

# *Prestige 681*

*SDSL Router*

## *User's Guide*

Version 2.50

(Dec. 1999)

**ZyXEL**

TOTAL INTERNET ACCESS SOLUTION

# **Prestige 681**

## **SDSL Internet Access Router**

### **Copyright**

Copyright ©1999 by ZyXEL Communications Corporation.

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

Published by ZyXEL Communications Corporation. All rights reserved.

### **Disclaimer**

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

### **Trademarks**

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners. ZyNOS is a registered trademark of ZyXEL Communications Corporation.

## **Federal Communications Commission (FCC) Interference Statement**

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

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

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

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

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

### Notice 1

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

### Notice 2

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

## **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(s) or desire assistance, please contact ZyXEL Communications Corporation offices worldwide, in any one of the following ways. Our ftp sites are also available for software and ROM upgrades.

Method Region	EMAIL – Support	Telephone	Web Site	Regular Mail
	EMAIL – Sales	Fax	FTP Site	
Worldwide	<a href="mailto:support@zyxel.com.tw">support@zyxel.com.tw</a>	+886-3-578-3942	<a href="http://www.zyxel.com">www.zyxel.com</a>	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, HsinChu, Taiwan.
	<a href="mailto:support@europe.zyxel.com">support@europe.zyxel.com</a>		<a href="http://www.europe.zyxel.com">www.europe.zyxel.com</a>	
North America	<a href="mailto:sales@zyxel.com">sales@zyxel.com</a>	+886-3-578-2439	<a href="http://ftp.europe.zyxel.com">ftp.europe.zyxel.com</a>	ZyXEL Communications Inc., 1650 Miraloma Avenue, Placentia, CA 92870, U.S.A.
	<a href="mailto:support@zyxel.com">support@zyxel.com</a>	+1-714-632-0882 800-255-4101	<a href="http://www.zyxel.com">www.zyxel.com</a>	
Scandinavia	<a href="mailto:sales@zyxel.com">sales@zyxel.com</a>	+1-714-632-0858	<a href="http://ftp.zyxel.com">ftp.zyxel.com</a>	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark.
	<a href="mailto:support@zyxel.dk">support@zyxel.dk</a>	+45-3955-0700	<a href="http://www.zyxel.dk">www.zyxel.dk</a>	
Austria	<a href="mailto:sales@zyxel.dk">sales@zyxel.dk</a>	+45-3955-0707	<a href="http://ftp.zyxel.dk">ftp.zyxel.dk</a>	ZyXEL Communications Services GmbH., Thaliastrasse 125a/2/2/4, A-1160 Vienna, Austria
	<a href="mailto:support@zyxel.at">support@zyxel.at</a>	+43-1-4948677-0 0810-099935	<a href="http://www.zyxel.at">www.zyxel.at</a>	
Germany	<a href="mailto:sales@zyxel.at">sales@zyxel.at</a>	+43-1-4948678	<a href="http://ftp.zyxel.at">ftp.zyxel.at</a> Note: for Austrian users with *.at domain only!	ZyXEL Deutschland GmbH., Adenauerstr. 20/A4, D-52146 Wuersele, Germany.
	<a href="mailto:support@zyxel.de">support@zyxel.de</a>	+49-2405-6909-0 0180-5213247 Tech Support hotline 0180-5099935 RMA/Repair hotline	<a href="http://www.zyxel.de">www.zyxel.de</a>	
	<a href="mailto:sales@zyxel.de">sales@zyxel.de</a>	+49-2405-6909-99		

# Table of Contents

<b>Customer Support</b> .....	<b>v</b>
<b>Table of Contents</b> .....	<b>vi</b>
<b>List of Figures</b> .....	<b>xi</b>
<b>List of Tables</b> .....	<b>xiv</b>
<b>Preface</b> .....	<b>xvi</b>
<b>Structure of this Manual</b> .....	<b>xviii</b>
<b>What is DSL?</b> .....	<b>xix</b>
<b>Chapter 1: Getting to Know Your SDSL Internet Access Router</b> .....	<b>1-1</b>
1.1 Prestige 681 SDSL Internet Access Router.....	1-1
1.2 Features of the Prestige 681 .....	1-1
1.3 Applications for the Prestige 681 .....	1-3
1.3.1 Internet Access .....	1-3
1.3.2 LAN to LAN Application.....	1-4
<b>Chapter 2: Hardware Installation &amp; Initial Setup</b> .....	<b>2-1</b>
2.1 Front Panel LEDs OF P681 .....	2-1
2.2 Prestige 681 Rear Panel and Connections .....	2-2
2.3 Additional Installation Requirements .....	2-3
2.4 Housing .....	2-3
2.5 Important Safety Instructions .....	2-3
2.6 Power On Your Prestige.....	2-5
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 Filename conventions .....	2-8
2.9.1 Resetting the Prestige.....	2-9
2.10 General Setup .....	2-9

2.10.1	Note on Bridging .....	2-10
2.11	Ethernet Setup.....	2-10
2.11.1	General Ethernet Setup.....	2-11
2.12	Protocol Dependent Ethernet Setup.....	2-11
<b>Chapter 3: WAN Setup.....</b>		<b>3-1</b>
3.1	Frame Relay .....	3-1
3.1.1	Frame relay frame format.....	3-2
3.1.2	Connection setup.....	3-3
3.2	Setting up the WAN link.....	3-4
3.2.1	Frame Relay Options.....	3-5
<b>Chapter 4: Internet Access.....</b>		<b>4-1</b>
4.1	Factory Ethernet Defaults .....	4-1
4.2	TCP/IP Parameters .....	4-1
4.2.1	IP Address and Subnet Mask.....	4-1
4.2.2	Private IP Addresses .....	4-2
4.2.3	RIP Setup.....	4-2
4.2.4	DHCP Configuration.....	4-3
4.3	Route IP Setup.....	4-4
4.4	TCP/IP Ethernet Setup and DHCP.....	4-4
4.5	LANs & WANs .....	4-7
4.5.1	LANs, WANs and the Prestige.....	4-7
4.6	Encapsulation.....	4-8
4.6.1	RFC 1490 .....	4-8
4.6.2	PPP .....	4-8
4.7	DLCI.....	4-8
4.8	Internet Access Configuration .....	4-9
4.9	Single User Account.....	4-10
4.9.1	Advantages of SUA.....	4-11
4.9.2	Single User Account Configuration .....	4-11
4.10	Multiple Servers behind SUA .....	4-12
4.10.1	Configuring a Server behind SUA.....	4-13
<b>Chapter 5: Remote Node Configuration.....</b>		<b>5-1</b>

5.1 Remote Node Setup.....	5-1
5.1.1 Remote Node Profile.....	5-1
5.1.2 Outgoing Authentication Protocol.....	5-4
5.1.3 Editing PPP Options.....	5-4
5.1.4 Remote Node Filter.....	5-5
<b>Chapter 6: Remote Node TCP/IP Configuration.....</b>	<b>6-1</b>
6.1 LAN-to-LAN Application.....	6-1
6.1.1 Editing TCP/IP Options.....	6-1
6.1.2 Static Route Setup.....	6-4
<b>Chapter 7: IPX Configuration.....</b>	<b>7-1</b>
7.1 IPX Network Environment.....	7-1
7.1.1 Network and Node Number.....	7-1
7.1.2 Frame Types.....	7-1
7.1.3 External Network Number.....	7-2
7.1.4 Internal Network Number.....	7-2
7.2 Prestige 681 in an IPX Environment.....	7-3
7.2.1 Prestige 681 on LAN with Server.....	7-3
7.2.2 Prestige 681 on LAN without Server.....	7-3
7.3 IPX Ethernet Setup.....	7-4
7.4 LAN-to-LAN Application with Novell IPX.....	7-5
7.4.1 IPX Remote Node Setup.....	7-6
7.4.2 IPX Static Route Setup.....	7-8
<b>Chapter 8: Bridging Setup.....</b>	<b>8-1</b>
8.1 Bridging in General.....	8-1
8.2 Bridge Ethernet Setup.....	8-1
8.2.1 Remote Node Bridging Setup.....	8-3
8.3 Bridge Static Route Setup.....	8-4
<b>Chapter 9: 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 Menu.....	9-4
9.3 Configuring a Filter Rule.....	9-6
9.3.1 TCP/IP Filter Rule.....	9-7



9.3.2	Generic Filter Rule .....	9-11
9.3.3	Novell IPX Filter Rule .....	9-13
9.4	Example Filter.....	9-15
9.5	Filter Types and SUA .....	9-18
9.6	Applying a Filter and Factory Defaults .....	9-18
9.6.1	Ethernet traffic .....	9-18
9.6.2	Remote Node Filters .....	9-19
<b>Chapter 10: SNMP Configuration.....</b>		<b>10-1</b>
10.1	About SNMP.....	10-1
10.2	Configuring SNMP.....	10-1
<b>Chapter 11: System Maintenance.....</b>		<b>11-1</b>
11.1	System Status.....	11-2
11.1.1	Console Port Speed .....	11-5
11.2	Log and Trace .....	11-5
11.2.1	Viewing Error Log.....	11-5
11.2.2	Syslog And Accounting .....	11-6
11.3	Diagnostic.....	11-9
11.4	Backup Configuration .....	11-10
11.5	Restore Configuration .....	11-11
11.6	Upload Firmware .....	11-12
11.6.1	Upload Router Firmware .....	11-13
11.6.2	Upload Router Firmware using FTP.....	11-13
11.6.3	Uploading Router Configuration File.....	11-14
11.6.4	Upload Router configuration File using FTP.....	11-15
11.7	TFTP Transfer.....	11-15
11.8	Command Interpreter Mode .....	11-17
11.9	Boot module commands .....	11-18
<b>Chapter 12: Troubleshooting .....</b>		<b>12-1</b>
12.1	Problems Starting Up the Prestige.....	12-1
12.2	Problems With the WAN Interface .....	12-2
12.3	Problems with the LAN Interface.....	12-2

12.4	Problems Connecting to a Remote Node or ISP .....	12-2
<b>Glossary</b>	.....	<b>A</b>
<b>Index</b>	.....	<b>G</b>

# List of Figures

Figure 1-1	Internet Access Application .....	1-4
Figure 1-2	LAN-to-LAN Application via Frame Relay .....	1-5
Figure 1-3	LAN-to-LAN Application via Direct Connection .....	1-5
Figure 2-1	Prestige 681 Front Panel. ....	2-1
Figure 2-2	Prestige 681 Rear Panel 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 23.1 - System Password .....	2-8
Figure 2-7	Menu 1 – General Setup .....	2-10
Figure 2-8	Menu 3 - Ethernet Setup .....	2-11
Figure 2-9	Menu 3.1 - General Ethernet Setup .....	2-11
Figure 3-1	Dedicated Leased Lines – Multiple Sites .....	3-1
Figure 3-2	Frame Relay Solution .....	3-2
Figure 3-3	Frame Relay Format .....	3-2
Figure 3-4	Menu 2 – WAN Setup .....	3-5
Figure 3-5	Menu 2.1 - Frame Relay Options .....	3-6
Figure 4-1	Menu 1 – General Setup .....	4-4
Figure 4-2	Menu 3.2 – TCP/IP and DHCP Ethernet Setup .....	4-5
Figure 4-3	LAN & WAN IPs .....	4-7
Figure 4-4	Internet Access Setup .....	4-9
Figure 4-5	Menu 4 – Internet Access Setup for Single User Account .....	4-12
Figure 4-6	Example of Multiple Servers behind SUA .....	4-13
Figure 4-7	Multiple Server Configuration .....	4-14
Figure 5-1	Menu 11.1 Remote Node Profile .....	5-2
Figure 5-2	Menu 11.2 - Remote Node PPP Options .....	5-4

<i>Figure 5-3</i>	<i>Menu 11.5 – Remote Node Filter</i>	<i>5-5</i>
<i>Figure 6-1</i>	<i>TCP/IP LAN-to-LAN Application</i>	<i>6-1</i>
<i>Figure 6-2</i>	<i>Menu 11.3</i>	<i>6-2</i>
<i>Figure 6-3</i>	<i>Sample IP Addresses for a TCPI/IP LAN-to-LAN Connection</i>	<i>6-2</i>
<i>Figure 6-4</i>	<i>Example of Static Routing Topology</i>	<i>6-5</i>
<i>Figure 6-5</i>	<i>Menu 12 - IP Static Route Setup</i>	<i>6-5</i>
<i>Figure 6-6</i>	<i>Edit IP Static Route</i>	<i>6-6</i>
<i>Figure 7-1</i>	<i>NetWare Network Numbers</i>	<i>7-2</i>
<i>Figure 7-2</i>	<i>Prestige 681 in an IPX Environment</i>	<i>7-3</i>
<i>Figure 7-3</i>	<i>Menu 3.3 - Novell IPX Ethernet Setup</i>	<i>7-4</i>
<i>Figure 7-4</i>	<i>LAN-to-LAN Application with Novell IPX</i>	<i>7-5</i>
<i>Figure 7-5</i>	<i>Menu 11.3 - Remote Node Novell IPX Options</i>	<i>7-6</i>
<i>Figure 7-6</i>	<i>Menu 12.2 - Edit IPX Static Route</i>	<i>7-8</i>
<i>Figure 8-1</i>	<i>Menu 3.5 - Bridge Ethernet Setup</i>	<i>8-2</i>
<i>Figure 8-2</i>	<i>Menu 11.3 - Remote Node Bridging Options</i>	<i>8-3</i>
<i>Figure 8-3</i>	<i>Menu 12.3 - Bridge Static Route Setup</i>	<i>8-4</i>
<i>Figure 8-4</i>	<i>Menu 12.3.1 - Edit Bridge Static Route</i>	<i>8-4</i>
<i>Figure 9-1</i>	<i>Filter Rule Process</i>	<i>9-2</i>
<i>Figure 9-2</i>	<i>Menu 21 - Filter Set Configuration</i>	<i>9-3</i>
<i>Figure 9-3</i>	<i>NetBIOS_WAN Filter Rules Summary</i>	<i>9-3</i>
<i>Figure 9-4</i>	<i>NetBIOS_LAN Filter Rules Summary</i>	<i>9-4</i>
<i>Figure 9-5</i>	<i>Telnet Filter Rules Summary</i>	<i>9-4</i>
<i>Figure 9-6</i>	<i>Menu 21.1.1 - TCP/IP Filter Rule</i>	<i>9-7</i>
<i>Figure 9-7</i>	<i>Executing an IP Filter</i>	<i>9-10</i>
<i>Figure 9-8</i>	<i>Menu 21.1.2 - Generic Filter Rule</i>	<i>9-11</i>
<i>Figure 9-9</i>	<i>Menu 21.1.3 - IPX Filter Rule</i>	<i>9-13</i>
<i>Figure 9-10</i>	<i>Telnet Filter Example</i>	<i>9-15</i>
<i>Figure 9-11</i>	<i>Example Filter – Menu 21.1.1</i>	<i>9-16</i>

Figure 9-12	Example Filter Rules Summary – Menu 21.3	9-17
Figure 9-13	Protocol and Device Filter Sets	9-18
Figure 9-14	Filtering Ethernet traffic	9-19
Figure 9-15	Filtering Remote Node traffic	9-19
Figure 10-1	Menu 22 - SNMP Configuration	10-1
Figure 11-1	Menu 24 - System Maintenance	11-1
Figure 11-2	Menu 24.1 - System Maintenance – Status	11-2
Figure 11-3	System Information and Console Port Speed	11-3
Figure 11-4	System Maintenance - Information	11-4
Figure 11-5	Menu 24.2.2 – System Maintenance – Console Port Speed	11-5
Figure 11-6	Examples of Error and Information Messages	11-6
Figure 11-7	Menu 24.3.2 - System Maintenance - Syslog and Accounting	11-6
Figure 11-8	Menu 24.4 - System Maintenance - Diagnostic	11-9
Figure 11-9	Backup Configuration	11-10
Figure 11-10	HyperTerminal Screen	11-10
Figure 11-11	Successful Backup	11-11
Figure 11-12	Restore Configuration	11-11
Figure 11-13	HyperTerminal Screen	11-12
Figure 11-14	Successful Backup	11-12
Figure 11-15	Menu 24.7 - System Maintenance - Upload Firmware	11-13
Figure 11-16	Menu 24.7.1 - Uploading Router Firmware	11-13
Figure 11-17	Menu 24.7.2 - System Maintenance - Upload Router Configuration File	11-15
Figure 11-18	TFTP Example	11-17
Figure 11-19	Command Mode	11-18
Figure 11-20	Boot module commands	11-19

# List of Tables

Table 2-1	Front Panel LED Description	2-1
Table 2-2	Main Menu Commands	2-6
Table 2-3	Main Menu Summary	2-7
Table 2-4	Filename Conventions	2-9
Table 2-5	General Setup Menu Fields	2-10
Table 3-1	Frame Relay Format	3-3
Table 3-2	SDSL Maximum Transmission Distances (AWG 26, 0.4mm)	3-4
Table 3-3	Menu 2 – WAN Setup Fields	3-5
Table 3-4	Menu 2.1 - Frame Relay Options Fields	3-6
Table 4-1	DHCP Ethernet Setup Menu Fields	4-6
Table 4-2	TCP/IP Ethernet Setup Menu Fields	4-6
Table 4-3	Data Link Connection Identifiers	4-8
Table 4-4	Internet Account Information	4-9
Table 4-5	Internet Access Setup Menu Fields	4-10
Table 4-6	Single User Account Menu Fields	4-12
Table 4-7	Services vs. Port number	4-14
Table 5-1	Remote Node Profile Menu Fields	5-2
Table 5-2	Remote Node PPP Options Menu Fields	5-4
Table 6-1	TCP/IP related fields in Menu 11.1 - Remote Node Profile	6-3
Table 6-2	TCP/IP Remote Node Configuration	6-3
Table 6-3	Edit IP Static Route Menu Fields	6-6
Table 7-1	Novell IPX Ethernet Setup Fields	7-4
Table 7-2	Remote Node Novell IPX Options	7-7
Table 7-3	Edit IPX Static Route Menu Fields	7-9
Table 8-1	Bridge Ethernet Setup Menu - Handle IPX Field Configuration	8-2
Table 8-2	P681 Remote Node Network Layer Menu Bridge Options	8-3

Table 8-3	Bridge Static Route Menu Fields	8-5
Table 9-1	Abbreviations Used in the Filter Rules Summary Menu	9-5
Table 9-2	Abbreviations Used If Filter Type Is IP	9-6
Table 9-3	Abbreviations Used If Filter Type Is IPX	9-6
Table 9-4	Abbreviations Used If Filter Type Is GEN	9-6
Table 9-5	TCP/IP Filter Rule Menu Fields	9-7
Table 9-6	Generic Filter Rule Menu Fields	9-12
Table 9-7	IPX Filter Rule Menu Fields	9-14
Table 10-1	SNMP Configuration Menu Fields	10-2
Table 11-1	System Maintenance - Status Menu Fields	11-3
Table 11-2	Fields in System Maintenance - Information	11-4
Table 11-3	System Maintenance Menu Syslog Parameters	11-7
Table 11-4	System Maintenance Menu Diagnostic	11-10
Table 12-1	Troubleshooting the Start-Up of your Prestige	12-1
Table 12-2	Troubleshooting the SDSL connection	12-2
Table 12-3	Troubleshooting the LAN Interface	12-2
Table 12-4	Troubleshooting a Connection to a Remote Node or ISP	12-2

# Preface

## About Your SDSL Internet Access Router

Congratulations on your purchase of the Prestige 681 SDSL Router. Don't forget to register your Prestige (fast, easy online registration at [www.zyxel.com](http://www.zyxel.com)) for free future product updates and information.

The Prestige 681 (P681) is an SDSL router used for Internet/LAN access via an SDSL line. The Prestige 681 supports multi-protocol routing for TCP/IP and Novell IPX, as well as transparent bridging for other protocols. We will refer to the Prestige 681 as the P681 or simply the Prestige from now on.

The P681 SDSL router supports symmetrical multi-rate data transmission speeds from 144Kbps up to 2320Kbps. The actual rate depends on the copper category of your telephone wire, distance from the central office and the type of SDSL service subscribed. See the sections below for more background information on DSL and SDSL.

The P681 uses 2B1Q line code with echo cancellation for high data rate transmissions over a single twisted telephone wire pair without being affected by bridge taps or mixed cable links. It also provides high immunity from background noise.

The P681's 10/100M auto-negotiating LAN interface enables fast data transfer of either 10Mbps or 100Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

Your Prestige is easy to install and to configure. All functions of the Prestige are software configurable via the SMT (System Management Terminal) Interface.

## About This User's Guide

This user's guide covers all operations of the Prestige 681 and shows you how to get the best out of the multiple advanced features of your SDSL Internet Access Router. It is designed to guide you through the correct configuration of your Prestige 681 for various applications.

## Related Documentation

### ➤ PNC Disk

More detailed information about the Prestige and examples of its use can be found in our PNC (Prestige Network Commander – an alternative windows-based configuration wizard) Disk. This disk contains information on configuring your P681 for Internet Access, a General FAQ, an Advanced FAQ, Applications Notes, Troubleshooting, Reference CI Commands as well as bundled software.

### ➤ Read Me First

Our Read Me First is designed to help you get your Prestige up and running right away. It contains a detailed easy to follow connection diagram, Prestige default settings, handy checklists, information on



setting up your PC, information on installing and using the Prestige Network Commander, our windows-based Internet Access configuration wizard.

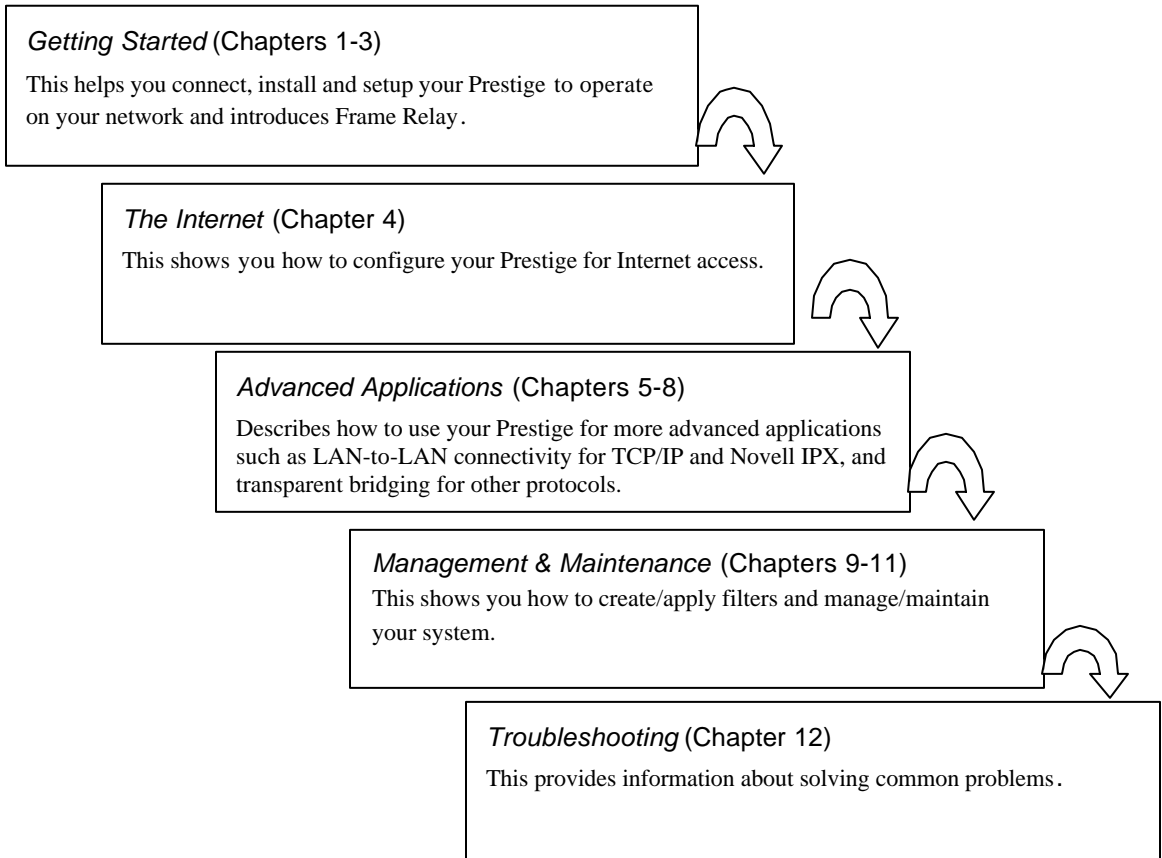
➤ Packing List Card

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

## **Syntax Conventions**

- “Enter” means for you to type one or more characters and press the carriage return. “Select” or “Choose” means for you to select one from the predefined choices.
- The SMT menu titles and labels are in **Bold Times** font. The choices of a menu item are 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.

# Structure of this Manual



The following section offers some background information on SDSL. Skip to Chapter 1 if you wish to begin working with your router right away.

# What is DSL?

DSL (Digital Subscriber Line) enhances the data capacity of the existing twisted-pair wire that runs between the local telephone company switching offices and most homes and offices. While the wire itself can handle higher frequencies, the telephone switching equipment is designed to cut off signals above 4,000 Hz to filter noise off the voice line, but now everybody is searching for ways to get more bandwidth to improve access to the Web - hence DSL technologies!

There are actually seven types of DSL service, ranging in speeds from 16 Kbits/sec to 52 Mbits/sec. The services are either symmetrical (traffic flows at the same speed in both directions), or asymmetrical (the downstream capacity is higher than the upstream capacity).

As data rates increase, the carrying distance decreases. That means that users who are beyond a certain distance from the telephone company's central office may not be able to obtain the higher speeds (*see Table 3-2* for SDSL Maximum Transmission Distances). A SDSL connection is a point-to-point dedicated circuit, meaning that the link is always up and there is no dialing required.

## SDSL

SDSL (Symmetrical Digital Subscriber Line) is a symmetrical, bi-directional DSL service that operates on one twisted-pair wire. It can provide data rates up to 2.3 Mbits/sec. Unlike traditional HDSL systems, which use two twisted pair, SDSL reduces equipment and lease-line costs by providing the same service using only one twisted pair and one modem at each end. SDSL is symmetric, which means you get the same amount of bandwidth to and from the Internet. SDSL provides speeds up to 12 times faster than an ISDN line and up to 50 times that of an analog modem connection at a fraction of the price of traditional dedicated access services.

The "always-on" digital connection provides the stability and consistent high bandwidth so crucial to today's online business community, allowing applications such as video conferencing, distance learning and high-powered Web browsing to perform with peak efficiency. SDSL allows Webmasters to set-up a web server, mail server and any other Internet service with increased bandwidth yet no additional charges. Because SDSL is symmetric, it is ideal for businesses, especially if you host a web site. It provides you with the high bandwidth required for uploading and downloading large data files and graphics. SDSL also gives you the bandwidth you need to retrieve information from Internet POPs, Internet servers and private data networks.

These are the main characteristics of SDSL:

- **Continuous Connection** SDSL users are never disconnected. There is no wait for dialup, where ISDN and regular analog modems often take half a minute to establish a connection.
- **Dedicated Bandwidth** You select the line speed and it is "symmetric," i.e., the same bandwidth in both directions.

- **Investment Protection** SDSL is scalable, offering customers a flexible upgrade path. You can adjust your SDSL router when you decide you need a higher access speed. This is an internal procedure; no site visit is necessary.
- **Low Maintenance** SDSL connectivity (unlike ISDN) requires no complex manual configuration; SDSL equipment is simply "plug and play."

## **Comparisons with other high-speed technologies:**

### **Cable Modems**

- With most Cable Modem systems, bandwidth is shared by a large number of clients. This means that users may not achieve maximum transfer rates if the network is busy. The SDSL circuit is point-to-point, which means that all bandwidth on the circuit is dedicated to a single client.
- If your company needs fast Internet access then SDSL allows you to transfer data up to 3 times faster than with a cable modem.

### **ISDN**

- ISDN service is considerably slower than SDSL. ISDN equipment is generally limited to 128k plus compression, which might give you speeds of up to 512 Kbps. SDSL gives you speeds of up to 2.3Mbps.
- ISDN does not have the ability to travel over very large distances (across the country) while SDSL is very distance limited.

### **T1**

- T1 is very expensive because it requires a high speed, noise conditioned phone line. SDSL works over a simple "copper loop" and does not require an expensive conditioned line.
- T1 delivers 1.5 Mbps in both directions over the line. SDSL delivers speeds of up to 2.3 Mbps in both directions.

# Chapter 1: Getting to Know Your SDSL Internet Access Router

*This chapter describes the key features and applications of the Prestige 681.*

## 1.1 Prestige 681 SDSL Internet Access Router

As its name implies, SDSL is a symmetric (equal upstream and downstream speeds) service that delivers scalable, high-speed data communication speeds up to 2.3 Mbps. SDSL is the most reliable of the DSL family members because it's based on proven technology that the telephone companies have been using for years for their E1 service. Your Prestige integrates a high-speed 10/100Mbps auto-negotiating LAN interface and one high-speed SDSL port into a single package. The Prestige is ideal for high-speed Internet browsing and making LAN-to-LAN connections to remote networks.

## 1.2 Features of the Prestige 681

Your Prestige is packed with a number of features that give it the flexibility to provide a complete networking solution for almost any user.

- **Ease of Installation**

Your Prestige is designed for quick, intuitive and easy installation. Physically, its compact size and lightweight make it easy to position anywhere in your busy office.

- **High Speed Scalability**

One of the best features of SDSL service is its scalability. The P681 SDSL router supports symmetrical multi-rate data transmission speeds from 144Kbps up to 2320Kbps. You can increase the capacity of the Internet connection (within certain distance limitations – *see Table 3-2*) without changing your ISP or purchasing new equipment. SDSL's high symmetrical speeds are ideal for applications like web hosting and videoconferencing as well as the two-way data traffic needs of businesses.

- **Frame Relay Support**

Frame relay employs a simple form of packet switching that perfectly suits today's powerful PCs, workstations and servers. Its high throughput and reliability easily copes with bandwidth-hungry business applications.

- **10/100M Fast Ethernet LAN Interface**

The P681's 10/100M auto-negotiating LAN interface enables fast data transfer of either 10Mbps or 100Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

- **Protocols Supported**

- ◆ TCP/IP (Transmission Control Protocol/Internet Protocol) network layer protocol.
- ◆ PPP (Point-to-Point Protocol) link layer protocol.
- ◆ SUA™ (Single User Account) and NAT (Network Address Translation).

- **Multiple Protocol Support**

- ◆ Novel IPX (Internetwork Packet eXchange) network layer protocol.
- ◆ Transparently bridging for unsupported network layer protocols.

- **DHCP Support**

DHCP (Dynamic Host Configuration Protocol) allows you to automatically assign TCP/IP settings to workstations on your network. Your P681 can act as a DHCP server or client.

- **Networking Compatibility**

Your Prestige is compatible with the major SDSL DSLAM (Digital Subscriber Line Access Multiplexer) providers, making configuration as simple as possible for you.

- **Encapsulation**

The Prestige 681 supports RFC 1490 (Multiprotocol over Frame Relay) and PPP over HDLC (RFC 1662) encapsulation.

- **NAT/SUA for single-IP-address Internet Access**

The Prestige's SUA (Single User Account) feature allows multiple user Internet access for the cost of a single ISP account. SUA supports popular Internet application, such as MS traceroute, CuSeeMe, IRC, RealAudio, VDOLive, Quake, and PPTP. No configuration is needed to support these applications.

- **Full Network Management**

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

- **PAP and CHAP Security**

The Prestige supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure since the password is scrambled prior to transmission. However, PAP is readily available on more platforms.

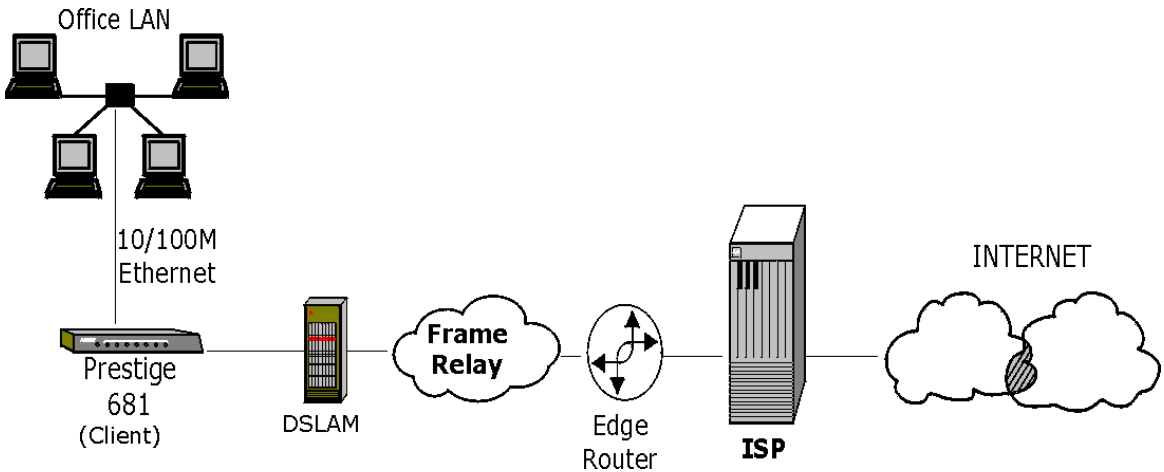
- **Filters**

The Prestige's packet filtering functions allows added network security and management.

## **1.3 Applications for the Prestige 681**

### **1.3.1 Internet Access**

The Prestige is the ideal high-speed Internet access solution. Your Prestige supports the TCP/IP protocol, which the Internet uses exclusively. It is compatible with all major SDSL DSLAM (Digital Subscriber Line Access Multiplexer) providers. A DSLAM is a rack of SDSL line cards with data multiplexed into a backbone network interface/connection (e.g., T1, OC3, DS3, ATM or Frame Relay). Think of it as the equivalent of a modem rack for SDSL. A typical Internet Access application is shown next.



**Figure 1-1 Internet Access Application**

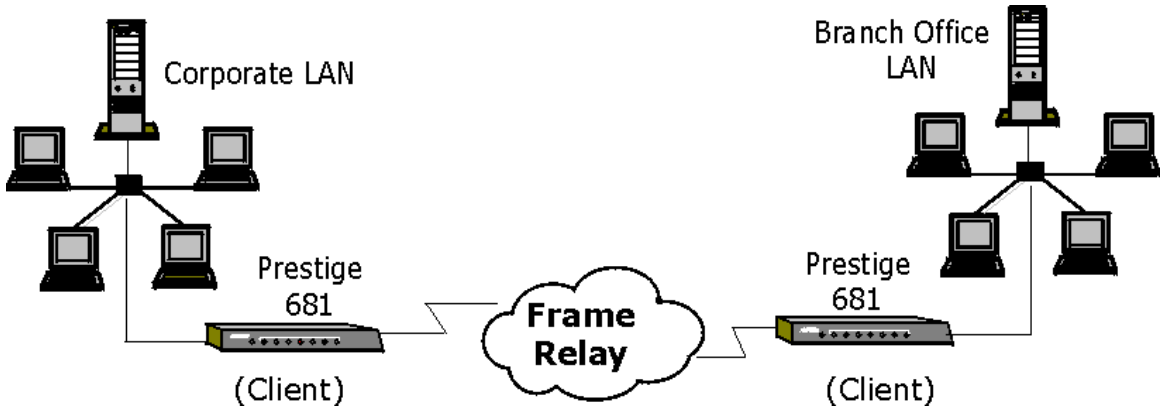
### **Internet Single User Account**

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

### **1.3.2 LAN to LAN Application**

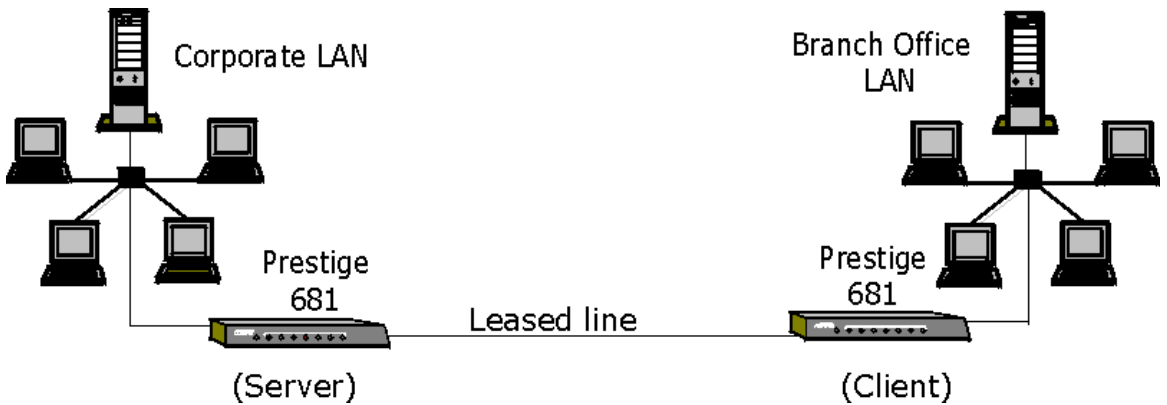
You can use the Prestige to connect two geographically dispersed networks over the SDSL line. Typical LAN-to-LAN applications for your Prestige are shown as follows.





**Figure 1-2 LAN-to-LAN Application via Frame Relay**

Both Prestiges act as clients when they are connected via a Frame Relay network. When they are connected directly via a leased line for example, then one Prestige must act as a server and the other as a client as shown in the next figure.



**Figure 1-3 LAN-to-LAN Application via Direct Connection**

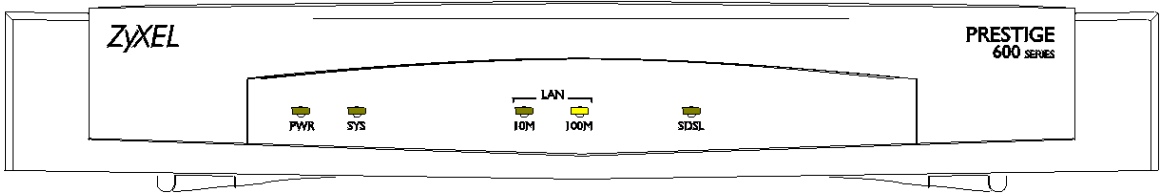


# Chapter 2: Hardware Installation & Initial Setup

*This chapter describes the physical features of the Prestige and how to make the cable connections.*

## 2.1 Front Panel LEDs OF P681

The LED indicators on the front panel indicate the operational status of the Prestige 681. The table below the diagram describes the LED functions:



**Figure 2-1 Prestige 681 Front Panel.**

**Table 2-1 Front Panel LED Description**

<b>PWR</b>	The PWR (power) LED is on when power is applied to the Prestige.
<b>SYS</b>	A steady on SYS (system) LED indicates the Prestige is on and functioning properly while an off SYS LED indicates the system is not ready or a malfunction. The system is rebooting when the SYS LED is blinking.
<b>LAN 10M</b>	A steady <i>green</i> light indicates a 10Mb Ethernet connection. The LED blinks when data is being sent/received.
<b>LAN 100M</b>	A steady <i>yellow</i> light indicates a 100Mb Ethernet connection. The LED blinks when data is being sent/received.
<b>SDSL</b>	The SDSL LED is on when the Prestige is connected successfully to a DSLAM. The LED blinks when the link is still synchronizing—note that this may take up to 10 minutes. The LED is off when the link is down.

## 2.2 Prestige 681 Rear Panel and Connections

The following figure shows the rear panel connections of your Prestige.

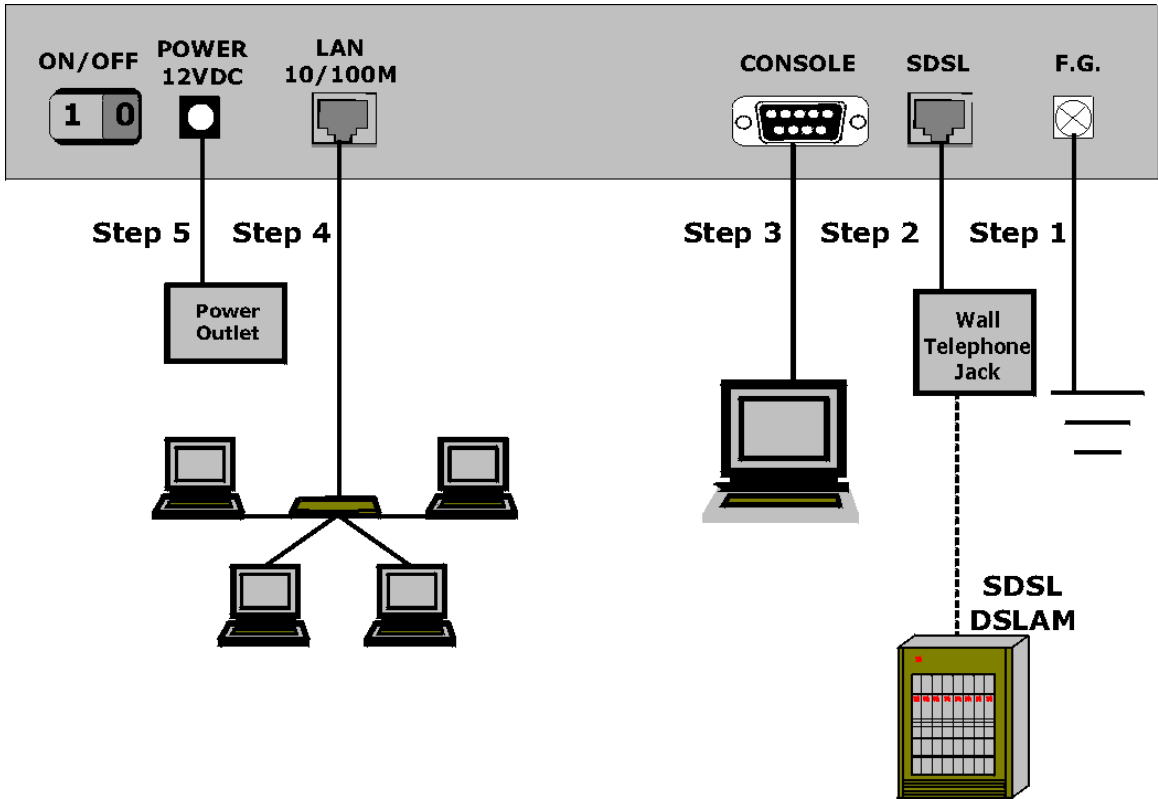


Figure 2-2 Prestige 681 Rear Panel Connections

### Step 1. Grounding the Prestige

Ground the Prestige by connecting a grounded wire to the **F.G.** (Frame Ground) of the Prestige.

### Step 2. Connecting the SDSL Line

Connect the Prestige directly to the telephone jack using the SDSL cable (included).

### Step 3. Connecting the Console Port

For the initial configuration of your Prestige, you need to use terminal emulator software on a workstation and connect it to the Prestige through the console port. Connect the 9-pin end of the console cable (9-pin to

25-pin console cable supplied) to the console port of the Prestige and the 25-pin 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.

#### **Step 4. Connecting a Workstation to the Prestige 10/100M LAN port**

Ethernet 10Base-T networks use Shielded Twisted Pair (STP) cable with RJ-45 connectors that look like a bigger telephone plug with 8 pins. Use the crossover cable (red tag) to connect your Prestige 681 to a computer directly. Use straight through Ethernet cable (white tag) to connect to an external hub and then connect one end of a straight through Ethernet cable (white tag) from the hub to the NIC on the workstation.

#### **Step 5. Connecting the Power Adapter to your Prestige**

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

## **2.3 Additional Installation Requirements**

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

- A computer with Ethernet 10Base-T/100Base-T NIC (Network Interface Card).
- A computer equipped with communications software (for example, Hyper Terminal in Win95) configured to the following parameters:
  - VT100 terminal emulation.
  - 9600 Baud rate.
  - No parity, 8 Data bits, 1 Stop bit.
  - Flow Control set to None

After the Prestige has been successfully connected to your network, you can make future changes to the configuration through telnet application.

## **2.4 Housing**

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

## **2.5 Important Safety Instructions**

The following safety instructions apply to the P681:

1. Be sure to read and follow all warning notices and instructions.

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

- Do not use a telephone or other equipment connected to telephone lines to report a gas leak in the vicinity of the leak.

## 2.6 Power On Your Prestige

At this point, you should have connected the console port, the SDSL line, the Ethernet port and the power port to the appropriate devices or lines. You can now apply power to the Prestige by turning the switch on.

### Step 1. Initial Screen

When you power on your Prestige, it performs several internal tests as well as line initialization.

```
Copyright (c) 1994 - 2000 ZyXEL Communications Corp.  
initialize ch =0, ethernet address: 00:a0:c5:33:86:81  
Start to initialize SDSL.....
```

**Figure 2-3 Power-On Display**

### Step 2. Entering Password

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

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

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

```
Enter Password : XXXX
```

**Figure 2-4 Login Screen**

## 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**

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



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

```

Copyright (c) 1994 - 2000 ZyXEL Communications Corp.
Prestige 681 Main Menu

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

Advanced Applications
11. Remote Node Setup
12. Static Routing Setup
15. SUA Server Setup

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

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 set up general information.
2	WAN Setup	Use this menu to configure the WAN link.
3	Ethernet Setup	Use this menu to set up your LAN connection.
4	Internet Access Setup	A quick and easy way to set up an Internet connection.
11	Remote Node Setup	Use this menu to set up the Remote Node for LAN-to-LAN connection, including Internet connection.
12	Static Routing Setup	Use this menu to set up static routes.
15	SUA Server Setup	Use this menu to specify inside servers when SUA is enabled.
21	Filter Set Configuration	Use this menu to set up filters to provide security, etc.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Password	Use this menu to change your password.
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
99	Exit	To exit from SMT and return to a 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 Password** as shown below.

When the Submenu 23 System Password appears, type in your existing system password, i.e., 1234, and press [ENTER].

```
Menu 23 - System Password
Old Password= ****
New Password= ****
Retype to confirm= ****

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

**Figure 2-6**      **Menu 23.1 - System Password**

**Step 2.** Enter your new system password (up to 30 characters), and press [ENTER].

**Step 3.** Re-type your new system password for confirmation and press [ENTER].

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

## 2.9 Filename conventions

The configuration file (sometimes called the romfile or romfile-0) contains the settings in the menus such as password, DHCP Setup defaults, TCP/IP Setup defaults etc. The external (i.e., not on the Prestige) configuration filename is usually the router model name with a \*.rom extension, e.g., P681.rom. The ZyNOS firmware file (sometimes referred to as the “ras” file) is the file that contains the ZyXEL Network Operating System firmware and the external firmware file is usually called the router model name with a \*.bin extension, e.g., P681.bin. Rename the configuration filename to “rom-0” and the firmware filename to “ras” when transferring files to the Prestige (i.e., the internal filenames on the Prestige). Renaming the files is not necessary when you transfer files to the Prestige using the X-Modem protocol. See *section 11.6 Upload Firmware* on page 11-12 for more information.

The following table is a summary. Please note that the internal filename refers to the filename on the Prestige and the external filename refers to the filename not on the Prestige, i.e., on your workstation, local network or ftp site and so the name (but not the extension) will vary. The AT command is the command you enter after you press “Y” when prompted in the SMT menu to go into debug mode. After uploading new firmware see the **ZyNOS S/W Version** field in **Menu 24.2.1** (*Figure 11-4*) to check you have uploaded the correct firmware version.

**Table 2-4 Filename Conventions**

File Type	Internal Name	External Name	Description	AT Command
<b>Configuration File</b>	Rom-0	*.rom	This is the router configuration filename on the Prestige. Uploading the rom-0 file replaces the entire ROM file system, including your Prestige configurations, system-related data (including the baud rate and default password), the error log and the trace log.	ATLC
<b>Firmware</b>	Ras	*.bin	This is the generic name for the ZyNOS firmware on the Prestige.	ATUR

## 2.9.1 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, you will lose all configurations that you had before and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity and 1 stop bit (8n1). The password will be reset to the default of 1234, also.

Turn off the Prestige and begin a Telnet session with the default console port settings. Turn on the Prestige again. When you see the message "Press Any key to enter Debug Mode within 3 seconds", press any key to enter debug mode. You should already have downloaded the correct file from your nearest ZyXEL FTP site. *See section 11.5 Restore Configuration* on page 11-11 for more information on how to transfer the configuration file to your Prestige.

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

```

Menu 1 - General Setup

System Name= P681
Location= branch
Contact Person's Name= JohnDoe

Route IP= Yes
Route IPX= No
Bridge= No

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

**Figure 2-7 Menu 1 – General Setup**

**Table 2-5 General Setup Menu Fields**

Field	Description	Example
System Name	Choose a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.	P681
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
Protocols :	Press the [SPACE BAR] to toggle on or off routing for the individual protocols.	
Route IP	Set this field to <b>Yes</b> to enable IP routing. You must enable IP routing for Internet access.	<b>Yes/No</b>
Route IPX	Set this field <b>Yes</b> to enable IPX routing.	<b>Yes/No</b>
Bridge	Turn on/off bridge forwarding for protocols not supported (e.g., SNA) or not turned on in the previous Route fields.	<b>Yes/No</b>

### 2.10.1 Note on Bridging

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

## 2.11 Ethernet Setup

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

```
Menu 3 - Ethernet Setup

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

**Figure 2-8**      **Menu 3 - Ethernet Setup**

### 2.11.1 General Ethernet Setup

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

```
Menu 3.1 - General Ethernet Setup

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

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

**Figure 2-9**      **Menu 3.1 - General Ethernet Setup**

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

### 2.12 Protocol Dependent Ethernet Setup

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

- For TCP/IP Ethernet setup *refer to Chapter 4: Internet Access.*
- For Novell IPX Ethernet setup *refer to Section 7.3 - IPX Ethernet Setup in Chapter 7: IPX Configuration.*
- For bridging Ethernet setup *refer to Chapter 8: Bridging Setup.*



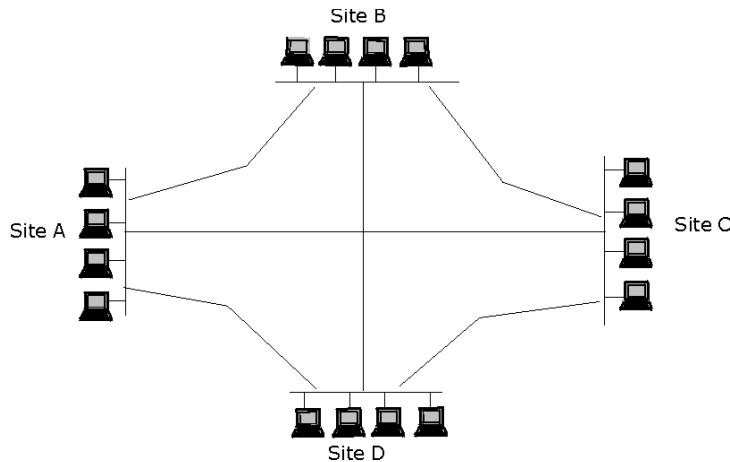
# Chapter 3: WAN Setup

*This chapter helps you set up your WAN link on the Prestige.*

## 3.1 Frame Relay

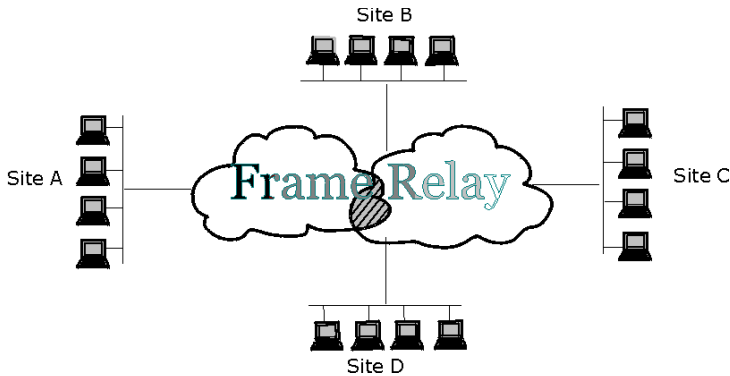
What follows is some background information on frame relay. Please skip to section 3.2 *Setting up the WAN link* to begin configuring your Prestige right away.

Frame relay is a form of packet-switching technology that routes frames of information from source to destination over a switching network owned by a carrier. Suppose a corporate network has 4 sites, site A, site B, site C and site D (as shown in the next figure) and you need to interconnect these sites with both data links and voice lines. As data traffic is relatively continuous throughout the day one solution (though inefficient) would be to set up dedicated leased lines connecting each office as shown in *Figure 3-1*.



**Figure 3-1 Dedicated Leased Lines – Multiple Sites**

The frame relay solution would be to rent short dedicated leased lines to the carrier's frame relay access point and then the carrier programs virtual circuits into the network between your sites.

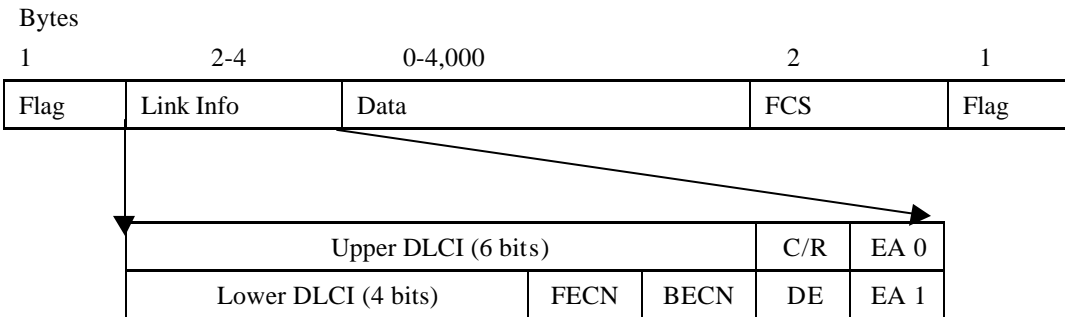


**Figure 3-2 Frame Relay Solution**

Frames are “relayed” through switches in the network, creating basically a virtual private network (VPN) between linked sites. This logical point-to-point circuit between customer sites is called a VC (virtual circuit) of which there are two types. Permanent VCs (PVCs) have constant end points and need to be set up in advance while switched VCs (SVCs) are set up on the fly as needed. The Prestige 681 supports PVCs only.

### 3.1.1 Frame relay frame format

The frame format for frame relay is as follows.



**Figure 3-3 Frame Relay Format**



Each frame is described as follows:

**Table 3-1 Frame Relay Format**

Frame	Description
<b>FLAG</b>	The flag field holds the “Start of frame” marker.
<b>LINK INFO</b>	This field holds the logical connection address and control fields as described here:
<b>DLCI</b>	<b>DLCI (data link connection identifier)</b> identifies the logical connections.
<b>C/R</b>	Command/Response bit related to congestion control.
<b>EA</b>	<b>EA (extended address)</b> is used to extend the header field to support DLCI addresses of more than 10 bits.
<b>FECN</b>	<b>FECN (forward explicit congestion notification)</b> warns receivers about network congestion.
<b>BECN</b>	<b>BECN (backward explicit congestion notification)</b> warns senders about network congestion.
<b>DE</b>	<b>DE (discard eligibility)</b> indicates whether frames can be discarded if the network is congested.
<b>DATA</b>	Control information or encapsulated data goes in this field.
<b>FCS</b>	<b>FCS (FRAME CHECK SEQUENCE)</b> is a checksum used for error detection.
<b>FLAG</b>	This flag field holds the “End of frame” marker.

### 3.1.2 Connection setup

The carrier gives you a specific DLCI (data link connection identifier) for each PVC which is a path number of a portion of the PVC (the DLCI changes for each hop through the network), not the address of the destination. It is a logical identifier with local significance only.

A management protocol called LMI (Local Management Interface) provides information about the status of PVC-to-network access devices. It defines management frames for monitoring the integrity of a link and whether a link is active or not.

The frame-relay network manages congestion by setting bits in frames that warn end devices that there is congestion on the network. A bit called FECN (forward explicit congestion notification) is set to notify a receiving system of congestion and a bit called BECN (backward explicit congestion notification) is set to notify sending devices of congestion. In the latter case, the sending device will temporarily slow down or stop transmissions.

## 3.2 Setting up the WAN link

You configure SDSL and Frame Relay settings in **Menu 2 – WAN Setup**. You need to know the following information.

- Q.1. Is your P681 acting as a SDSL server or as a client (*see Figure 1-1, Figure 1-2 and Figure 1-3*)? If acting as a SDSL server, then select **Server** (Central Office) from the **Service Type** field. If acting as a client, then select **Client** (Remote Terminal) from the **Service Type** field.
- Q.2. Is your SDSL link compatible (**Link Compatibility** field) with **Ascend/Lucent**? This version of the Prestige 681 currently supports Ascend (now part of Lucent) type SDSL routers only<sup>1</sup>.
- Q.3. What is the actual transmission rate? The P681 SDSL router supports symmetrical multi-rate data transmission speeds from 144Kbps up to 2320Kbps. You can increase the capacity of the Internet connection (within certain limitations – *see Table 3-2*) without changing your ISP or buying new equipment. Note that this table outlines the distance limitations only and does not mean that distance determines the actual transmission speed agreed between you and the peer. Both the Prestige and the peer must have the same transmission rate. Press the [SPACEBAR] in the **Transfer Rate** = field to step through the transmission speed options and then press [ENTER] to select the matching transmission speed of the peer.

The following table outlines distance limitations on data transmission rates for AWG 26. AWG (American Wire Gauge) is a measurement system for wire that specifies its thickness. As the thickness of the wire increases, the AWG number decreases and the further you can transmit; the transmission distance is in proportion to the square of the wire gauge (diameter)<sup>2</sup>.

**Table 3-2 SDSL Maximum Transmission Distances (AWG 26, 0.4mm)**

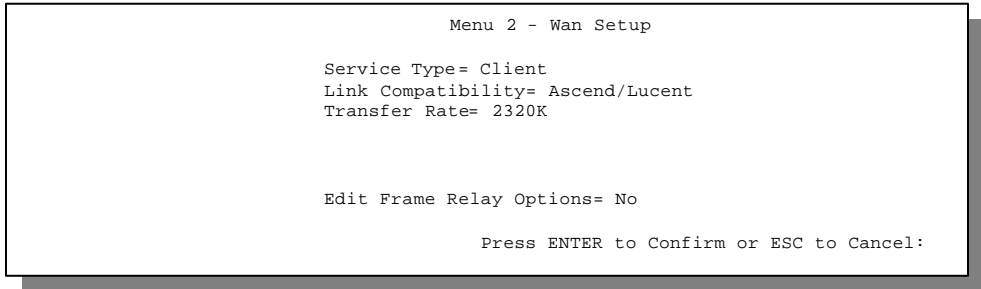
<b>Data Rate</b>	<b>Distance (feet)</b>	<b>(meters)</b>
144K	16,000	4876
272K	14,000	4267
400K	13,000	3962
528K	12,000	3658
784K	11,500	3505
1168K	11,000	3352
1552K	10,000	3048
2320K	7,500	2289

---

<sup>1</sup> Future versions may support other type SDSL routers.

<sup>2</sup> According to the table the maximum distance for a 0.4mm line (without any noise) transmitting at 528Kbps is 12000 ft. If you want to transmit at 528Kbps over a 0.6mm (AWG 24) line the maximum distance you can transmit is  $12000 \times (.6)^2 / (.4)^2 = 27000$  ft or 8,228m (not taking noise factor into account).

If you are unsure of any of this information, please check with your telephone company. Enter 2 from the main menu to open **Menu 2 – WAN Setup**.



**Figure 3-4 Menu 2 – WAN Setup**

The following table describes the fields in this menu.

**Table 3-3 Menu 2 – WAN Setup Fields**

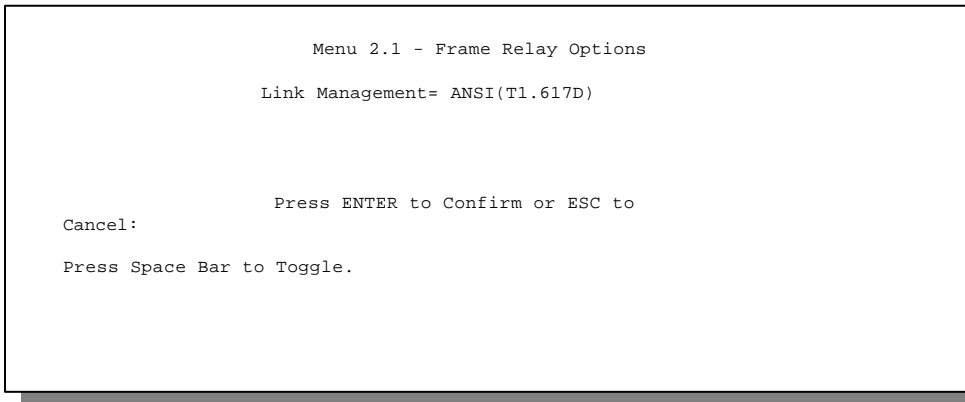
Field	Description	Option
Service Type=	Choose <b>Server</b> if your P681 is acting as a SDSL server and <b>Client</b> if it is acting as a client. Press the [SPACEBAR] to toggle between choices and then press [ENTER] to select.	<b>Server</b> <b>Client</b>
Link Compatibility=	This field is not selectable as this version of the P681 supports <b>Ascend/Lucent</b> type SDSL routers only <sup>1</sup> .	<b>Ascend/Lucent</b>
Transfer Rate=	Press the [SPACEBAR] to step through the transmission speed options and then press [ENTER] to select the matching transmission speed of the peer.	e.g., 784K
Edit Frame Relay Options=	Press the [SPACEBAR] to change <b>No</b> to <b>Yes</b> , then press [ENTER] to go to <b>Menu 2.1 – Edit Frame Relay Options</b> (see the next section).	<b>No</b> <b>Yes</b>

### 3.2.1 Frame Relay Options

Press the spacebar to toggle the default **No** to **Yes** in the **Edit Frame Relay Options=** field in Figure 3-4 to display **Menu 2.1 - Frame Relay Options**.

## Standards

The two main groups that create recommendations and standards in the telecommunications field are ITU – T (International Telecommunication Union – Telecommunications Standardization Sector) and ANSI (American National Standards Institute). Standards vary slightly for both organizations, so please select the correct organization in the **Link Management** field in menu 2.1. Your Network Service Provider (NSP) should provide you with this information.



**Figure 3-5**      **Menu 2.1 - Frame Relay Options**

**Table 3-4**      **Menu 2.1 - Frame Relay Options Fields**

<b>Field</b>	<b>Description</b>	<b>Options</b>
Link Management=	This function is responsible for monitoring the up/down status and error performance of an individual link. If failure occurs, it also initiates recovery actions for the restoration of the failed link. Press the [SPACEBAR] and then [ENTER] to select which standard is compatible with your Prestige. Both the Prestige and the peer must use the same standard.	<b>ITU-T(Q.933A)</b> <b>ANSI(T1.617D)</b>

# Chapter 4: Internet Access

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

## 4.1 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.

## 4.2 TCP/IP Parameters

### 4.2.1 IP Address and Subnet Mask

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

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

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

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

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

## 4.2.2 Private IP Addresses

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

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

For this reason, it is recommended that you choose your network number from the above list.

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

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

## 4.2.3 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 an unusual network topology.

Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP

packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

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

## 4.2.4 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. The Prestige can also act as a surrogate DHCP server where it relays IP address assignment from the actual DHCP server to the clients.

### IP Pool Setup

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

### DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, e.g., the IP address of *www.zyxel.com* is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. 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**, otherwise, leave them blank.

Some ISPs 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.

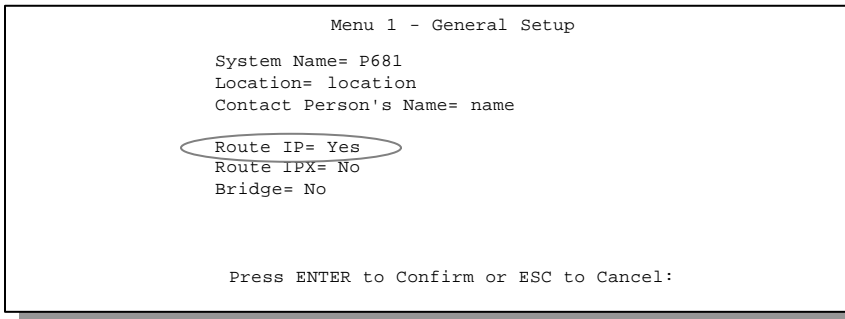
Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you

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.

### 4.3 Route IP Setup

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

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



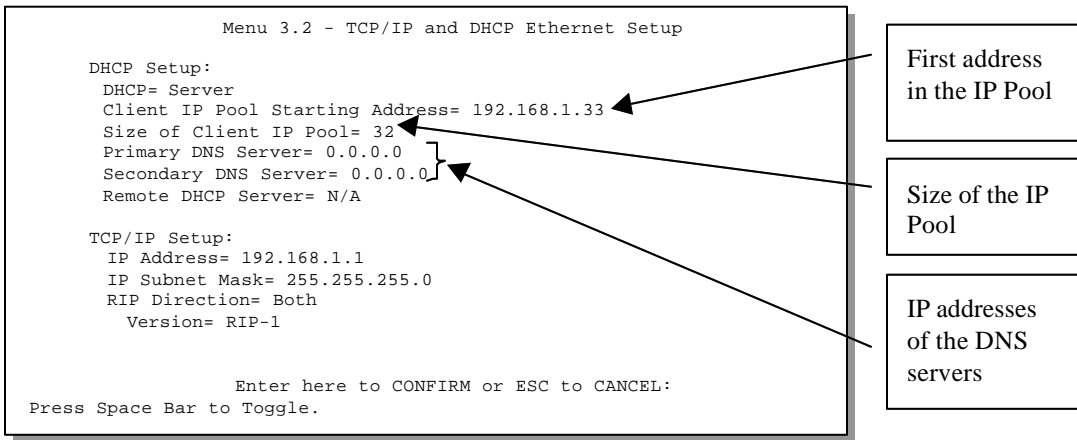
**Figure 4-1**      **Menu 1 – General Setup**

### 4.4 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, enter 3 to open the **Menu 3 - Ethernet Setup** from 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 4-2 Menu 3.2 – TCP/IP and DHCP Ethernet Setup**

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

**Table 4-1 DHCP Ethernet Setup Menu Fields**

Field	Description	Example
DHCP Setup		
DHCP=	If this field is set to <b>Server</b> , your Prestige can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. 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 DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the <b>Remote DHCP Server</b> in this case. When DHCP is used, the following items need to be set:	<b>None Server</b> (default) <b>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	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	
Secondary DNS Server		
Remote DHCP Server	If <b>Relay</b> is selected in the <b>DHCP=</b> field above, 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 4-2 TCP/IP Ethernet Setup Menu Fields**

Field	Description	Example
TCP/IP Setup		
IP Address	Enter the (LAN) IP address of your Prestige in dotted decimal notation	192.168.1.1 (default)
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige	255.255.255.0
RIP Direction	Press the [SPACE BAR] to select the RIP direction from <b>Both/In Only/Out Only</b> or <b>None</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)
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm...] to save your configuration, or press [Esc] at any time to cancel.		

## 4.5 LANs & WANs

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

### 4.5.1 LANs, WANs and the Prestige

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

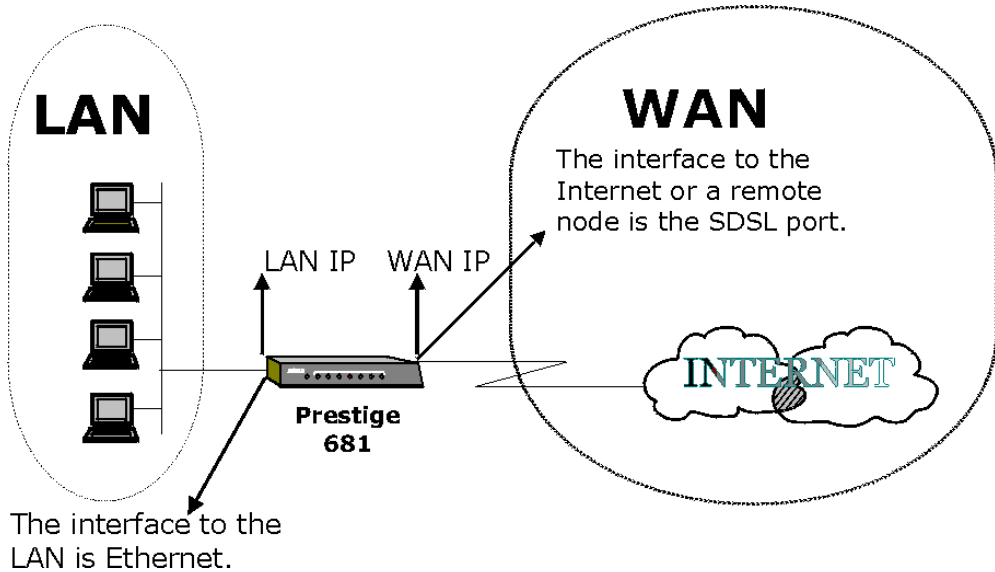


Figure 4-3 LAN & WAN IPs

## 4.6 Encapsulation

**Note: The P681 must reboot when the Encapsulation method is changed in Menu 4 or Menu 11.1**

### 4.6.1 RFC 1490

RFC 1490 describes Multiprotocol over Frame Relay encapsulation which is an encapsulation method for carrying network interconnect traffic (both bridging and routing) over a frame relay backbone. It also describes a simple fragmentation procedure for carrying large frames over a frame relay network with a smaller MTU (Maximum Transmission Unit).

### 4.6.2 PPP

RFC 1662 defines PPP over HDLC (High-level Data Link Control). HDLC is a bit-oriented, (meaning that the data is monitored bit by bit) link layer protocol for the transmission of data over synchronous networks. Transmissions consist of binary data without any special control codes. Information in the frame contains control and response commands, however. HDLC supports full-duplex transmission in which data is transmitted in two directions at the same time, resulting in higher throughput. HDLC is suitable for point-to-point and multipoint (multidrop or one-to-many) connections.

## 4.7 DLCI

The carrier gives you a specific DLCI (data link connection identifier) for each PVC which is a path number of a portion of the PVC (the DLCI changes for each hop through the network), not the address of the destination. It is a logical identifier with local significance only. Identifiers can range from 1 to 1023 with restrictions shown in the following table. The default DLCI for the P681 is 16 when you choose RFC 1490 encapsulation and N/A (not applicable) for PPP encapsulation.

**Table 4-3 Data Link Connection Identifiers**

DLCI	Usage
0	Channel signaling
1-15	Reserved
16 – 1007	Frame Relay
1008 – 1022	Reserved
1023	LMI

## 4.8 Internet Access Configuration

Menu 4 allows you to enter the Internet Access information in one screen. Menu 4 is actually a simplified setup for the remote node 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 and telephone company. Use the following table to record your Internet Account Information.

**Table 4-4 Internet Account Information**

Internet Account Information	Write your account information here
Telephone Company Information	
DLCI (see section 4.7 above)	—
ISP Information	
Login Name	—
Password for ISP authentication	—
Link Compatibility (see page 3-4, Q.2)	

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

```

Menu 4 - Internet Access Setup

ISP Name= myISP
Encapsulation= rfc 1490

DLCI= 16

My Login= kitty
My Password= *****
Single User Account= No
IP Address= N/A

Press ENTER to confirm or ESC to cancel:

```

Get this information from the telephone company. Get the other information from your ISP.

**Figure 4-4 Internet Access Setup**

**Table 4-5 Internet Access Setup Menu Fields**

<b>Field</b>	<b>Description</b>	<b>Options/E.G.</b>
ISP Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.	<b>e.g., MyISP</b>
Encapsulation <sup>3</sup>	Press the [Spacebar] to select the method of encapsulation used by your ISP. DLCI is N/A for PPP encapsulation. Please <i>see section 4.6</i> for more information.	<b>RFC 1490</b> <b>PPP</b>
DLCI	Enter the DLCI (Data Link Connection Identifier) that the carrier gave you. The default DLCI for the P681 is 16 using RFC 1490 encapsulation. <i>See section 4.7</i> for more information.	<b>e.g., 16</b>
My Login	Enter the login name that your ISP gives you.	<b>e.g., kitty</b>
My Password	Enter the password associated with the login name above.	<b>*****</b>
Single User Account	Press the spacebar to enable or disable SUA. Please see the following section for a more detailed discussion on the Single User Account feature.	<b>Yes/No</b>
IP Address	Enter the IP address supplied by your ISP if applicable i.e., if you enabled SUA. <i>See Table 4-6 Single User Account Menu Fields</i> for more information in this case.	<b>e.g.,</b> <b>192.168.1.100</b>

At this point, if all your settings are correct your Prestige should connect automatically to the Internet. If the connection fails, note the error message that you receive on the screen and take the appropriate troubleshooting steps.

## 4.9 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

---

<sup>3</sup> Note: You must reboot the Prestige when you change the Encapsulation method in Menu 4 or Menu 11.

your ISP before you enable this feature). SUA supports popular Internet applications such as MS traceroute, CuSeeMe, IRC, RealAudio, VDOLive, Quake and PPTP with no extra configuration needed.

The IP address for the SUA can be either fixed or dynamically assigned by the ISP. In addition, you can designate servers, e.g., a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any server, SUA offers the additional benefit of firewall protection. If no server is defined, all incoming inquiries will be filtered out by your Prestige, thus preventing intruders from probing your network. Your Prestige accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. For more information on IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

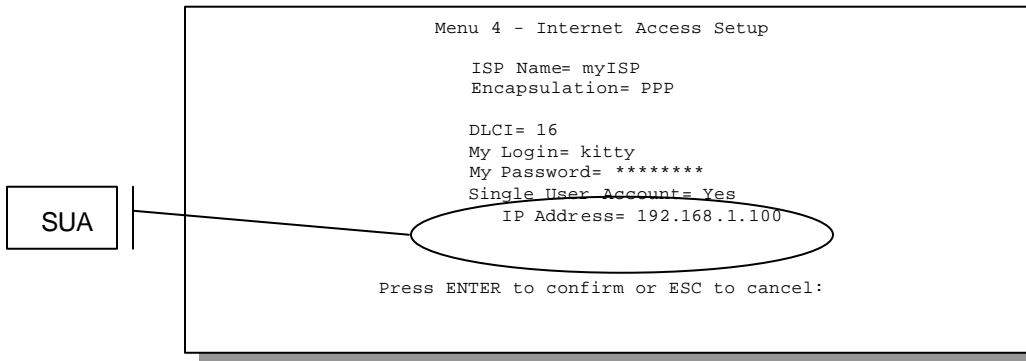
### **4.9.1 Advantages of SUA**

In summary:

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

### **4.9.2 Single User Account Configuration**

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



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

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

**Table 4-6 Single User Account Menu Fields**

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

## 4.10 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 (see the following figure), if you have a web server at 192.168.1.36 and an FTP server 192.168.1.33, then you need to specify for port 80 (web) the server at IP address 192.168.1.36 and for port 21 (FTP) another at IP address 192.168.1.33.

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



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

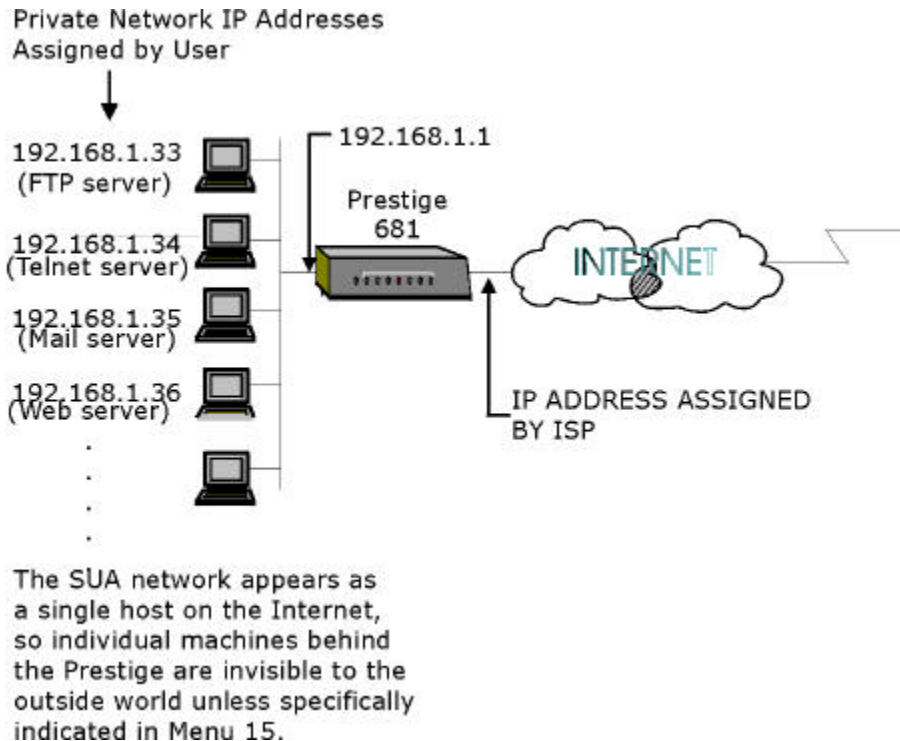


Figure 4-6 Example of Multiple Servers behind SUA

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**.

### 4.10.1 Configuring a Server behind SUA

Follow the steps below to configure a server behind SUA:

- Step 1.** Enter 15 in the main menu to go to **Menu 15 - Multiple Server Configuration**.
- Step 2.** Enter an index number in menu 15 to go to **Menu 15.1 - SUA Server Configuration**.
- Step 3.** Enter the service port number in the **Port #** field and the inside IP address of the server in the **IP Address** field.

```
Menu 15 - Multiple Server Configuration
Port #           IP Address
-----
1.Default       192.168.1.33
2.21            192.168.1.34
3.23            192.168.1.35
4.25            192.168.1.36
5.80            192.168.1.37
6. 0            0.0.0.0
7. 0            0.0.0.0
8. 0            0.0.0.0

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

**Step 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 4-7 Multiple Server Configuration**

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to our PNC Disk for more examples and details on SUA.

**Table 4-7 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 5: Remote Node Configuration

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

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 a remote node.

## 5.1 Remote Node Setup

This section describes the protocol-independent parameters for a remote node. Menu 4 (discussed previously – see *Figure 4-4*) is actually a simplified setup for the remote node that you can access in Menu 11.

### 5.1.1 Remote Node Profile

To configure a remote node, do the following:

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

When **Menu 11.1 - Remote Node Profile** appears fill in the fields as described in the table that follows to define this remote profile. The Remote Node Profile Menu Fields table (*Table 5-1*) shows you how to configure the Remote Node Menu (*Figure 5-1*).

```

Menu 11.1 - Remote Node Profile

Rem Node Name= nodename      Route= None
Active= Yes                  Bridge= Yes

Encapsulation= RFC 1490     Edit PPP Options= N/A
Incoming:                   Rem IP Addr= 192.168.2.1
  Rem Login= N/A             Edit IP/IPX/Bridge= No
  Rem Password=N/A
Outgoing:                   Session Options:
  My Login= N/A              Edit Filter Sets= No
  My Password= N/A
  Authen= N/A

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

Enter a unique name of less than 8 characters for the remote name.

Enter the IP address of the remote gateway here.

**Figure 5-1 Menu 11.1 Remote Node Profile**

**Table 5-1 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.	
Active	Press the spacebar 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.	<b>Yes/No</b>
Encapsulation= <sup>3</sup>	Press the spacebar to select the method of encapsulation used by your ISP. Please see <i>section 4.6</i> for more information.	<b>RFC 1490 PPP</b>
Incoming: <sup>4</sup> Rem 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 Password	Enter the password used when this remote node calls your Prestige.	
Outgoing: <sup>4</sup> My Login	Enter the login name for your Prestige when it calls this remote node.	

<sup>4</sup> All Incoming and Outgoing fields are not applicable (N/A) for RFC 1490.

Field	Description	Options
Outgoing: My Password Outgoing: Authen	Enter the password for your Prestige when it calls this remote node.  This field sets the authentication protocol used for outgoing calls.  Options for this field are: <ul style="list-style-type: none"> <li>● <b>CHAP/PAP</b> - Your Prestige will accept either CHAP or PAP when requested by this remote node.</li> <li>● <b>CHAP</b> - accept CHAP only.</li> <li>● <b>PAP</b> - accept PAP only.</li> <li>● <b>None</b> – no authentication protocol is used for outgoing calls.</li> </ul>	<b>CHAP/PAP</b>  <b>CHAP</b> <b>PAP</b> <b>None</b>
Route	This field determines the protocols that your Prestige will route.	<b>IP, IPX, IP+IPX, None</b>
Bridge	Bridging is used for protocols that the Prestige does not support, e.g., SNA, or not turned on in the previous Route field. When bridging is enabled, your Prestige will forward any packet that it does not route to this remote node; otherwise, the packets are discarded. .	Press [SPACE BAR] to toggle <b>Yes/No</b>
Edit PPP Options	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 <b>Menu 11.2 - Remote Node PPP Options</b> . For more information on configuring PPP options, see <i>section 5.1.3</i> Editing PPP Options.	Press [SPACE BAR] to toggle to <b>Yes</b> and then press [ENTER]
Rem IP Addr	Enter the IP address of the remote gateway here. If you don't know this IP, then enter 0.0.0.0 .	
Edit IP/IPX/Bridge	Press the [SPACE BAR] to toggle this field to <b>Yes</b> and then press [ENTER] to go to <b>Menu 11.3 - Remote Node Network Layer Options</b> menu.	<b>Yes or 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= <b>No</b>
Once you have completed filling in Menu 11.1 – Remote Node Profile, press [ENTER] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] at any time to cancel.		

## 5.1.2 Outgoing Authentication Protocol

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

## 5.1.3 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 toggle this field to **Yes**. Press [ENTER] to open Menu 11.2, as shown next.

```

Menu 11.2 - Remote Node PPP Options

Encapsulation= Standard PPP
Compression= No

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

**Figure 5-2 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 5-2 Remote Node PPP Options Menu Fields**

Field	Description	Option
Encapsulation	Select the CISCO PPP only when this remote node is a Cisco machine; otherwise, select the Standard PPP.	<b>Standard PPP</b> <b>CISCO PPP</b>
Compression	Turn on/off Stac Compression. The default for this field is <b>No</b> .	<b>Yes/No</b> (Default = <b>No</b> )
Once you have completed filling in Menu 11.2 – Remote Node PPP Options, press [ENTER] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] at any time to cancel.		

## 5.1.4 Remote Node Filter

Use **Menu 11.5 – Remote Node Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige. You can specify up to 4 filter sets separated by comma, e.g., 1, 5, 9, 12, in each filter field.

Note that spaces are accepted in this field. For more information on defining the filters, *see Chapter 9: Filter Configuration*.

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters= 3
  device filters=
Output Filter Sets:
  protocol filters= 1
  device filters=

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

**Figure 5-3**      **Menu 11.5 – Remote Node Filter**



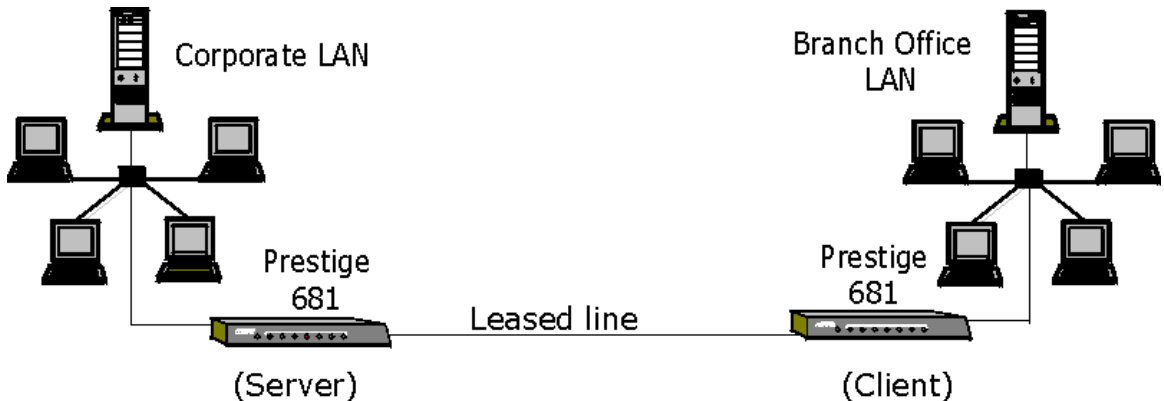


# Chapter 6: Remote Node TCP/IP Configuration

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

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

## 6.1 LAN-to-LAN Application



**Figure 6-1 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.

### 6.1.1 Editing TCP/IP Options

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

In Menu 11.1, move the cursor to the **Edit IP/IPX/Bridge**, 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

Frame Relay Parameters :
  DLCI= 16
IP Options :
  Rem IP Addr: 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  Single User Account= No
  Metric= 2
  Private= No
  RIP Direction= Both
  Version= RIP-2B
  Hop Count= 1
  Tick Count= 2
  Bridge Options:
    Ethernet Addr Timeout(min)= 0

IPX Options :
  Rem LAN Net #= 00000000
  My WAN Net #= 00000000

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

Get this information from your telephone company.

Figure 6-2 Menu 11.3

The following diagram shows some sample IP addresses to help you to understand the field of **My Wan Addr** in Menu 11.3. Refer to Figure 4-3 LAN & WAN I for a brief review of what a WAN IP is. **My WAN Addr** indicates the local Prestige WAN IP while **Rem IP Address** indicates the peer WAN IP.

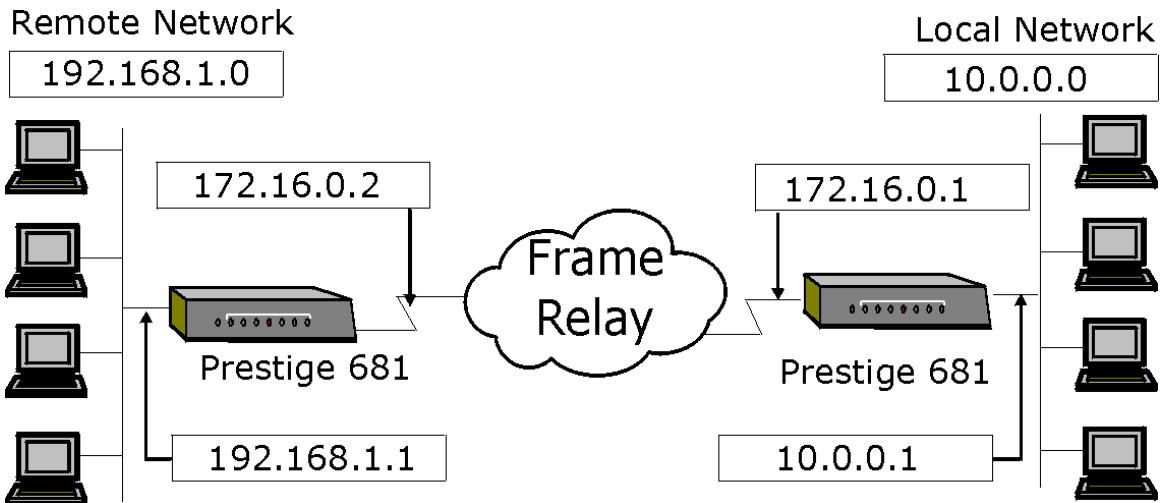


Figure 6-3 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection

To configure the TCP/IP parameters of a remote node, first configure these fields in **Menu 11 – Remote Node Profile**, as shown in the next table.

**Table 6-1 TCP/IP related fields in Menu 11.1 - Remote Node Profile**

Field	Description	Option
Route	Make sure <b>IP</b> is among the protocols in the [Route] field in <b>Menu 11.1 - Remote Node Profile</b> .	<b>IP</b>
Rem IP Address	Enter the IP address of the remote gateway in <b>Menu 11.1 - Remote Node Profile</b> . You must fill in either the remote Prestige WAN IP address or the remote Prestige LAN IP address. This depends on the remote router's WAN IP i.e., for the (remote) Prestige, the <b>My WAN Addr</b> settings in <b>Menu 11.3 – Remote Node Network Layer Options</b> . For example (see <i>Figure 6-3</i> ), if the remote WAN IP is set to 172.16.0.2 (the remote router's WAN IP), then you should enter 172.16.0.2 in the <b>Rem IP Address</b> field. If the remote WAN IP is 0.0.0.0, then enter 192.168.1.1 (the remote router's LAN IP) in the <b>Rem IP Address</b> field).	
Edit IP	Press the [SPACE BAR] to toggle this field to <b>Yes</b> and then press [ENTER] to go to <b>Menu 11.3 - Remote Node Network Layer Options</b> menu.	<b>Yes (Yes/No)</b>

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

**Table 6-2 TCP/IP Remote Node Configuration**

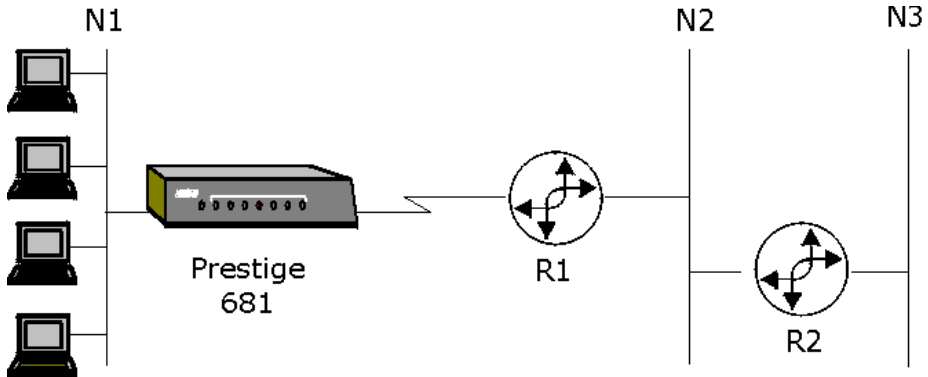
Field	Description	Option
Rem IP Address	This will show the IP address you entered for this remote node in the previous menu.	
Rem IP Subnet Mask	Enter the subnet mask for the remote network.	
My WAN Addr	Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your Prestige.  Note that this is the address assigned to your local Prestige WAN, not the remote router. If the remote router is a Prestige, then this entry determines the local Prestige <b>Rem IP Address</b> in menu 11.1 (see <i>Table 6-1</i> above).	
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 4: Internet Access</i> for more information on the	<b>Yes/No</b>

Field	Description	Option
	Single User Account feature.	
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 Direction=  Version=	Press the [SPACE BAR] to select the <b>RIP direction</b> from <b>Both/In Only/Out Only</b> or <b>None</b> .  Press the [SPACE BAR] to select the RIP version from <b>RIP-1/RIP-2B/RIP-2M</b> .	(Default= <b>Both</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.		

### 6.1.2 Static Route Setup

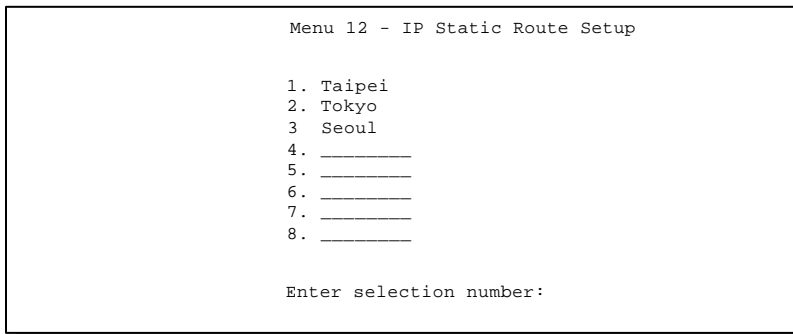
Static routes tell the Prestige routing information that it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN or a remote network is beyond the one that is directly connected to a remote node.

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



**Figure 6-4 Example of Static Routing Topology**

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



**Figure 6-5 Menu 12 - IP Static Route Setup**

From Menu 12, enter the index of the static route you wish to edit to open **Menu 12.1 -Edit IP Static Route**.

```

Menu 12.1 - Edit IP Static Route

Route #: 1
Route Name= Taipei
Active= Yes
Destination IP Address= 10.255.255.1
IP Subnet Mask= 255.0.0.0
Gateway IP Address= 172.31.255.1
Metric= 3
Private= Yes

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

**Figure 6-6 Edit IP Static Route**

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

**Table 6-3 Edit IP Static Route Menu Fields**

Field	Description
Route #	This is the route index number chosen in Menu 12.
Route Name	Enter a descriptive name for this route. This is for identification purposes only.
Active	Press the [SPACEBAR] to activate ( <b>Yes</b> ) or deactivate ( <b>No</b> ) 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.
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 7: IPX Configuration

*This chapter shows you how to configure the IPX parameters of the Prestige 681.*

## 7.1 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.

### 7.1.1 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 681, we recommend that you set up a NetWare server as a seed router. Even though the Prestige 681 is capable as a seed router, a NetWare server offers a much more extensive facility for network management.

### 7.1.2 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.

### 7.1.3 External Network Number

Each of the four logical networks (based on frame type) has its own external network number (see Figure 7-1).

### 7.1.4 Internal Network Number

In addition to the external network numbers, each NetWare server has its own internal network number that is a virtual network to which the server is attached. It is important to remember that every network number must be unique for that entire internetwork, either internal or external (see Figure 7-1).

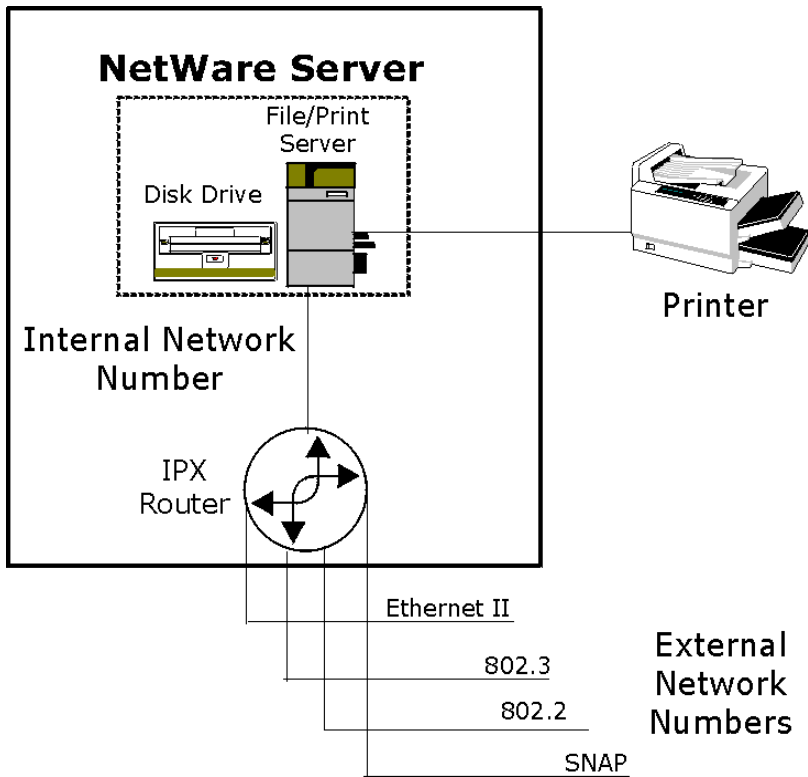


Figure 7-1 NetWare Network Numbers



## 7.2 Prestige 681 in an IPX Environment

There are two scenarios in which your Prestige 681 is deployed, depending on whether there is a NetWare server on the LAN, as depicted in the following diagram.

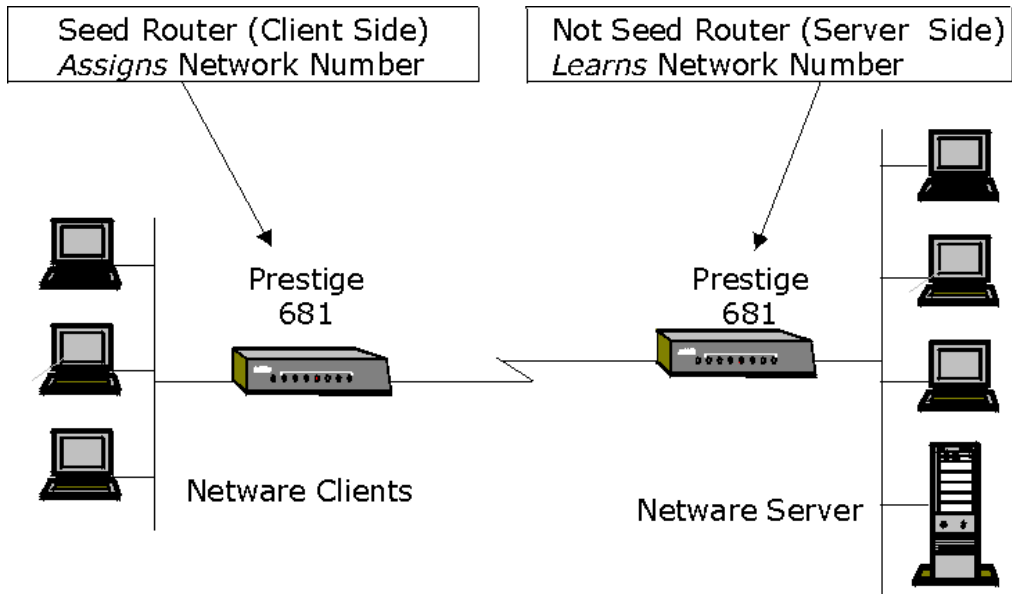


Figure 7-2 Prestige 681 in an IPX Environment

### 7.2.1 Prestige 681 on LAN with Server

If your Prestige 681 is on a LAN with a seed router, you do not need to configure the LAN network numbers. Your Prestige 681 will learn the network number from the seed router and add the routes to its routing table.

### 7.2.2 Prestige 681 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 681 as a seed router and set up unique network numbers for each frame type enabled using the Ethernet Setup Menu.

## 7.3 IPX Ethernet Setup

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

```

Menu 3.3 - Novell IPX Ethernet Setup

Seed Router= No

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

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

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

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

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

**Figure 7-3 Menu 3.3 - Novell IPX Ethernet Setup**

The following table describes the Novell IPX Ethernet Setup Menu.

**Table 7-1 Novell IPX Ethernet Setup Fields**

Field	Description	Options
Seed Router	Determine if your Prestige 681 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 681 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.		

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

A typical LAN-to-LAN application is to use your Prestige 681 to call from a branch office to the corporate headquarters to enable the stations in the branch office to access the NetWare servers at the headquarters, as depicted in the figure below.

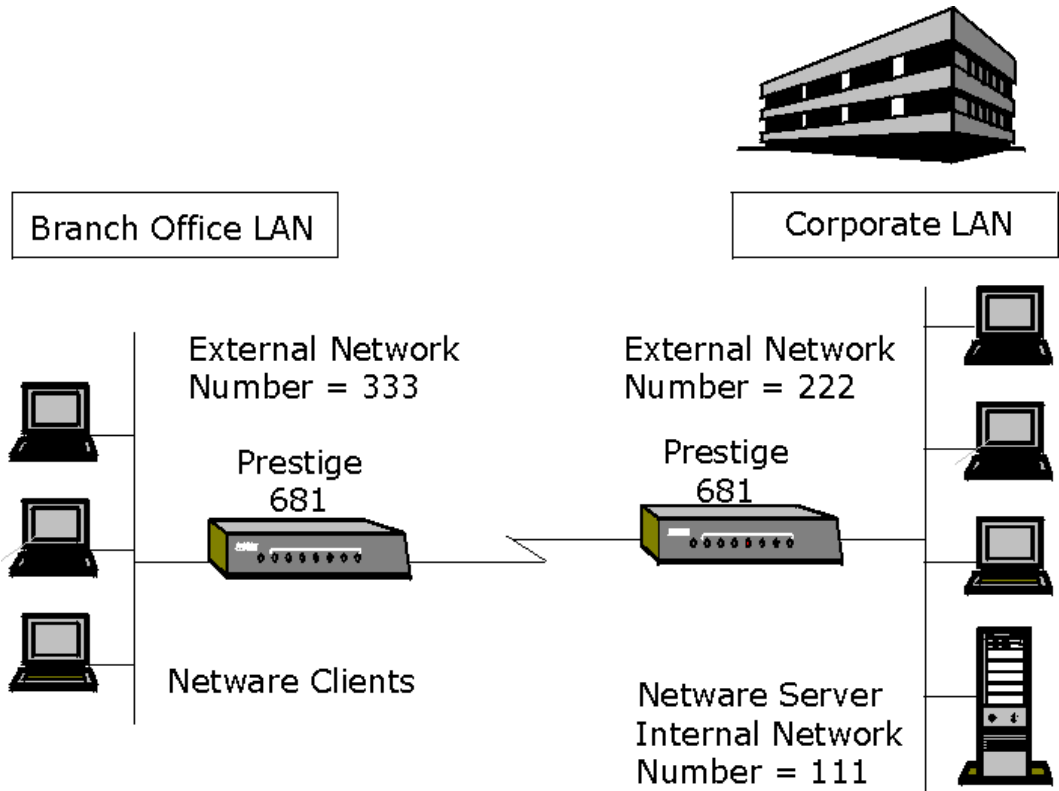


Figure 7-4 LAN-to-LAN Application with Novell IPX

## 7.4.1 IPX Remote Node Setup

Follow the procedure in Chapter 5: to configure the protocol-independent parameters in **Menu 11.1 - Remote Node Profile**. For the IPX-specific parameters in **Menu 11.3 - Remote Node Network Layer Options** follow the instructions below.

- 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 toggle this field to **Yes** and press [ENTER] to open **Menu 11.3 - Network Layer Options**.

```
Menu 11.3 - Remote Node Network Layer Options

Frame Relay Parameters :
  DLCI= 16
  IP Options:
  Rem IP Addr= N/A
  Rem Subnet Mask= N/A
  My WAN Addr= N/A
  Single User Account= N/A
  Metric= N/A
  Private= N/A
  RIP Direction= N/A
  Version= N/A

IPX Options:
  Rem LAN Net #= 00000000
  My WAN Net #= 00000000
  Hop Count= 1
  Tick Count= 2

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

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

**Figure 7-5** Menu 11.3 - Remote Node Novell IPX Options

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

**Table 7-2 Remote Node Novell IPX Options**

<b>Field</b>	<b>Description</b>	<b>Option</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 WAN 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)
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.		

## 7.4.2 IPX Static Route Setup

Similar to IP, IPX static routes tell the Prestige 681 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 #= 11
Server Name= ?
Active= Yes
Network #= ?
Node #= 000000000001
Socket #= 0451
Type #= 0004
Hop Count= 2
Tick Count= 3
Gateway Node= 1

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

**Figure 7-6**      **Menu 12.2 - Edit IPX Static Route**

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

**Table 7-3 Edit IPX Static Route Menu Fields**

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





# Chapter 8: Bridging Setup

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

## 8.1 Bridging in General

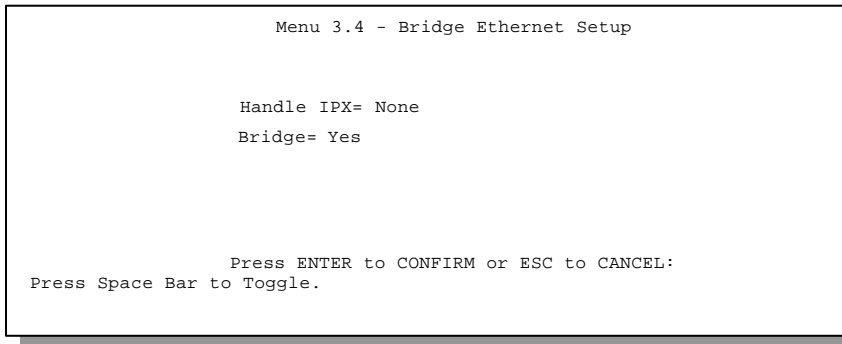
Bridging bases the forwarding decision on the MAC (Media Access Control), or hardware address, while routing does it on the network layer (IP or IPX) address. Bridging allows the Prestige 681 to transport packets of network layer protocols that the Prestige 681 does not route, e.g., SNA, from one network 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 reasons, 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 681 can route.

## 8.2 Bridge Ethernet Setup

Basically, all non-local packets are bridged to the WAN; however, your Prestige 681 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 4 to bring up **Menu 3.4 - Bridge Ethernet Setup** as shown next.



**Figure 8-1 Menu 3.5 - Bridge Ethernet Setup**

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

**Table 8-1 Bridge Ethernet Setup Menu - Handle IPX Field Configuration**

Field	Description
<b>Handle IPX Field</b>	Press the [SPACE BAR] to toggle between the options for this field.  <b>None</b> When there is no IPX traffic on the LAN or when you do not want to apply any special handling for IPX.  <b>Client</b> When there are only client workstations on the LAN. RIP and SAP (Service Advertising Protocol) response packets will not trigger calls.  <b>Server</b> 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 681 will reply to watchdog messages from the servers on behalf of remote clients. The period of time that your Prestige 681 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.
<b>Bridge</b>	Press the [SPACE BAR] to select <b>Yes</b> to activate the bridge on the LAN interface. Make sure that the <b>Bridge</b> field in Menu 1 (see <i>Figure 2-7</i> ) is also set to <b>Yes</b> .

## 8.2.1 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 set up **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 toggle this field to **Yes** and press [ENTER] to open **Menu 11.3 - Network Layer Options**.

```

Menu 11.3 - Remote Node Network Layer Options

Frame Relay Parameters :
  DLCI= 16
IP Options :
  Rem IP Addr= 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  Single User Account= No
  Metric= 2
  Private= No
  RIP Direction= Both
  Version= RIP-2B

IPX Options :
  Rem LAN Net #= 00000000
  My WAN Net #= 00000000
  Hop Count= 1
  Tick Count= 2

Bridge Options:
  Ethernet Addr Timeout(min)= 0

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

**Figure 8-2 Menu 11.3 - Remote Node Bridging Options**

The following table describes the bridging-specific parameters in **Menu 11.1 - Remote Node Profile** and **Menu 11.3 - Remote Node Network Layer Options**.

**Table 8-2 P681 Remote Node Network Layer Menu Bridge Options**

Field	Description
Bridge (menu 11.1)	Make sure this field is set to <b>Yes</b> .
Edit IP/IPX/Bridge (menu 11.1)	Press the [SPACE BAR] to change the default to <b>Yes</b> and then press [ENTER] to go to <b>Menu 11.3 - Network Layer Options</b> .
Ethernet Addr Timeout (min) (menu 11.3)	In this field, enter the time (number of minutes) that you wish your Prestige 681 to retain the Ethernet Addr information in its internal tables while the line is down. If this information is retained, your Prestige 681 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.

## 8.3 Bridge Static Route Setup

Similar to network layer static routes, a bridging static route tells the Prestige 681 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 below.

```
Menu 12.3.1 - Edit Bridge Static Route

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

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

**Figure 8-3**      **Menu 12.3 - Bridge Static Route Setup**

```
Menu 12.3 - Bridge Static Route Setup

1. _____
2. _____
3. _____
4. _____

Enter selection number:
```

**Figure 8-4**      **Menu 12.3.1 - Edit Bridge Static Route**

The following table describes the Bridge Static Route Menu.

**Table 8-3 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.
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 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 divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. These filters are further subdivided into device and protocol filters, which are discussed later.

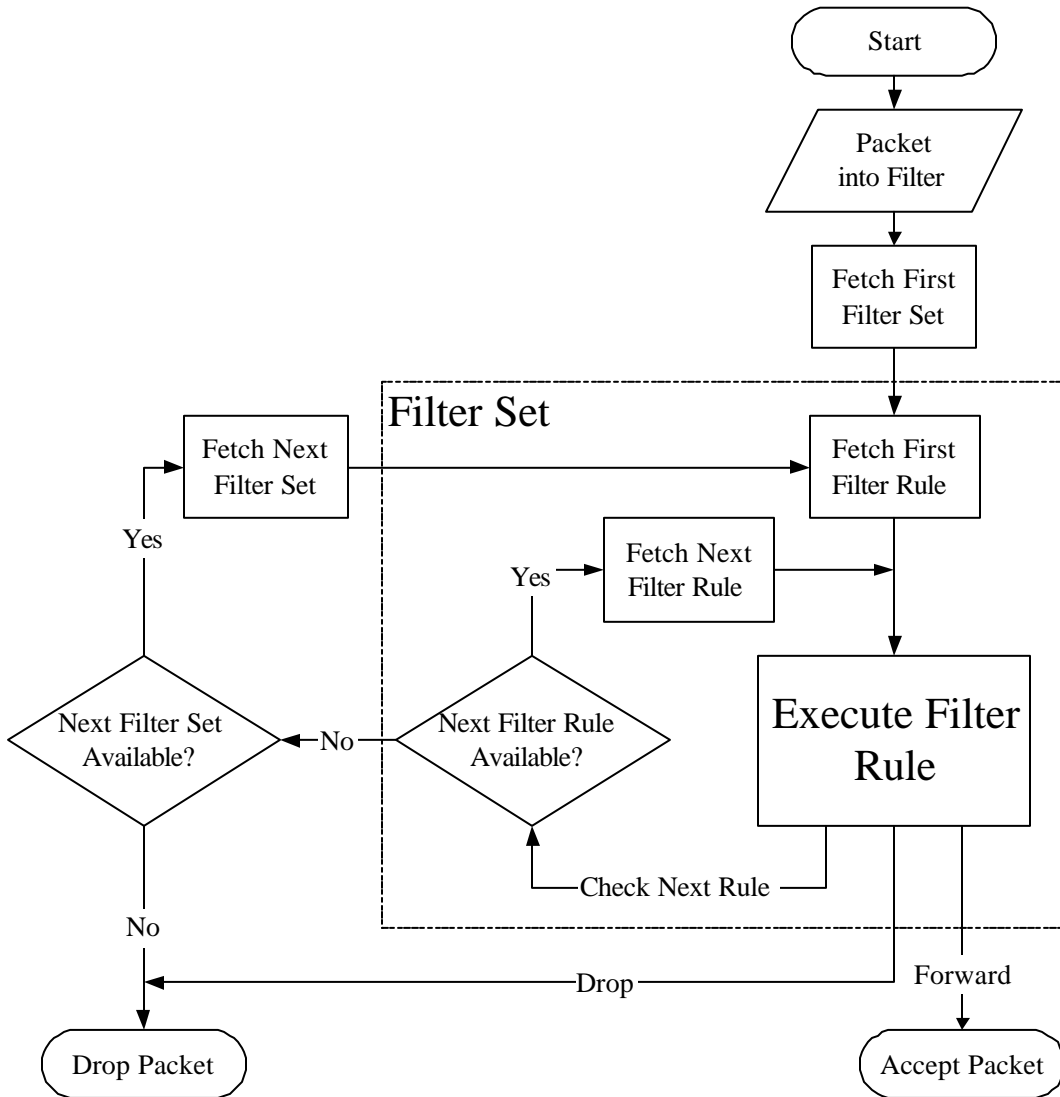
The following sections describe how to configure filter sets.

### The Filter Structure of the Prestige

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

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

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



**Figure 9-1 Filter Rule Process**

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



## 9.2 Configuring a Filter Set

To configure a filter sets, follow this procedure:

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

```

Menu 21 - Filter Set Configuration

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

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

```

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

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

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

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

```

Menu 21.1 - Filter Rules Summary

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

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

Edit Comments= NetBIOS_WAN

Press ENTER to Confirm or ESC to Cancel:
Enter Filter Rule Number (1-6) to Configure:

```

**Figure 9-3 NetBIOS\_WAN 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 Y
3 Y
4 Y
5 Y
6 Y

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

**Figure 9-4** NetBIOS\_LAN Filter Rules Summary

```
Menu 21.3 - Filter Rules Summary

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

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

**Figure 9-5** Telnet Filter Rules Summary

### 9.2.1 Filter Rules Summary Menu

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

**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, IP for TCP/IP	[GEN] for Generic [IP] for TCP/IP
Filter Rules	The filter rule parameters are displayed here (see below).	
M	Refers to More. [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. [N] means you can now specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked. If More is <b>Yes</b> , then <b>Action Matched</b> and <b>Action Not Matched</b> will be <b>N/A</b>	[Y] [N]
m	Refers to <b>Action Matched</b> . [F] means to forward the packet immediately and skip checking the remaining rules.	[F] means to forward the packet. [D] means to drop the packet. [N] means check the next rule.
n	Refers to <b>Action Not Matched</b> . [F] means to forward the packet immediately and skip checking the remaining rules.	[F] means to forward the packet. [D] means to drop the packet. [N] means check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

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

- Abbreviations Used If Filter Type Is IPX

**Table 9-3 Abbreviations Used If Filter Type Is IPX**

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

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

**Table 9-4 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 three types of filter rules: **TCP/IP**, **IPX** and **Generic**. Depending on the type of rule, the parameters below the type will be different. Use the [SPACE BAR] to select the type of rule that you wish to create in the **Filter Type** field and press [ENTER] to open the respective menu.

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.

### 9.3.1 TCP/IP Filter Rule

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

To configure a TCP/IP rules, select TCP/IP Filter Rule from the Filter Type field and press [ENTER] to open **Menu 21.1.1 - TCP/IP Filter Rule**, as shown 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= Check Next Rule
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.

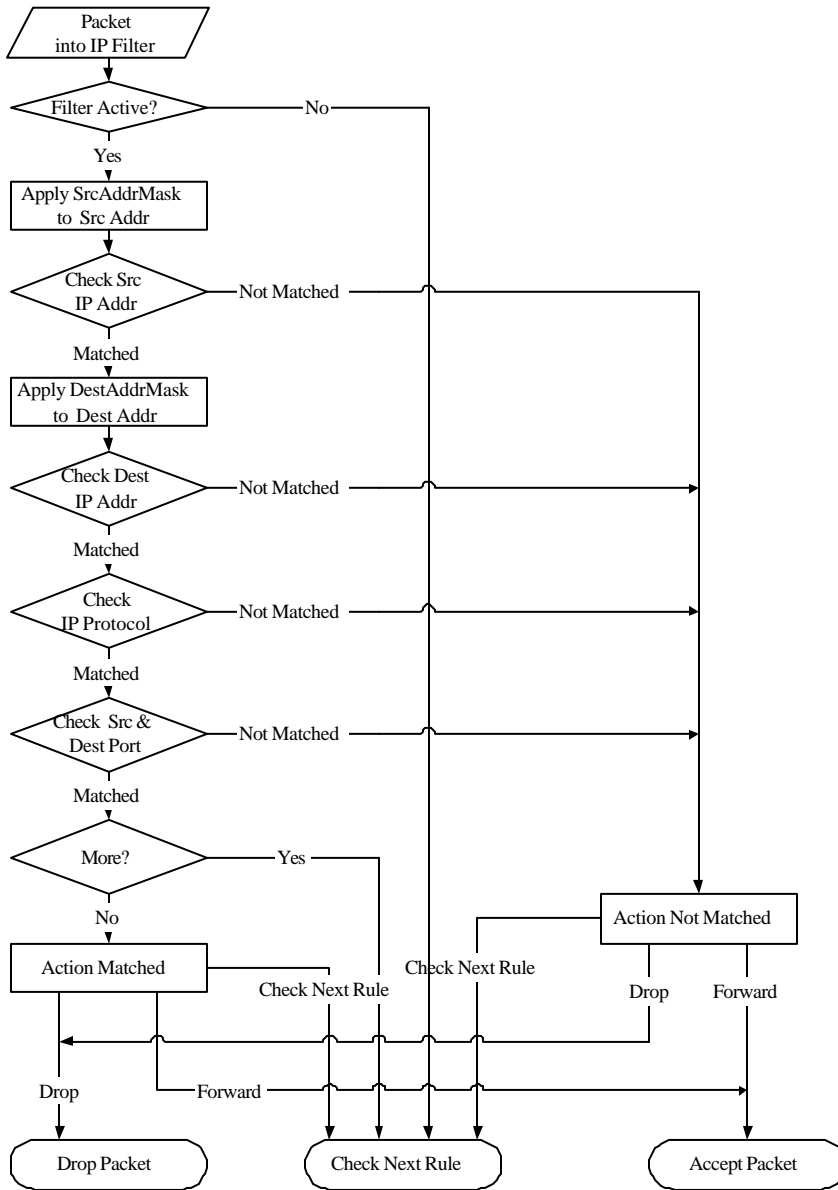
**Table 9-5 TCP/IP Filter Rule Menu Fields**

Field	Description	Option
Active	Press the [SPACEBAR] to activate ( <b>Yes</b> ) or deactivate ( <b>No</b> ) the filter rule.	<b>Yes/No</b>
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6,	0-255

Field	Description	Option
	UDP is 17 and ICMP is 1. This value must be between 0 and 255	
IP Source Route	If <b>Yes</b> , the rule applies to packet with IP source route option; else the packet must not have source route option. The majority of IP packets do not have source route.	<b>Yes/No</b>
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>N/A</b> .	<b>Yes / N/A</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>	<p><b>None</b></p> <p><b>Action Matched</b></p> <p><b>Action Not Matched</b></p> <p><b>Both</b></p>

<b>Field</b>	<b>Description</b>	<b>Option</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 21.1.1 - 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 an IP Filter**



### 9.3.2 Generic Filter Rule

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

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

To configure a generic rule, select Generic Filter Rule in the Filter Type field and press [ENTER] to open **Menu 21.1.2 - Generic Filter Rule**, as shown next.

```
Menu 21.1.2 - Generic Filter Rule

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

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

**Figure 9-8**      **Menu 21.1.2 - Generic Filter Rule**

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

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

<b>Field</b>	<b>Description</b>	<b>Option</b>
Filter #	This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third filter rule of that set.	
Filter Type	Use the [SPACE BAR] to toggle between types of rules. Parameters displayed below each type will be different.	<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>N/A</b> .	<b>Yes / N/A</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</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.		

### 9.3.3 Novell IPX Filter Rule

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

To configure an IPX rules, select **IPX Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.1.3 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**

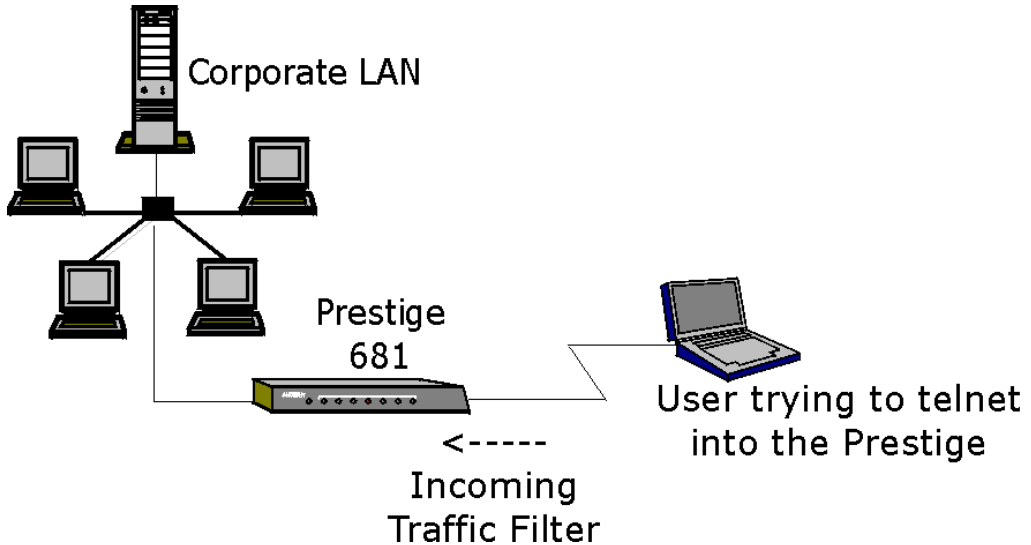
The next table describes the IPX Filter Rule.

**Table 9-7 IPX Filter Rule Menu Fields**

Field	Description
IPX Packet Type	Enter the IPX packet type (1-byte in hexadecimal) you wish to filter.  <b>The popular types are (in hexadecimal):</b> 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 Example Filter

Let's look at the third default ZyXEL filter, TELNET\_WAN (see *Figure 9-2* and *Figure 9-5*) as an example. Please see our PNC Disk for more example filters. This filter is designed to block outside users telnetting into the Prestige.



**Figure 9-10 Telnet Filter Example**

- Step 1.** Enter **21** from the Main Menu to open **Menu 21 - Filter Set Configuration**.
- Step 2.** Enter the index of the filter set you wish to configure (in this case, 3) and press [ENTER].
- Step 3.** Enter a descriptive name or comment in the **Edit Comments** field (in this case TELNET\_WAN) and press [ENTER].
- Step 4.** Press [ENTER] at the message: [Press ENTER to confirm] to open **Menu 21.1 - Filter Rules Summary**.
- Step 5.** Enter **1** to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

```
Menu 21.1.1 - TCP/IP Filter Rule

Filter #: 3,1
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 # = 23
                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= Forward

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

Press the [SPACEBAR] to choose this filter rule type. The first filter rule type determines all subsequent filter types within a set.

Select **Yes** to make the rule active.

**6** is the TCP protocol.

The port number for the telnet service (TCP protocol) is **23**. See RFC 1060 for port numbers of well-known services.

There are no more rules to check.

Select **Drop** here so that the packet will be dropped if its destination is the telnet port.

Select **Equal** here as we are looking for packets going to port 23 only.

Select **Forward** here so that the packet will be forwarded if its destination is not the telnet port.

**Figure 9-11 Example Filter – Menu 21.1.1**

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

```

Menu 21.3 - Filter Rules Summary
-----
# A Type                               Filter Rules                               M m D
-----
1 Y IP Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23      N D F
2 N
3 N
4 N
5 N
6 N

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

This shows you that you have configured and activated (**A = Y**) a TCP/IP filter rule (**Type = IP, Pr = 6**) for destination telnet ports (**DP = 23**).

**M = N** means an action can be taken immediately. The action is to drop the packet (**m = D**) if the action is matched and to forward the packet immediately (**n = F**) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

**Figure 9-12 Example Filter Rules Summary – Menu 21.3**

After you've created the filter set, you must apply it.

- Step 1.** Enter **11** from the main menu to go to Menu 11.
- Step 2.** Go to the **Edit Filter Sets** field, press the [SPACEBAR] to toggle **Yes** to **No** and press [ENTER].
- Step 3.** This brings you to Menu 11.5. Apply the TELNET\_WAN filter set (filter set 3) as shown in Figure 9-15.

## 9.5 Filter Types and SUA

There are two classes of filter rules, **Generic Filter** (Device) rules and Protocol Filter (**TCP/IP** and **IPX**) rules. Generic Filter rules act on the raw data from/to LAN and WAN. Protocol Filter rules act on the IP and IPX 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 an Ethernet port or any other hardware port. The following diagram illustrates this.

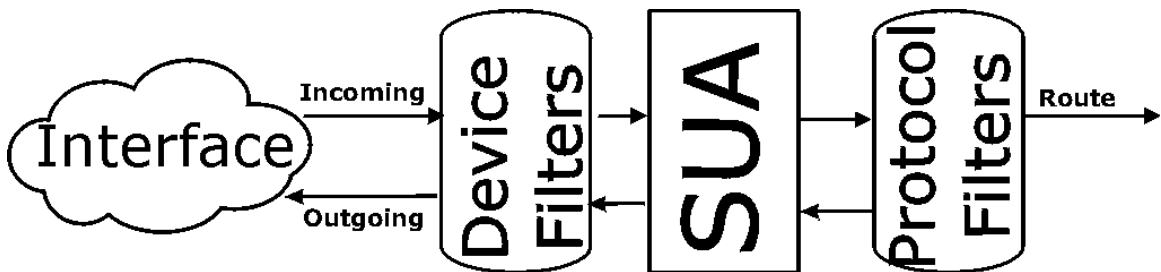


Figure 9-13 Protocol and Device Filter Sets

## 9.6 Applying a Filter and Factory Defaults

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

### 9.6.1 Ethernet traffic

You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to Menu 3.1 (shown 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



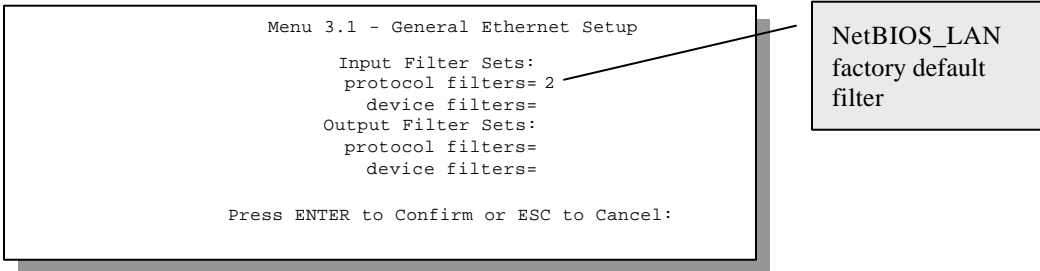


Figure 9-14 Filtering Ethernet traffic

### 9.6.2 Remote Node Filters

Go to Menu 11.5 (shown next) 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. The TELNET filter is designed to block outside users telnetting into the Prestige see (Figure 9-10)

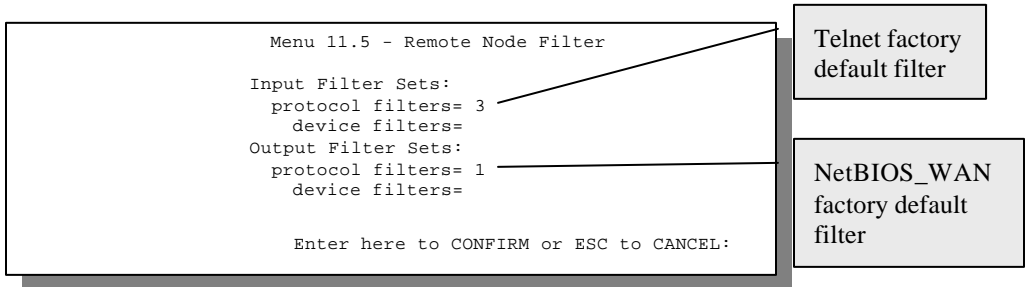


Figure 9-15 Filtering Remote Node traffic



# Chapter 10: SNMP Configuration

*This chapter discusses SNMP (Simple Network Management Protocol) for network management and monitoring.*

## 10.1 About SNMP

Your Prestige 681 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 **SNMP Configuration** (enter 22) from the Main Menu to open **Menu 22 - SNMP Configuration**, as shown in the figure below. The “community” for Get, Set and Trap fields is simply SNMP’s terminology for password.

```
Menu 22 - SNMP Configuration

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

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

**Figure 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 GetNext- requests from the management station.	public
Set Community	Enter the set community, which is the password for incoming Set-requests from the management station.	public
Trusted Host	If you enter a trusted host, your Prestige will only respond to SNMP messages from this address. If you leave the field blank (default), your Prestige will respond to all SNMP messages it receives, regardless of source.	blank
Trap: Community	Enter the trap community, which is the password sent with each trap to the SNMP manager.	public
Trap: Destination	Enter the IP address of the station to send your SNMP traps to.	blank
Once you have completed filling in <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 Maintenance

*This chapter covers the diagnostic tools that help you to maintain your Prestige.*

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

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

```
Menu 24 - System Maintenance

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

Enter Menu Selection Number:
```

**Figure 11-1**      **Menu 24 - System Maintenance**

## 11.1 System Status

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

To get to the System Status, enter number **24** to go to **Menu 24 - System Maintenance**. From this menu, select number **1, System Status**. There are two commands in **Menu 24.1 - System Maintenance - Status**. Entering **1** resets the counters and **ESC** takes you back to the previous screen.

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

Please note that displaying this screen degrades system performance.

```
Menu 24.1 -- System Maintenance - Status

NodeName  Status  TXPkts  RXPkts  Errors  Tx  B/s  Rx B/s  Up Time
John      Up      1462    1567    0       222  211    2:15:16

Ethernet:
Status: 100M/Full Duplex  Tx Pkts: 1583  WAN:
Collisions: 0             Rx Pkts: 1521  Line Status: Synchronizing
                          Transfer Rate: 784 kbps

CPU Load = 4.25%

Press Command:
CMDS: 1-Reset Counters  ESC-Exit
```

**Figure 11-2 Menu 24.1 - System Maintenance – Status**

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

**Table 11-1 System Maintenance - Status Menu Fields**

Field	Description
NodeName	This is the remote node name that you determined in Menu 11.1.
Status	Shows the status of the remote node – either <b>Up</b> or <b>N/A</b> .
TXPkts	The number of packets transmitted to this remote node.
RXPkts	The number of packets received from this remote node.
Errors	The number of error packets on this connection.
Tx B/s	Shows the transmission rate in bytes per second.
Rx B/s	Shows the receiving rate in bytes per second.
Up Time	Time this channel has been connected to the remote node.
Ethernet	
Status	Shows the current status of the LAN.
Tx Pkts	The number of transmitted packets to the LAN.
Rx Pkts	The number of received packets from the LAN.
Collision	Number of collisions.
WAN	
Line Status	Shows the current status of the SDSL line, which can be <b>Synchronizing</b> , or <b>Normal</b> .
Transfer Rate	Shows the SDSL line speed.
CPU Load	Specifies the percentage of CPU utilization.
Press Command	
1 - Reset Counters	Press 1 to reset all the above statistics to 0.
ESC - Exit	Press ESC to go back to Menu 24.

**Menu 24.2 System Information and Console Port Speed** is as follows.

<p>Menu 24.2 - System Information and Console Port Speed</p> <p>1. System Information</p> <p>2. Console Port Speed</p>
--

**Figure 11-3 System Information and Console Port Speed**

Press 1 to display the next screen, **Menu 24.2.1 - System Maintenance - Information**.

```

Menu 24.2.1 - System Maintenance - Information

Name:
Routing: IP
ZyNOS S/W Version: V2.50(T.00)b04 | 11/11/1999
SDSL Driver Version: 4.5

LAN

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

Press ESC or RETURN to Exit:
    
```

**Figure 11-4 System Maintenance - Information**

**Table 11-2 Fields in System Maintenance - Information**

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 ZyNOS (ZyXEL Network Operating System) software version and date created. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
SDSL Driver Version	Displays the driver version number of the SDSL chipset.
ANSI Version	Displays the ANSI version number.
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. See <i>Table 4-1</i> for an explanation of these terms.



## 11.1.1 Console Port Speed

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

Console Port Speed: 115200

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

**Figure 11-5** Menu 24.2.2 – System Maintenance – Console Port Speed

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

## 11.2 Log and Trace

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

### 11.2.1 Viewing Error Log

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

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

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

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

```
45      7203 PINI  INFO Channel 11 ok
46      7204 PINI  INFO Channel 10 ok
47      7205 PINI  INFO Channel 9 ok
48      7206 PINI  INFO Channel 8 ok
49      7207 PINI  INFO Channel 7 ok
50      7208 PINI  INFO Channel 6 ok
51      7209 PINI  INFO Channel 5 ok
52      7210 PINI  INFO Channel 4 ok
53      7211 PINI  INFO Channel 3 ok
54      7212 PINI  INFO Channel 2 ok
55      7213 PINI  INFO Channel 1 ok
Clear Error Log (y/n):
```

**Figure 11-6** Examples of Error and Information Messages

## 11.2.2 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 - 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= N/A
      Filter log= No
      PPP log= No
      Press ENTER to Confirm or ESC to Cancel:
      Press Space Bar to Toggle.
```

**Figure 11-7** Menu 24.3.2 - System Maintenance - Syslog and Accounting

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

**Table 11-3 System Maintenance Menu Syslog Parameters**

Parameter	Description
UNIX Syslog:	
Active	Use the [SPACE BAR] to turn on or off syslog.
Syslog IP Address	Enter the IP Address of the server that will log the CDR (Call Detail Record) and system messages i.e., the syslog server.
Log Facility	Use the [SPACE BAR] to toggle between the 7 different Local options. The log facility allows you to log the message to different files in the server. Please refer to your UNIX manual for more 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. Some examples (not P681 specific) of these syslog messages with their message formats are shown next:

**1. CDR**

CDR Message Format
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 f or each new call
str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)
L02 Tunnel Connected(L2TP)
C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call Number)
L02 Call Terminated
C02 Call Terminated

Jul 19 11:19:27 192.168.102.2 ZyXEL 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

### Packet triggered Message Format

```
sdcmdSyslogSend( SYSLOG_PKTTRI, SYSLOG_NOTICE, String );  
String = Packet trigger: Protocol=xx Data=xxxxxxxx....x  
Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)  
Data: We will send forty-eight Hex characters to the server
```

Jul 19 11:28:39 192.168.102.2 ZyXEL 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

### Filter log Message Format

```
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
```

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

##### PPP Log Message Format

```
sdcmdSyslogSend( SYSLOG_PPPLOG, SYSLOG_NOTICE, String );  
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown  
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP /  
IPXCP
```

Jul 19 11:42:44 192.168.102.2 ZyXEL 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

## 11.3 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, as shown.

```
Menu 24.4 - System Maintenance - Diagnostic  
  
WAN                                     System  
 1. Reset SDSL                          21. Reboot System  
                                         22. Command Mode  
  
TCP/IP  
 12. Ping Host  
  
Enter Menu Selection Number:  
  
Host IP Address= N/A
```

**Figure 11-8 Menu 24.4 - System Maintenance - Diagnostic**

Follow the procedure below to get to the Diagnostic menu.

**Step 1.** From the Main Menu, enter 24 to open **Menu 24 - System Maintenance**.

**Step 2.** From this menu, enter 4 to 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 11-4 System Maintenance Menu Diagnostic**

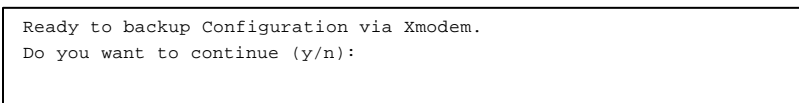
Field	Description
Reset SDSL	This command re-initializes the SDSL link to the telephone company.
Ping Host	This diagnostic test pings the host, which determines the functionality of the TCP/IP protocol on both systems and the links in between.
Reboot System	This option reboots the Prestige.
Command Mode	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.

## 11.4 Backup Configuration

Option 5 in **Menu 24 - System Maintenance** allows you to save the current Prestige configuration to a file on your computer. Backup is highly recommended once your Prestige is functioning properly.

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

**Step 1.** Go to Menu 24.5 (shown next).

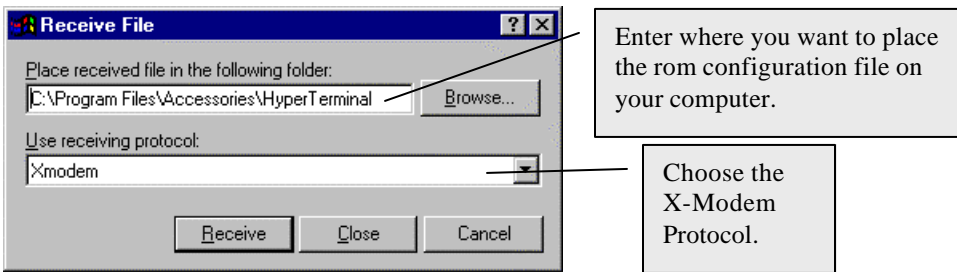


**Figure 11-9 Backup Configuration**

**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. Run the HyperTerminal program.

**Step 1.** Click “Transfer”, then “Receive File” to display the following screen



**Figure 11-10 HyperTerminal Screen**

- Step 2.** Enter a path and name for the rom configuration file on your computer (*see section 2.9 Filename conventions*) and make sure you choose the X-Modem Protocol. Then press “Receive”.
- Step 3.** After a successful backup you will see the following screen. Press any key to return to the SMT menu.

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

**Figure 11-11 Successful Backup**

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

## 11.5 Restore Configuration

Selecting option 6 from **Menu 24 - System Maintenance** to copy the configuration from your computer to the Prestige. Again, when using the console port to restore the configuration, select the XMODEM protocol.

- Step 1.** Go to Menu 24.6 (shown next).

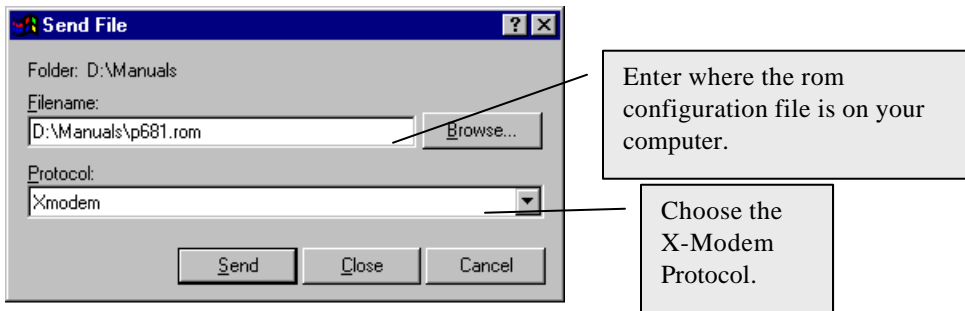
```
Ready to restore Configuration via Xmodem.  
Do you want to continue (y/n):
```

**Figure 11-12 Restore Configuration**

- Step 2.** Press “Y” to indicate that you want to continue.

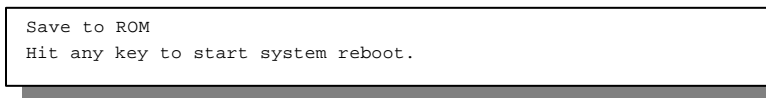
The following procedure is for the HyperTerminal program. The procedure for other serial communications programs should be similar. Run the HyperTerminal program.

- Step 3.** Click “Transfer”, then “Send File” to display the following screen.



**Figure 11-13 HyperTerminal Screen**

- 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 11-14 Successful Backup**

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

## 11.6 Upload Firmware

**Menu 24.7 -- System Maintenance - Upload Firmware** allows you to upgrade the firmware and the configuration file via the console port. The firmware and configuration file may also be uploaded via FTP. There are 2 components in the system: the router firmware and the configuration file, as shown in the next figure. Restoring the configuration as in menu 24.6 copies your (customized) backup configuration from your computer to the Prestige. Note you must be able to access the SMT to do this. Uploading the configuration file via menu 24.7.2 on the other hand rewrites all configuration data, as well as system-related data, the error log and the trace log. If you forget your password for instance (see section 2.9.1) you will need to use menu 24.7.2 as you can use this method in debug mode. However, your customized settings will be reset to the default values (including your password being reset to 1234, the Prestige default password).



```
Menu 24.7 -- System Maintenance - Upload Firmware
1. Upload Router Firmware
2. Upload Router Configuration File

Enter Menu Selection Number:
```

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

### 11.6.1 Upload Router Firmware

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 before activating Xmodem upload on your terminal.
- Step 3.** After successful firmware upload, enter “atgo” to restart the Prestige.

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

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

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

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

**Figure 11-16 Menu 24.7.1 - Uploading Router Firmware**

### 11.6.2 Upload Router Firmware using FTP

To transfer the firmware, follow the procedure below:

- Step 1.** Launch the FTP client on your workstation.
- Step 2.** Type `open` and the IP address of your Prestige.
- Step 3.** Type `root` and your SMT password as requested.
- Step 4.** Type `put firmwarefilename ras` where “firmwarefilename” is the name of your firmware upgrade file on your workstation and “ras” is the remote file name on the Prestige.
- Step 5.** The system reboots automatically after a successful firmware upload.

### **11.6.3 Uploading Router Configuration File**

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

Menu 24.7.2 shows you the instructions for uploading the 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 “`atlc`” 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., P681.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 "atlc" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
   Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart the
   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 (menu 23) may change 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 11-17 Menu 24.7.2 - System Maintenance - Upload Router Configuration File**

## 11.6.4 Upload Router configuration File using FTP

To transfer the firmware, follow the procedure below:

- Step 6.** Launch the FTP client on your workstation.
- Step 7.** Type `open` and the IP address of your Prestige.
- Step 8.** Type `root` and your SMT password as requested.
- Step 9.** Type `put RouterConfiguration rom-0` where “RouterConfiguration” is the name of your firmware upgrade file on your workstation and “rom-0” is the remote file name on the Prestige.
- Step 10.** The system reboots automatically after a successful firmware upload.

## 11.7 TFTP Transfer

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

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

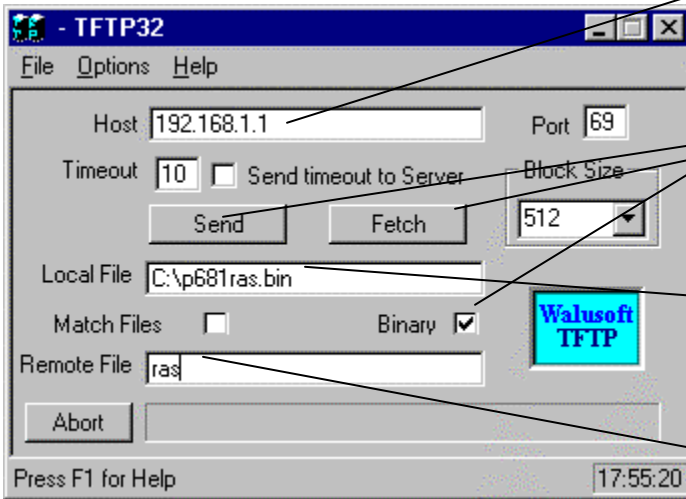
- Step 1.** Use telnet from your workstation to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.
- Step 2.** Put the SMT in command interpreter (CI) mode by entering **8** in **Menu 24 – System Maintenance**.
- Step 3.** Enter command “`sys stdio 0`” to disable the SMT timeout, so the TFTP transfer 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. Set the transfer mode to binary before starting data transfer.
- Step 5.** Use the TFTP client (see the example below) to transfer files between the Prestige and the workstation. The file name for the firmware is “`ras`” and for the configuration file, is “`rom-0`” (rom-zero, not capital o).

**Note**

If you upload the firmware to the Prestige, it will reboot automatically when the file transfer is completed (the SYS LED will flash).

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

**Example Using the Walusoft TFTP client**



Enter the IP address of the Prestige. 192.168.1.1 is the Prestige default IP address when shipped.

Press “Send” to upload the file to the Prestige and “Fetch” to back up the file on your computer. Transfer the file in binary mode.

Enter the path and name of the firmware file (\*.bin extension) or configuration file (\*.rom extension) on your computer.

This is the filename on the Prestige. The filename for the firmware is “ras” and for the configuration file, is “rom-0”.

**Figure 11-18**

**TFTP Example**

## 11.8 Command Interpreter Mode

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

```
Enter Menu Selection Number: 8

Copyright (c) 1994 - 1999 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys          exit          device        ether
wan          frelay        ip            ppp
bridge       ipx            hdap
```

**Figure 11-19 Command Mode**

## 11.9 Boot module commands

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

```
===== Debug Command Listing =====  
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  
ATLC              upload router configuration file to flash ROM  
ATXSx            xmodem select: x=0: CRC mode(default); x=1: checksum mode
```

**Figure 11-20 Boot module commands**





# Chapter 12: Troubleshooting

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

## 12.1 Problems Starting Up the Prestige

**Table 12-1 Troubleshooting the Start-Up of your Prestige**

Problem	Corrective Action	
None of the LEDs are on when you power on the Prestige	Check the connection between the AC adapter and the Prestige. If the error persists, you may have a hardware problem. In this case you should contact technical support.	
Cannot access the Prestige via the console port.	1. Check to see if the Prestige is connected to your computer's serial port.	
	2. Check to see if the communications program is configured correctly. The communications software should be configured as follows:	VT100 terminal emulation
		9600 bps
No parity, 8 Data bits, 1 Stop bit, Flow Control set to None.		

## 12.2 Problems With the WAN Interface

**Table 12-2 Troubleshooting the SDSL connection**

Problem	Corrective Action
Initialization of the PVC connection failed.	Ensure that the cable is connected properly from the SDSL port to the wall jack. The SDSL LED on the front panel of the Prestige should be on. If not, check <b>Menu 24.1</b> to verify that the <b>Line Status</b> is <b>Synchronizing</b> , then wait 10 minutes until the PVC synchronizes and this field shows <b>Normal</b> . If this field does not eventually show <b>Normal</b> , go to <b>Menu 2</b> and check that the <b>Service Type (Client or Server)</b> and the <b>Transfer Rate</b> are the same as the peer. If you still have problems, you may need to verify these variables with the telephone company and/or ISP or the peer router (in a LAN-to-LAN application).

## 12.3 Problems with the LAN Interface

**Table 12-3 Troubleshooting the LAN Interface**

Problem	Corrective Action
Can't ping any station on the LAN	Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a station connected. 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.

## 12.4 Problems Connecting to a Remote Node or ISP

**Table 12-4 Troubleshooting a Connection to a Remote Node or ISP**

Problem	Corrective Action
Can't connect to a remote node or ISP	Go to <b>Menu 4</b> or <b>Menu 11.1</b> and verify your <b>Encapsulation</b> for the remote node. Note that the P681 must reboot when the <b>Encapsulation</b> method is changed in <b>Menu 4</b> or <b>Menu 11.1</b> .

# Glossary

<b>10BaseT</b>	The 10-Mbps baseband Ethernet specification that uses two pairs of twisted-pair cabling (Category 3 or 5): one pair for transmitting data and the other for receiving data.
<b>ARP</b>	Address Resolution Protocol is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.
<b>Backbone</b>	A high-speed line or series of connections that forms a major pathway within a network.
<b>Bandwidth</b>	This is the capacity on a link usually measured in bits-per-second (bps).
<b>Bit</b>	(Binary Digit) -- A single digit number in base-2, in other words, either a 1 or a zero. The smallest unit of computerized data.
<b>Byte</b>	A set of bits that represent a single character. There are 8 bits in a Byte.
<b>CDR</b>	Call Detail Record. This is a name used by telephone companies for call related information.
<b>CHAP</b>	Challenge Handshake Authentication Protocol is an alternative protocol that avoids sending passwords over the wire by using a challenge/response technique.
<b>Client</b>	A software program that is used to contact and obtain data from a Server software program on another computer. Each Client program is designed to work with one or more specific kinds of Server programs, and each Server requires a specific kind of Client. A Web Browser is a specific kind of Client.
<b>crossover Ethernet cable</b>	A cable that wires a pin to its opposite pin, for example, RX+ is wired to TX+. This cable connects two similar devices, for example, two data terminal equipment (DTE) or data communications equipment (DCE) devices.
<b>CSU/DSU</b>	Channel Service Unit/Data Service Unit. CSUs (channel service units) and DSUs (data service units) are actually two separate devices, but they are used in conjunction and often combined into the same box. The devices are part of the hardware you need to connect computer equipment to digital transmission lines. The Channel Service Unit device connects with the digital communication line and provides a termination for the digital signal. The Data Service Unit device, sometimes called a digital service unit, is the hardware component you need to transmit digital data over the hardware channel. The device converts signals from bridges, routers, and multiplexors into the bipolar digital signals used by the digital lines. Multiplexors mix voice signals and data on the same line.
<b>DCE</b>	Data Communications Equipment is typically a modem or other type of communication device. The DCE sits between the DTE (data terminal equipment) and a transmission circuit such as a phone line.
<b>DHCP</b>	Dynamic Host Configuration Protocol automatically assigns IP addresses to clients when they log on. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses for a period of time which means that addresses are made available to assign to other systems.
<b>DLCI</b>	For Frame Relay connections, DLCI (Data Link Connection Identifier) is a path number of a portion of the PVC (the DLCI changes for each hop through the network). It is a logical

identifier with local significance only and is not the address of the destination.

- DNS** Domain Name System links names to IP addresses. When you access Web sites on the Internet, you can type the IP address of the site or the DNS name. When you type a domain name in a Web browser, a query is sent to the primary DNS server defined in your Web browser's configuration dialog box. The DNS server converts the name you specified to an IP address and returns this address to your system. From then on, the IP address is used in all subsequent communications.
- Domain Name** The unique name that identifies an Internet site. Domain Names always have 2 or more parts, separated by dots. The part on the left is the most specific, and the part on the right is the most general.
- DRAM** Dynamic RAM that stores information in capacitors that must be refreshed periodically.
- DSL** Digital Subscriber Line technologies enhances the data capacity of the existing twisted-pair wire that runs between the local telephone company switching offices and most homes and offices. There are actually seven types of DSL service, ranging in speeds from 16 Kbits/sec to 52 Mbits/sec. The services are either symmetrical (traffic flows at the same speed in both directions), or asymmetrical (the downstream capacity is higher than the upstream capacity). DSL connections are point-to-point dedicated circuits, meaning that they are always connected. There is no dial-up. There is also no switching, which means that the line is a direct connection into the carrier's frame relay, ATM (Asynchronous Transfer Mode), or Internet-connect system.
- DSLAM** A Digital Subscriber Line Access Multiplexer (DSLAM) is a network device, usually at a telephone company central office, that receives signals from multiple customer Digital Subscriber Line connections and puts the signals on a high-speed backbone line using multiplexing techniques. Depending on the product, DSLAM multiplexers connect DSL lines with some combination of asynchronous transfer mode ATM, frame relay, or IP networks.
- DTE** Originally, the DTE (data terminal equipment) was a dumb terminal or printer, but today it is a computer, or a bridge or router that interconnects local area networks.
- HDLC** HDLC (High-level Data Link Control) is a bit-oriented (the data is monitored bit by bit), link layer protocol for the transmission of data over synchronous networks.
- EMI** ElectroMagnetic Interference. The interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.
- Ethernet** A very common method of networking computers in a LAN. There are a number of adaptations to the IEEE 802.3 Ethernet standard, including adaptations with data rates of 10 Mbits/sec and 100 Mbits/sec over coaxial cable, twisted-pair cable, and fiber-optic cable. The latest version of Ethernet, Gigabit Ethernet, has a data rate of 1 Gbit/sec.
- FAQ** (Frequently Asked Questions) -- FAQs are documents that list and answer the most common questions on a particular subject.
- FCC** The FCC (Federal Communications Commission) is in charge of allocating the electromagnetic spectrum and thus the bandwidth of various communication systems.
- Flash memory** The nonvolatile storage that can be electrically erased and reprogrammed so that data can be stored, booted, and rewritten as necessary.

<b>FTP</b>	File Transfer Protocol is an Internet file transfer service that operates on the Internet and over TCP/IP networks. FTP is basically a client/server protocol in which a system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files.
<b>Gateway</b>	A gateway is a computer system or other device that acts as a translator between two systems that do not use the same communication protocols, data formatting structures, languages, and/or architecture.
<b>Host</b>	Any computer on a network that is a repository for services available to other computers on the network. It is quite common to have one host machine provide several services, such as WWW and USENET.
<b>IANA</b>	Internet Assigned Number Authority acts as the clearinghouse to assign and coordinate the use of numerous Internet protocol parameters such as Internet addresses, domain names, protocol numbers, and more. The IANA Web site is at <a href="http://www.isi.edu/iana">http://www.isi.edu/iana</a> .
<b>ICMP</b>	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and are not directly apparent to the application user.
<b>internet</b>	(Lower case i) Any time you connect 2 or more networks together, you have an internet.
<b>Internet</b>	(Upper case I) The vast collection of inter-connected networks that all use the TCP/IP protocols and that evolved from the ARPANET of the late 60's and early 70's. The Internet now (July 1995) connects roughly 60,000 independent networks into a vast global internet
<b>Intranet</b>	A private network inside a company or organization that uses the same kinds of software that you would find on the public Internet, but that is only for internal use.
<b>IP</b>	Internet Protocol the IP (currently IP version 4, or IPv4), is the underlying protocol for routing packets on the Internet and other TCP/IP-based networks.
<b>IPCP (PPP)</b>	IP Control Protocol allows changes to IP parameters such as the IP address.
<b>IPX</b>	Internetwork Packet eXchange The native NetWare internetworking protocol is IPX (Internetwork Packet Exchange). Like IP (Internet Protocol), IPX is an internetworking protocol that provides datagram services.
<b>ISP</b>	Internet Service Providers provide connections into the Internet for home users and businesses. There are local, regional, national, and global ISPs. You can think of local ISPs as the gatekeepers into the Internet.
<b>LAN</b>	Local Area Network is a shared communication system to which many computers are attached. A LAN, as its name implies, is limited to a local area. This has to do more with the electrical characteristics of the medium than the fact that many early LANs were designed for departments, although the latter accurately describes a LAN as well. LANs have different topologies, the most common being the linear bus and the star configuration.
<b>MAC</b>	On a local area network (LAN) or other network, the MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.) The MAC layer frames data for transmission over the network, then passes the frame to the physical layer interface where it is transmitted as a stream of bits.

<b>NAT</b>	Network Address Translation is the translation of an Internet Protocol address used within one network to a different IP address known within another network - <i>see also SUA</i> .
<b>NDIS</b>	Network Driver Interface Specification is a Windows specification for how communication protocol programs (such as TCP/IP) and network device drivers should communicate with each other.
<b>Network</b>	Any time you connect 2 or more computers together so that they can share resources, you have a computer network. Connect 2 or more networks together and you have an internet.
<b>NIC</b>	Network Interface Card. A board that provides network communication capabilities to and from a computer system. Also called an adapter.
<b>Node</b>	Any single computer connected to a network
<b>PAP</b>	Password Authentication Protocol PAP is a security protocol that requires users to enter a password before accessing a secure system. The user's name and password are sent over the wire to a server, where they are compared with a database of user account names and passwords. This technique is vulnerable to wiretapping (eavesdropping) because the password can be captured and used by someone to log onto the system.
<b>PNC</b>	Prestige Network Commander, a Windows-based setup wizard for Prestige routers (not all).
<b>Port</b>	An Internet port refers to a number that is part of a URL, appearing after a colon (:) right after the domain name. Every service on an Internet server listens on a particular port number on that server. Most services have standard port numbers, e.g. Web servers normally listen on port 80.
<b>POTS</b>	Plain Old Telephone Service is the analog telephone service that runs over copper twisted-pair wires and is based on the original Bell telephone system. Twisted-pair wires connect homes and businesses to a neighborhood central office. This is called the local loop. The central office is connected to other central offices and long-distance facilities.
<b>PPP</b>	Point to Point Protocol. PPP encapsulates and transmits IP (Internet Protocol) datagrams over serial point-to-point links. PPP works with other protocols such as IPX (Internetwork Packet Exchange). The protocol is defined in IETF (Internet Engineering Task Force) RFC 1661 through 1663. PPP provides router-to-router, host-to-router, and host-to-host connections.
<b>PSTN</b>	Public Switched Telephone Network was put into place many years ago as a voice telephone call-switching system. The system transmits voice calls as analog signals across copper twisted cables from homes and businesses to neighborhood COs (central offices); this is often called the local loop. The PSTN is a circuit-switched system, meaning that an end-to-end private circuit is established between caller and callee.
<b>PVC</b>	Permanent Virtual Circuit. A PVC is a logical point-to-point circuit between customer sites. PVCs are low-delay circuits because routing decisions do not need to be made along the way. Permanent means that the circuit is preprogrammed by the carrier as a path through the network. It does not need to be set up or torn down for each session.
<b>RFC</b>	An RFC (Request for Comments) is an Internet formal document or standard that is the result of committee drafting and subsequent review by interested parties. Some RFCs are informational in nature. Of those that are intended to become Internet standards, the final

version of the RFC becomes the standard and no further comments or changes are permitted. Change can occur, however, through subsequent RFCs.

<b>RIP</b>	Routing Information Protocol is an interior or intra-domain routing protocol that uses the distance-vector routing algorithms. RIP is used on the Internet and is common in the NetWare environment as a method for exchanging routing information between routers.
<b>SAP</b>	In NetWare, the SAP (Service Advertising Protocol) broadcasts information about available services on the network that other network devices can listen to. A server sends out SAP messages every 60 seconds. A server also sends out SAP messages to inform other devices that it is closing down. Workstations use SAP to find services they need on the network.
<b>SDSL</b>	Symmetrical Digital Subscriber Line is a symmetrical, bi-directional DSL service that operates on one twisted-pair wire. It can provide data rates up to the T1 rate of 1.544 Mbits/sec, and it operates above the voice frequency, so voice and data can be carried on the same wire.
<b>Server</b>	A computer, or a software package, that provides a specific kind of service to client software running on other computers.
<b>SNMP</b>	System Network Management Protocol is a popular management protocol defined by the Internet community for TCP/IP networks. It is a communication protocol for collecting information from devices on the network.
<b>STP</b>	Twisted-pair cable consists of copper-core wires surrounded by an insulator. Two wires are twisted together to form a pair, and the pair form a balanced circuit. The twisting prevents interference problems. STP (shielded twisted-pair) provides protection against external crosstalk.
<b>Straight through Ethernet cable</b>	A cable that wires a pin to its equivalent pin. This cable connects two dissimilar devices, for example, a data terminal equipment (DTE) device and a data communications equipment (DCE) device. A straight through Ethernet cable is the most common cable used.
<b>SUA</b>	Single User Account – The Prestige's SUA (Single User Account) feature allows multiple user Internet access for the cost of a single ISP account - <i>see also NAT</i> .
<b>TCP</b>	Transmission Control Protocol handles flow control and packet recovery and IP providing basic addressing and packet-forwarding services.
<b>Telnet</b>	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
<b>Terminal</b>	A device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard and a display screen and some simple circuitry.
<b>Terminal Software</b>	Software that pretends to be (emulates) a physical terminal and allows you to type commands to a computer somewhere else.
<b>TFTP</b>	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP (File Transfer Protocol), but it is scaled back in functionality so that it requires fewer resources to run. TFTP uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
<b>UDP</b>	UDP is a connectionless transport service that dispenses with the reliability services provided by TCP. UDP gives applications a direct interface with IP and the ability to address a

particular application process running on a host via a port number without setting up a connection session.

- URL** (Uniform Resource Locator) URL is an object on the Internet or an intranet that resides on a host system. Objects include directories and an assortment of file types, including text files, graphics, video, and audio. A URL is the address of an object that is normally typed in the Address field of a Web browser. The URL is basically a pointer to the location of an object.
- WAN** Wide Area Network s link geographically dispersed offices in other cities or around the globe. Just about any long-distance communication medium can serve as a WAN link, including switched and permanent telephone circuits, terrestrial radio systems, and satellite systems.
- WWW** (World Wide Web) -- Frequently used when referring to "The Internet", WWW has two major meanings - First, loosely used: the whole constellation of resources that can be accessed using Gopher, FTP, HTTP, telnet, USENET, WAIS and some other tools. Second, the universe of hypertext servers (HTTP servers).



# Index

## 1

10/100M Fast Ethernet LAN Interface, 1-2

## 2

2B1Q line, xvi

## A

ANSI (American National Standards Institute), 3-6  
Ascend/Lucent, 3-4, 3-5  
AT command, 2-8  
Authentication, 5-3, 5-4

## B

BECN (backward explicit congestion notification), 3-3  
Bridge. *See* Bridging  
Bridging, 2-10, 2-11, 5-3, 8-1, 8-3  
    Ethernet Setup, 8-1  
    Handle IPX, 8-2  
    Remote Node, 8-3  
    Static Route, 8-4

## C

CDR, 11-7  
CHAP, 5-3  
CO (Central Office), 3-4  
Comparisons  
    Cable Modems, xx  
    ISDN, xx  
    T1, xx  
Connecting the Prestige, 2-2  
Connections  
    Additional Requirements, 2-3  
    Console Port, 2-2  
    LAN Port, 2-3  
    Power Adapter, 2-3  
    Rear Panel, 2-2

SDSL Line, 2-2

Console Port Speed, 11-5  
Continuous Connection, xix  
Copyright, ii  
CPU Load, 11-3  
Customer Support, v

## D

Dedicated Bandwidth, xix  
Diagnostic Tools, 11-1, 11-9  
    Backup, 11-10  
    Boot Module Commands, 11-18  
    Command Interpreter Mode, 11-17  
    Firmware Update, 11-12  
        Upload Router Configuration, 11-14  
        Upload Router Firmware, 11-13  
    Reset SDSL, 11-10  
    Restore, 11-11  
Digital Subscriber Line Access Multiplexer, 1-3  
DLCI, 3-2, 3-3, 4-8, 4-9, 4-10, A  
DNS, 4-6  
Domain Name System, 4-3  
DSL (Digital Subscriber Line), xix  
DSLAM. *See* Digital Subscriber Line Access Multiplexer  
Dynamic Host Configuration Protocol, 4-3

## E

Encapsulation, 1-2, 4-8, 4-10, 5-2, 5-4  
    RFC 1490, 4-8  
Ethernet, 2-10

## F

FCC Rules, iii  
FCS (FRAME CHECK SEQUENCE), 3-3  
Features, 1-1  
FECN (forward explicit congestion notification), 3-3  
FECN (forward explicit congestion notification), 3-3

Filename Conventions, 2-8

Filter, 2-11

    About, 9-1

    Applying, 9-18

        Ethernet, 9-18

        Remote Node, 9-19

    Configuring a Filter Set, 9-3

    Filter log, 11-7

    Generic Rule, 9-11

    IPX

        Packet Types, 9-14

    IPX Rule, 9-13

    Remote Node, 5-5

    Rules, 9-4

    Structure, 9-1

    SUA, 9-18

    TCP/IP, 9-7

Filters, 1-3

    Executing a Filter Rule, 9-1

    Logic Flow of an IP Filter, 9-9

FLAG, 3-3

Frame Relay, 1-3, 3-1

    Standards, 3-6

Frame relay frame format, 3-2

Frame Relay Options, 3-5

Frame Relay Solution, 3-2

Frame Relay Support, 1-1

Frame Types, 7-1, 7-4

Front Panel, 2-1

Full Network Management, 1-2

## **G**

Gateway, 6-6, 7-9, 8-5

General Setup, 2-9

## **H**

Hop Count, 7-7, 7-9

Host a web site, xix

Housing, 2-3

HyperTerminal Screen, 11-10

## **I**

IANA, 4-1, 4-2

Initial Screen, 2-5

Initialization, 2-5

Internet Access, ii, xvi, 1-1, 1-2, 1-3, 1-4, 2-7, 4-1, 4-9, 4-10, 4-11, 4-12

Internet Assigned Numbers Authority. See IANA

Investment Protection, xx

IP Address, 4-2, 4-6, 5-3, 6-3, 6-6, 8-5

IP Address Assignment, 4-8

IP network number, 4-1

IP Pool, 4-3

IP static route, 6-4

*IPX*, 2-11, 7-1

    Ethernet Setup, 7-4

    LAN-to-LAN, 7-5

    Network Number, 7-2

    Node Number, 7-1

    Novell, 7-5

    Prestige, 7-3

    Remote Node Setup, 7-6

    Static Route, 7-8

IPX

    Network Number, 7-1

ITU – T (International Telecommunication Union – Telecommunications Standardization Sector), 3-6

## **L**

LAN, 11-3

LAN (Local Area Network), 4-7

LAN-to-LAN, 1-4, 6-1

LED Indicators, 2-1

Link Compatibility, 3-4

Link Management, 3-6

LMI. See Local Management Interface

Local Management Interface, 3-3

Log and Trace, 11-5

    View Error Log, 11-5

Log Facility, 11-7

Low Maintenance, xx

## **M**

MAC, 8-1

Main Menu, 2-7

Media Access Control. See MAC

Metric, 6-4, 6-6  
Multiple Protocol Support, 1-2

## N

NAT/SUA, 1-2, 9-18  
NetWare Clients, 7-3  
NIC, 2-3  
Novell, 7-1

## P

Packet triggered, 11-7  
Packing List Card, xvii  
PAP, 5-3  
Password, 2-5, 2-8  
Ping, 11-10  
PNC Disk, xvi  
Point-to-Point, xix  
Power On, 2-5  
PPP, 5-3, 5-4  
PPP log, 11-7  
Private, 6-4, 6-6  
Protocols, 2-10

## R

RAS code, 11-13  
Read Me First, xvi  
Rear Panel, 2-2  
Related Documentation, xvi  
Remote DHCP Server, 4-6  
Remote Node, 5-1, 11-3  
    Profile, 5-1  
    Setup, 5-1  
Resetting the Prestige, 2-9  
RIP, 4-6, 6-4  
Route, 5-3  
Routing Information Protocol, 4-2  
RT (Remote Terminal), 3-4  
RXPkts, 11-3

## S

Safety Instructions, 2-3  
Safety Instructions, 2-3

Scalability, 1-1  
SDSL (Symmetrical Digital Subscriber Line), xix  
SDSL Chipset Vendor, 11-4  
SDSL Maximum Transmission Distances, 3-4  
Security, 1-3  
Seed Router, 7-3, 7-4  
Service Type, 3-5  
Single User Account, 4-10. *See* SUA  
SNMP  
    About, 10-1  
    Configuring, 10-1  
        Community, 10-1  
        Trap, 10-2  
        Trusted Host, 10-2  
SNMP (Simple Network Management Protocol),  
    1-2  
Socket, 7-9  
Static Route Setup, 6-4  
STP, 2-3  
SUA, 1-4, 4-10, 6-3  
    Advantages, 4-11  
    Configuration, 4-11  
    Multiple Servers, 4-12  
Submenus, 2-6  
Subnet Mask, 4-2, 4-6, 6-3, 6-6  
Syntax Conventions, xvii  
Syslog IP Address, 11-7  
System  
    Unix Syslog And Accounting, 11-6  
System Management Terminal, 2-5  
System Status, 11-2

## T

TCP/IP, 6-1, 11-10  
TCP/IP Parameters, 4-1  
Tick Count, 7-7, 7-9  
Transfer Rate, 3-4, 3-5  
Transmission Rates, xvi, 1-1, **3-4**  
Troubleshooting, 12-1  
    LAN, 12-2  
    Remote Node, 12-2  
    SDSL, 12-2  
TXPkts, 11-3

**U**

UNIX Syslog, 11-6, 11-7  
Up Time, 11-3  
Upload Firmware  
    FTP, 11-13, 11-15

**V**

VC (virtual circuit), 3-2  
virtual private network, 3-2  
VPN. See virtual private network

**W**

WAN (Wide Area Network), 4-7  
WAN Address, 6-3  
WAN link, 3-4  
Webmasters, xix

**Z**

ZyNOS (ZyXEL Network Operating System), 11-4