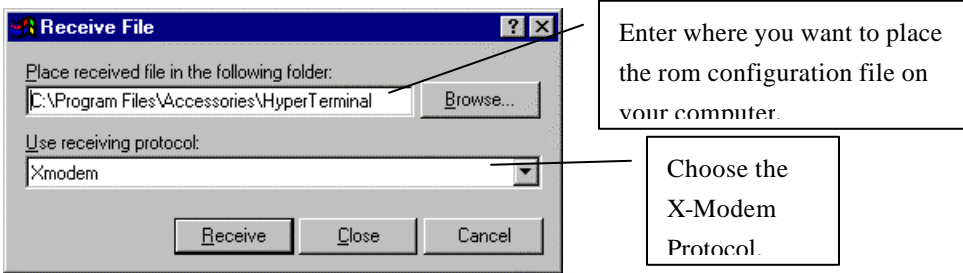
A screenshot of a terminal window showing the text for Menu 24.5. The text is centered and reads: "Menu 24.5 - Backup Configuration", "FTP or TFTP are the preferred methods for backing up the current Prestige configuration to your workstation since FTP or TFTP is faster.", and "Ready to back up Configuration via Xmodem." The text is displayed in a monospaced font within a rectangular box that has a thin border and a slight drop shadow.

```
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.
```

**Figure 14-1 Menu 24.5 –Backup Configuration using the Console Port**

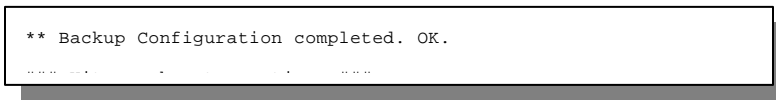
**Step 1.** Go to Menu 24.5.

- Step 2.** Press “Y” to indicate that you want to continue. The following procedure is for the HyperTerminal program. The procedure for other serial communications programs should be similar.
- Step 3.** Click “Transfer” in the HyperTerminal toolbar, then “Receive File” in the popup menu to display the following screen.



**Figure 14-2 Receive File**

- Step 4.** Enter where you want to place the rom configuration file on your computer, give it a suitable name, e.g.p1600.rom, and make sure you choose the X-Modem Protocol. Then press “Receive”.
- Step 5.** After a successful backup you will see the following screen. Press any key to return to the SMT menu



**Figure 14-3 Successful Backup**

### 14.1.2 Back up using FTP

To transfer the firmware and 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.

### **14.1.3 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:

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

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

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

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

**Step 5.** Go to SMT menu 24.5. Note that you must remain in this menu until backup is complete.

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

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands, 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.

### Example Using Walusoft TFTP Client

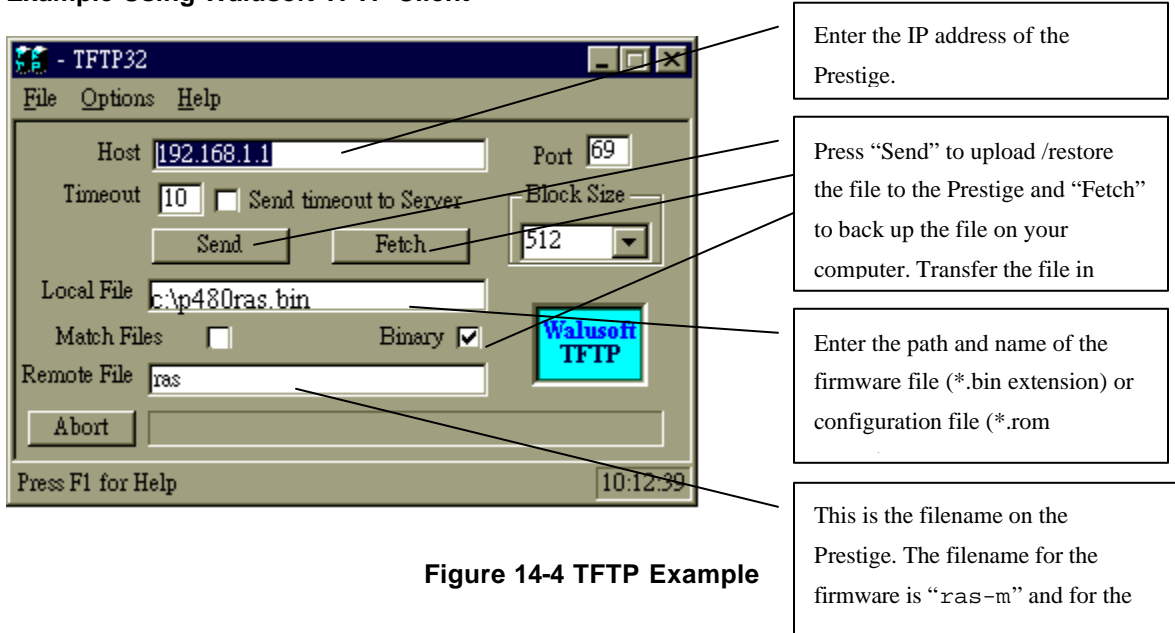


Figure 14-4 TFTP Example

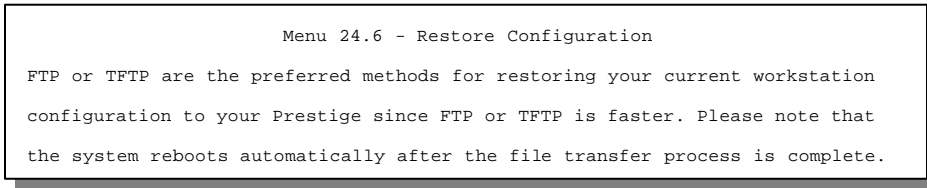
## 14.2 Restore Configuration

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

### 14.2.1 Restore using the Console Port

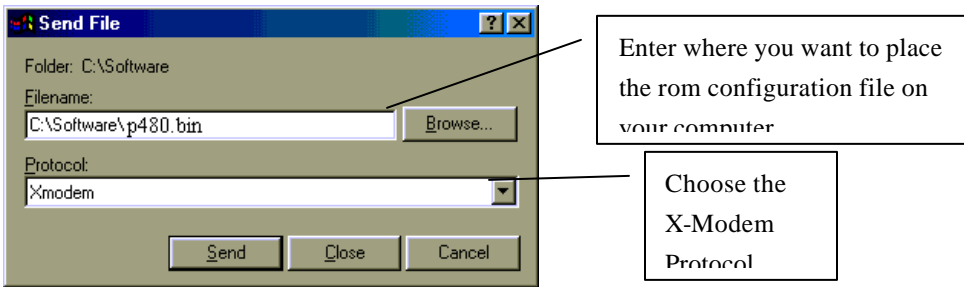
You can restore the configuration either through an FTP or TFTP client program (preferred method) or through the RS-232 console port (in the event of the network being down). Restoring via the console port under normal conditions is not recommended since FTP or TFTP is faster.

Please note that the system reboots automatically after the file transfer process is complete.



**Figure 14-5 Menu 24.6 –Restore Configuration using the Console Port**

- Step 1.** Go to Menu 24.6 .
- Step 2.** Press “Y” to indicate that you want to continue. The following procedure is for the HyperTerminal program. The procedure for other serial communications programs should be similar.
- Step 3.** Click “Transfer” in the HyperTerminal toolbar, then “Send File” in the popup menu to display the following screen.



**Figure 14-6 Send File**

- Step 4.** Enter where the rom configuration file is on your computer, and make sure you choose the X-Modem Protocol. Then press “Send”.
- Step 5.** After a successful restoration you will see the following screen. Press any key to return to reboot the system.

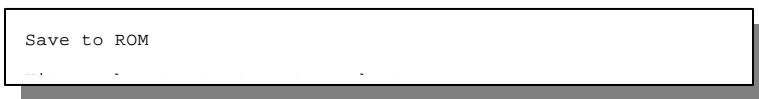


Figure 14-7 Successful Restoration

## 14.2.2 Restore using FTP

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

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.

## 14.2.3 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 firmware and the configuration file, follow the procedure below.

- Step 1.** Use telnet from your workstation to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.
- Step 2.** Put the SMT in Command Interpreter (CI) mode by entering **8** in **Menu 24 – System Maintenance**.
- Step 3.** Enter command “`sys stdio 0`” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “`sys stdio 5`” to restore the five-minute SMT timeout (default) when the file transfer is complete.
- Step 4.** Launch the TFTP client on your workstation and connect to the Prestige.

- Step 5.** Go to SMT menu 24.6. Note that you must remain in this menu until file transfer is complete.
- Step 6.** Use the TFTP client to transfer files between the Prestige and the workstation. The remote file name on the Prestige is “rom-spt”.
- Step 7.** The system reboots automatically after the file transfer process is complete.

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands, 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.

## 14.3 Firmware Update

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

Note that this function erases the old data before installing the new one; please do not attempt to update unless you have the new firmware at hand. There are 2 components in the system: the router firmware and the configuration file, as shown next.

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

1. Upload Router Firmware
2. Upload Router Configuration File

Enter Menu Selection Number:
```

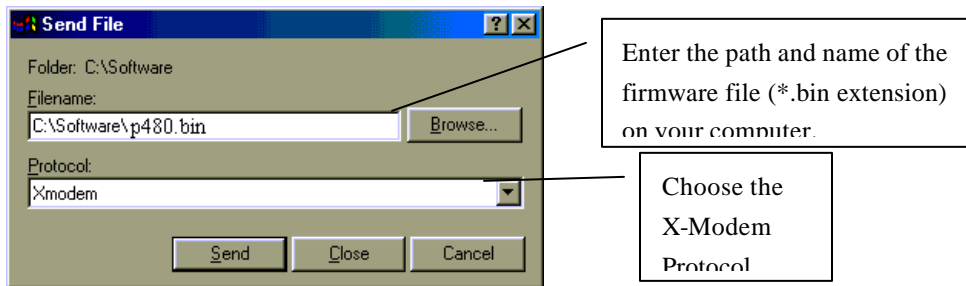
**Figure 14-8 Menu 24.7 - System Maintenance - Upload Firmware**

## 14.3.1 Upload through the Console Port

### *Upload Firmware File*

The firmware is the program that controls the functions of the Prestige. **Menu 24.7.1** shows you the instructions for uploading the firmware. If you answer yes to the prompt, the Prestige will go into debug mode. Follow the procedure below to upload the firmware:

- Step 1.** Enter “atur” after the “Enter Debug Mode” message.
- Step 2.** Wait for the "Starting XMODEM upload" message. The following procedure is for the HyperTerminal program. The procedure for other serial communications programs should be similar.
- Step 3.** Click “Transfer” in the HyperTerminal toolbar, then “Send File” in the popup menu to display the following screen.



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



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

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

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

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

**Figure 14-9 Menu 24.7.1 - Uploading Router Firmware**

### ***Upload Configuration File***

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

**Menu 24.7.2** shows you the instructions for uploading the configuration file. If you answer yes to the prompt, the Prestige will go into debug mode. Follow the procedure below to upload the configuration file:

- Step 1.** Enter "atur3" after the "Enter Debug Mode" message.
- Step 2.** Wait for the "Starting XMODEM upload" message before activating Xmodem upload on your terminal.
- Step 3.** After successful firmware upload, enter "atgo" to restart the Prestige.

If you replace the current configuration file with the default configuration file, i.e., p480.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 communications software to the default before you can connect to the Prestige again. The password will be reset to the default of 1234, also.

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

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

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

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

**Figure 14-10 Menu 24.7.2 - System Maintenance - Upload Router Configuration File**

### 14.3.2 Upload using FTP

In addition to uploading the firmware and configuration via the console port and TFTP client, you can also upload the P480 firmware and configuration files using FTP.

To use this feature, your workstation must have an FTP client. To transfer the firmware and the configuration file, follow the examples below:

#### ***Using FTP command in terminal***

**Step 1.** Use FTP client from your workstation to the Prestige 480 and log in by entering the IP address of the Prestige.

**Step 2.** Press [ENTER] key to ignore user name.

- Step 3.** Enter the administrator password. The default is 1234
- Step 4.** Enter the command “bin” to set binary transfer type
- Step 5.** Use the command “put” to transfer files between the Prestige and the workstation. The file name for the firmware is “ras” and for the configuration file “rom-0” (rom-zero, not capital o).

```
Connected to 480.x.x.x
220 P480 FTP version 1.0 ready at Thu Jan  8 18:00:02 1970
User (480.x.x.x:(none)): <Enter>
331 Enter PASS command
Password:
230 Logged in
ftp> bin
ftp> ha
```

**Figure 14-11 FTP Example**

The system reboots after a successful upload.

***Using FTP client software***

- Step 1.** Rename the local firmware and configuration files to '**ras**' and '**rom-0**', because we can not specify the remote file name in the FTP client software.
- Step 2.** Use FTP client from your workstation to the Prestige 480 and log in by entering the IP address of the Prestige.
- Step 3.** Set the transfer type to '**Auto-Detect**' or '**Binary**'.



Figure 14-12 Edit Host

**Step 4.** Press **'OK'** to ignore the 'Username' prompt.



Figure 14-13 Username Prompt

**Step 5.** To upload the firmware file, transfer the local **'ras'** file to overwrite the remote **'ras'** file.  
To upload the configuration file, transfer the local **'rom-0'** to overwrite the remote **'rom-0'** file.

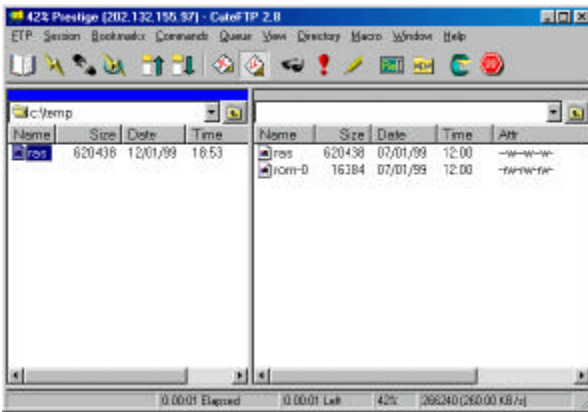


Figure 14-14 Files Transfer

The system reboots after a successful upload.

### 14.3.3 Upload using TFTP

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

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

- Step 1.** Use telnet from your workstation to connect to the Prestige and log in. Because TFTP does not have any security check, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.
- Step 2.** Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- Step 3.** Enter command “`sys studio 0`” to disable SMT timeout, so the TFTP transfer will not be interrupted.

- Step 4.** Launch TFTP client on your workstation and connect to the Prestige. Set the transfer mode to binary before starting data transfer.
- Step 5.** Use the TFTP client to transfer files between the Prestige and the workstation. The file name for the firmware is “`ras`” and for the configuration file, “`rom-0`” (rom-zero, not capital o).

If you upload the firmware to the Prestige, it will reboot automatically when the file transfer is completed.

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

# Chapter 15

## IP Policy Routing

### 15.1 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.

#### 15.1.1 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 bulk traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.

#### 15.1.2 Routing Policy

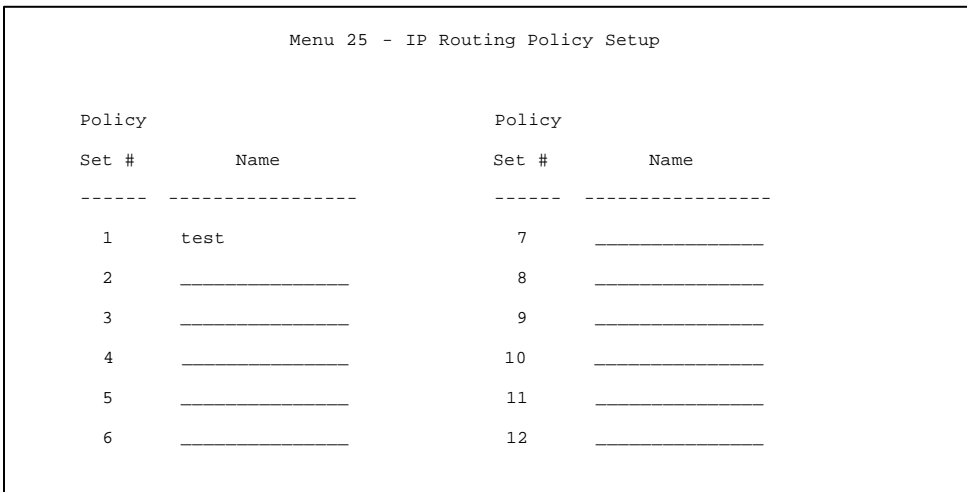
A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria include the source address and port, IP protocol (ICMP, UDP, TCP, etc.), destination address and port, TOS and precedence (fields in the 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.

### 15.1.3 IP Routing Policy Setup

Menu 25 shows all the policies defined



```
Menu 25 - IP Routing Policy Setup

Policy
Set #      Name
-----
1          test
2          _____
3          _____
4          _____
5          _____
6          _____

Policy
Set #      Name
-----
7          _____
8          _____
9          _____
10         _____
11         _____
12         _____
```

**Menu 25 - 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 Routing Policy Setup**.

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



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

```
Menu 25.1 - IP Routing Policy Summary

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

**Menu 25 - IP Routing Policy Summary**

### 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 Type    = Gateway node   Gateway addr = 1.2.3.4
  Type of Service= No Change       Gateway node = 2
  Precedence      = No Change      Log= No

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

```

**Figure 15-1 Menu 25.1.1 - IP Routing Policy**

**Table 15-1 IP Routing Policy Menu Fields**

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 <b>Yes</b> 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 <b>Don't Care/ Normal / Min Delay / Max Thruput / Max Reliability</b> .
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 <b>Equal / Not Equal / Less / Greater / Less or Equal / Greater or Equal</b> .
Precedence	Precedence value of the incoming packet. Values range from <b>0</b> to <b>7</b> or <b>Don't Care</b> .
Source:	
addr start= / end=	Source IP address range from start to end.
port start= /	Source port number range from start to end; applicable only for TCP/UDP.

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 <b>Matched</b> or <b>Not Matched</b> .
Gateway type	Allows you to choose the outgoing gateway type. The gateway can be on the same subnet as the Prestige if it's on the LAN, otherwise, the gateway can be the IP address of a remote node. You can choose <b>Gateway addr</b> if you want to assign the gateway IP address by yourself. Or you can specify the remote node as your gateway by choosing <b>Gateway node</b> .
Gateway addr	Enter the IP address of your gateway.
Gateway node	This can be set as 0 to 12. 0 means no change. 1 means remote node 1 in Menu 11 and so on.
Type of Service	Set the new TOS value of the outgoing packet. Choose from Prioritize incoming network traffic by choosing from <b>No Change / Normal / Min Delay / Max Thruput / Max Reliability</b> .
Precedence	Set the new precedence value of the outgoing packet. Values range from <b>0</b> to <b>7</b> or <b>No Change</b> .
Log	Press the spacebar to select <b>Yes</b> to make an entry in the system log when a policy is executed.

## 15.2 Applying an IP Policy

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

### 15.2.1 Ethernet IP Policies

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

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

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

DHCP Setup
  DHCP= Server
  Client IP Pool Starting Address= 192.168.1.33
  Size of Client IP Pool= 32
  Primary DNS Server= 0.0.0.0
  Secondary DNS Server= 0.0.0.0
  Remote DHCP Server= N/A

TCP/IP Setup:
  IP Address= 192.168.1.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
    Version= RIP- 1
  Multicast = IGMP-v2
  IP Policies=
  Edit IP Alias= Yes

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

Enter your IP  
Policy sets  
here.

**15-2 Menu 3.2 – TCP/IP Ethernet Setup**



# Chapter 16

## Troubleshooting

*This chapter covers the potential problems you may run into and the possible remedies.*

After each problem description, some instructions are provided to help you to diagnose and to solve the problem. If you still have problems, check all the connections and settings, refer to your user's guide and if the problem persists e-mail or call your dealer for assistance.

### 16.1 Problems Starting Up the Prestige

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

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

<p>The Prestige drops the call even though the authentication phase was successful.</p>	<p>Check the IP address of the remote node. The Prestige uses the IP address as another form of authentication. Hence, if the address supplied by the remote node does not match the address the Prestige is expecting, the call will be dropped.</p> <p>You can rectify this problem by using the Internet Access Setup <b>Menu 4</b> to configure your remote node.</p> <p>You can enter the ISP's IP address field as 0.0.0.0. In this case, the Prestige will accept any IP address sent from the device and the call won't be dropped.</p>
-----------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



## 16.2 Problems With the ISDN Lines

**Table 16-2 Troubleshooting the ISDN Lines**

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

## 16.3 Problems with the Ethernet Connection

**Table 16-3 Troubleshooting the Ethernet Connection**

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

## 16.4 Problems Connecting to a Remote Node or ISP

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

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

## 16.5 Problems for Remote User to Dial-in

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

<b>Problem</b>	<b>Corrective Action</b>
A remote user cannot dial-in	First verify that you have configured the authentication parameters in Menu 13. These would be CLID Authen and Recv. Authen.
	In Menu 14, verify the user name and password for the remote dial-in user.
	If the remote dial-in user is negotiating IP, verify that the IP address is supplied correctly in Menu 13. Check that either the remote dial-in user is supplying a valid IP address, or that the Prestige is assigning a valid address from the IP pool.



# Information Worksheet

This information worksheet has been provided to help you collect the following information for future use.

General Information		
System Name		
Protocol Routing	<input type="checkbox"/> TCP/IP	
ISDN Information		
Switch Type	<input type="checkbox"/> DSS1	
B-Channel Usage	<input type="checkbox"/> Switch/Switch	<input type="checkbox"/> Switch/Leased
	<input type="checkbox"/> Leased/Switch	<input type="checkbox"/> Leased/Unused
	<input type="checkbox"/> Unused/Leased	<input type="checkbox"/> Leased/Leased
	<input type="checkbox"/> Switch/Unused	
European ISDN (DSS1)		
ISDN Line	ISDN 1	
ISDN Data Number		
Outside Line Prefix		
PABX # (S/T bus)		
ISDN Line	ISDN 2	
ISDN Data Number		
Outside Line Prefix		
PABX # (S/T bus)		
Ethernet Information		
Ethernet Interface	<input type="checkbox"/> STP	
IP Address	_____ . _____ . _____ . _____	
IP Subnet Mask	_____ . _____ . _____ . _____	

## General Information

The Prestige requires certain system information. You can obtain all the pertinent information from your network administrator.

**System Name** - This is the name given by you in **Menu 1** to the Prestige for identification purpose.

**Protocol Routing** – This refers to the protocols used for moving information across different networks. P480 supports TCP/IP protocol.

## ISDN Information

Refer to the section *ISDN Setup Menus* in the chapter **Hardware Installation and Setup** for further details.

**Switch Type** - This is the type of switch used by your telephone company.

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

## Ethernet Information

Refer to the chapter **Internet Access** of this guide for more details.

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

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

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

**Table 16-6 IP Subnet Masks and the Number of Hosts**

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





# Enhanced Syslog

The following are the message formats that Syslog sends to the server.

<b>CDR</b>
SdcmSyslogSend( SYSLOG_CDR, SYSLOG_INFO, String ); String = board xx line xx channel xx, call xx, str board = the hardware board ID line = the WAN ID in a board Channel = channel ID within the WAN call = the call reference number which starts from 1 and increments by 1 for each new call str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.) C01 Incoming Call xxxxBps xxxxx (L2TP,xxxxx means Remote Call ID) C01 Incoming Call xxxx (means connected speed) xxxxx (means Remote Call ID) L02 Tunnel Connected(L2TP) C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call ID) C02 CLID call refused L02 Call Terminated C02 Call Terminated
<b>Packet triggered</b>
sdcmSyslogSend( SYSLOG_PKTTRI, SYSLOG_NOTICE, String ); String = Packet trigger: Protocol=xx Data=xxxxxxxxx .....x Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG) Data: We will send forty -eight Hex characters to the server
<b>Filter log</b>
SdcmSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String ); String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD  IP[...] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m) drop (D). Src: Source Address Dst: Destination Address prot: Protocol ("TCP","UDP","ICMP") spo: Source port dpo: Destination port
<b>PPP Log</b>
sdcmSyslogSend( SYSLOG_PPPLOG, SYSLOG_NOTICE, String ); String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP



# 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
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	Service Advertising Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
STP	Shielded Twisted Pair (cable)
SUA	Single User Account
TA	(ISDN) Terminal Adapter
TFTP	Trivial File Transfer Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WAN	Wide Area Network

# Index

## 8

802.2, 6-1  
802.3, 6-1

## A

acronyms and abbreviations, G  
authentication protocol, 4-5  
auto-negotiation, 1-2

## B

backup configuration, 14-1  
BACP, 4-6  
Bandwidth on Demand. *See* BOD  
BAP, 1-3, 4-6  
Base Transmission Rate, 4-6  
blacklist, 13-17  
BOD, 1-3, 4-6, 4-7  
boot module commands, 13-14  
Bridge Ethernet Setup, 7-1  
bridge static route, 7-4  
bridging, 7-1  
BTR. *See* Base Transmission Rate  
budget, 13-18

## C

call control, 13-15  
call direction, 4-3  
callback, 8-9, 8-12, 8-14

CDR, 1-3, 13-9  
CHAP, 1-4, 4-4  
CI, 13-15  
CLID, 1-4, 8-4, 8-9, 8-12  
Command Interpreter. *See* CI  
community, 10-1  
console port, 2-3, 13-7  
customer support, v, xxi

## D

default dial-in setup, 8-4  
DHCP, 1-2, 3-3, 3-5  
diagnostic, 13-11  
dial-in server, 1-1  
dial-in user, 8-2  
dial-in user setup, 8-7  
dial-on-broadcast, 7-3  
dial-on-query, 6-8  
DIX, 6-1  
DNS, 1-2, 3-3, 3-5  
dual BRI, 1-1

## E

Ethernet II, 6-1  
Ethernet setup, 2-18

## F

factory Ethernet defaults, 3-1  
filter, 2-18, 4-10, 8-7, 9-1, 9-16

Filter  
    IPX  
        Packet Types, 9-14  
filter log, 13-9  
frame type, 6-1  
front panel, 2-1

## **G**

gateway, 7-5  
gateway IP address, 5-8  
general setup, 2-10  
generic filter rule, 9-11

## **H**

housing, 2-4

## **I**

IANA, 3-2  
idle timeout, 4-5  
Interactive Applications, 15-1  
Internet access, 1-5, 3-1, 3-14  
IP address, 3-2, 4-4, 5-5, 5-8, 7-5, B  
IP Alias, 3-6  
IP Alias Setup, 3-7  
IP network number, 3-2  
IP Policies, 15-7  
IP Policy Routing (IPPR), 15-1  
    Applying an IP Policy, 15-7  
    Benefits, 15-1  
    Cost Savings, 15-1  
    Criteria, 15-1

Ethernet IP Policies, 15-7  
Gateway, 15-6  
Load Sharing, 15-1  
    Setup, 15-2  
IP pool, 3-3  
IP Routing Policy, 15-5  
IP Routing Policy Setup, 15-4  
IP static route, 5-6  
IP subnet mask, B  
IP Subnet Mask, C  
IPX, 6-1  
IPX Ethernet Setup, 6-4  
IPX LAN-to-LAN, 6-6  
IPX network number, 6-1, 6-2  
IPX node number, 6-1  
IPX Spoofing, 6-4  
IPX static route, 6-9  
ISDN, 1-1  
ISDN setup, 2-11, 2-12  
ISP, 3-17

## **L**

LAN, 13-4  
LAN-to-LAN, 5-1, 8-3  
log, 13-7

## **M**

MAC, 7-1  
main menu, 2-6  
Max. Transmission Rate, 4-6  
Media Access Control. *See* MAC  
Mega Bundle

Configuration, 3-16

MP, 4-6

Multilink. *See* MP

Multiple ISPs Support. *See* Mega Bundle

multiple servers, 8-16

## N

nailed-up connection, 4-5

NetCAPI, 2-14

CAPI, 2-14

ISDN-DCP, 2-14

RVS-CE and RVS-COM Lite, 2-15

NetCAPI Configuration, 2-16

## P

PABX, 2-13

packet triggered, 13-9

PAP, 1-4, 4-4, 8-5

password, 2-4, 2-7, 11-1

ping host, 13-12

PNC, xxi, 1-3, 2-3

Point-to-Point Protocol/Multilink Protocol. *See*

PPP/MP

power adapter, 2-3

PPP, 4-4, 4-7

PPP log, 13-9

PPP/MP, 1-2, 1-8, 3-11

Precedence, 15-1, 15-5

Prestige Network Commander. *See* PNC

## Q

Quality of Service, 15-1

## R

RADIUS, 1-4

Accounting, 11-6

Authentication, 11-3

For CLID authentication, 11-6

Server Configuration, 11-4

RAS code, 14-7

remote access, 8-11. *See* dial-in user setup

remote node, 4-1, 13-12

resetting the prestige, 2-8

RIP, 3-2, 5-5, 6-8

ROM File, 14-8

Routing Policy, 15-1

## S

SAP, 6-8

settings, 2-3

Single User Account. *See* SUA

SMT, 1-3, 2-5

SNAP, 6-1

SNMP, 1-3, 10-1

software update, 14-7

SUA, 1-6, 3-11, 3-12, 3-14, 5-5, 8-16

subnet mask, 3-2, 5-5

switch types, 16-2

System Maintenance

Backup

Console Port, 14-1

FTP, 14-2  
TFTP, 14-2  
Restore, 14-4  
  Console Port, 14-4  
  FTP, 14-6  
  TFTP, 14-6  
system management, 13-1  
System Management Terminal. *See* SMT  
system status, 13-2

## **T**

target utility, 4-7  
TCP/IP, 3-2, 3-4, 5-1, 13-12, B  
TCP/IP filter rule, 9-7  
Telco options, 3-11  
telnet, 12-1  
TFTP, 1-5, 14-11  
tick count, 6-8  
time and date setting, 13-20  
TOS (Type of Service), 15-1

trace, 13-7  
troubleshooting, 16-1  
Type of Service, 15-1, 15-4, 15-5, 15-6

## **U**

UNIX syslog, 1-3, 13-8

## **V**

VT100, 2-3

## **W**

WAN address, 5-5  
watchdog, 6-8  
worksheet, A

## **Z**

ZyNOS, 15-2