

RM356D

User's Manual

Version 1.0

NETGEAR

RM356D

PSTN Router/Hub

Copyright

Copyright © 1998 by NETGEAR.

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 NETGEAR.

Published by NETGEAR. All rights reserved.

Disclaimer

NETGEAR 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. NETGEAR further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

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

Federal Communications Commission (FCC) Interference Statement

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

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

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

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

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

Notice 1

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

Notice 2

Shielded RS-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.

Information for Canadian Users

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operation, and safety requirements. The Industry Canada does not guarantee that the equipment will operate to a user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly. The customer should be aware that the compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

For their own protection, users should ensure that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution

Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

Note

This digital apparatus does not exceed the class A limits for radio noise emissions from digital apparatus set out in the radio interference regulations of Industry Canada.

NETGEAR Limited Warranty

NETGEAR 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, NETGEAR 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 NETGEAR. 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. NETGEAR 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 NETGEAR'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 NETGEAR) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by NETGEAR to the corresponding return address, Postage Paid (USA and territories only). If the customer desires some other return destination beyond the U.S. borders, the customer shall bear the cost of the return shipment. This warranty gives you specific legal rights, and you may also have other rights which vary from state to state.

Customer Support

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

Worldwide Support

NETGEAR

Product Information

For product information, visit our site on the **World Wide Web**: <http://www.NETGEAR.baynetworks.com>.

Table of Contents

List of Figures	xiii
List of Tables	xvii
Preface	xix

Chapter 1

Getting to Know Your Router/Hub

1.1	RM356D PSTN Bridge Router	1-1
1.2	Front Panel LEDs and Back Panel Ports	1-2
1.3	Features of RM356D	1-5
1.4	Applications for RM356D	1-8

Chapter 2

Hardware Installation & Initial Setup

2.1	Unpacking your Router/Hub	2-1
2.2	Additional Installation Requirements	2-2
2.3	Connect your PSTN Router/Hub	2-3
2.4	Power On Your Prestige	2-6
2.5	Navigating the SMT Interface	2-8
2.6	Configure the SMT Password	2-10
2.7	General Setup	2-12
2.8	WAN Setup	2-14
2.9	General Ethernet Setup	2-21
2.10	Protocol Dependent Ethernet Setup	2-22

Chapter 3

Internet Access Application

3.1	IP Addresses and the Internet	3-1
3.2	Route IP Setup	3-5
3.3	TCP/IP Ethernet Setup and DHCP	3-6
3.4	Internet Access Configuration	3-9

3.5	Single User Account	3-13
3.6	Configuring Backup ISP Accounts	3-16
3.7	Editing Script Options	3-18
 Chapter 4		
Telecommuting		
4.1	Telecommuting	4-2
4.2	Dial-In Server Application	4-3
4.3	Default Dial-In Setup	4-4
4.4	Dial-In Users Setup	4-8
4.5	More on CLID	4-10
 Chapter 5		
Remote Node Configuration for LAN-to-LAN		
5.1	Remote Node Setup	5-1
5.2	Leased Line Connection	5-12
 Chapter 6		
TCP/IP Configuration for LAN-to-LAN		
6.1	LAN-to-LAN Application	6-1
 Chapter 7		
Novell IPX Configuration for LAN-to-LAN		
7.1	IPX Network Environment	7-1
7.2	<i>Prestige</i> Operating in IPX Environment	7-2
7.3	IPX Spoofing	7-3
7.4	IPX Ethernet Setup	7-4
7.5	LAN-to-LAN Application with Novell IPX	7-6
 Chapter 8		
Bridge Configuration for LAN-to-LAN		
8.1	IPX Spoofing	8-1
8.2	Bridge Ethernet Setup	8-2
8.3	LAN-to-LAN Application	8-4

Chapter 9

Filter Configuration

9.1	Configuring a Filter Set	9-3
9.2	Configuring a Filter Rule	9-7

Chapter 10

Simple Network Management Protocol (SNMP)

10.1	Configuring Your <i>Prestige</i> For SNMP Support.....	10-1
------	--	------

Chapter 11

System Security

11.1	Using RADIUS Authentication.....	11-1
11.2	Configure the SMT Password	11-5

Chapter 12

Telnet Configuration and Capabilities

12.1	About Telnet Configuration.....	12-1
12.2	Telnet Capabilities	12-2

Chapter 13

System Maintenance

13.1	System Status	13-2
13.2	Terminal Baud Rate.....	13-5
13.3	Log and Trace	13-5
13.4	Diagnostic.....	13-9
13.5	Backup Configuration.....	13-12
13.6	Restore Configuration	13-12
13.7	Software Update	13-12
13.8	Command Interpreter Mode.....	13-15
13.9	Call Control.....	13-16

Chapter 14**Troubleshooting**

14.1	Problems Starting Up the <i>Prestige</i>	14-1
14.2	Problems With the WAN Ports	14-2
14.3	Problems with the LAN Interface	14-2
14.4	Problems Connecting to a Remote Node or ISP	14-3
14.5	Problems Connecting to a Remote User	14-4
Index.....		I-1

List of Figures

Figure 1-1.	<i>RM356D</i> Front Panel LEDs	1-2
Figure 1-2.	<i>RM356D</i> Back Panel Ports	1-4
Figure 1-3.	Internet Access Application.....	1-8
Figure 1-4.	LAN-to-LAN Connection Application.....	1-9
Figure 1-5.	Telecommuting/Remote Access Application.....	1-10
Figure 2-1.	Connect <i>RM356D</i>	2-3
Figure 2-2.	Power-On Display	2-6
Figure 2-3.	Login Screen.....	2-7
Figure 2-4.	SMT Main Menu.....	2-9
Figure 2-5.	Menu 23 - System Security.....	2-10
Figure 2-6.	Menu 23.1 - System Security - Change Password.....	2-11
Figure 2-7.	Menu 1 - General Setup.....	2-12
Figure 2-8.	Menu 2 - WAN Port Setup.....	2-15
Figure 2-9a.	Menu 2.1 - Async WAN Port Setup for Serial WAN Port 1	2-15
Figure 2-9b.	Menu 2.1 - Async WAN Port Setup for WAN Port 1,2 (LINE 1,2).....	2-16
Figure 2-10.	Menu 2.1.1 - Advanced WAN Port Setup	2-18
Figure 2-11.	Menu 3 - Ethernet Setup.....	2-21
Figure 2-12.	Menu 3.1 - General Ethernet Setup.....	2-21
Figure 3-1.	Menu 1 - General Setup.....	3-5
Figure 3-2.	Menu 3.2 - TCP/IP and DHCP Ethernet Setup.....	3-6
Figure 3-3.	Menu 4 - Internet Access Setup.....	3-9
Figure 3-4.	Single User Account Topology	3-13
Figure 3-5.	Menu 4 - Internet Access Setup for Single User Account	3-15
Figure 3-6.	Menu 11.4 - Remote Node Script.....	3-18
Figure 4-1.	Example of Remote User: Telecommuter	4-2
Figure 4-2.	Example of a Dial-in Server Application	4-3
Figure 4-3.	Menu 13 - Default Dial-in Setup.....	4-4

Figure 4-4.	Menu 14 - Dial-in User Setup.....	4-8
Figure 4-5.	Menu 14.1 - Edit Dial-in User.....	4-8
Figure 5-1.	Menu 11 - Remote Node Setup.....	5-2
Figure 5-2.	Menu 11.1 - Remote Node Profile for Dial-up Line Applications.....	5-2
Figure 5-3.	Menu 11.2 - Remote Node PPP Options	5-9
Figure 5-4.	Menu 11.1 - Remote Node Profile for Leased Line Applications	5-13
Figure 5-5.	Menu 11.2 - Remote Node PPP Options for Leased Line Applications.....	5-19
Figure 6-1.	LAN-to-LAN Application with TCP/IP	6-1
Figure 6-2.	Menu 11.3- Remote Node Network Layer Options for a TCP/IP Application	6-2
Figure 6-3.	Sample IP Addresses for a LAN-to-LAN Connection with TCP/IP	6-3
Figure 6-4.	Example of Static Routing Topology	6-6
Figure 6-5.	Menu 12 - Static Route Setup.....	6-7
Figure 6-6.	Menu 12.1 - Edit IP Static Route.....	6-7
Figure 7-1.	<i>Prestige</i> Operating in IPX Environment.....	7-2
Figure 7-2.	Menu 3.3 - Novell IPX Ethernet Setup.....	7-4
Figure 7-3.	LAN-to-LAN Application with Novell IPX.....	7-6
Figure 7-4.	Menu 11.3 - Remote Node Network Layer Options for Novell IPX Application	7-7
Figure 7-5.	Netware Servers or Both Sides of the Link.....	7-9
Figure 7-6.	Menu 12.2 - Edit IPX Static Route	7-10
Figure 8-1.	Menu 3.5 - Bridge Ethernet Setup	8-3
Figure 8-2.	Menu 11.3 - Remote Node Network Layer Options for Bridging Configuration	8-4
Figure 8-3.	Menu 12.3 - Edit Bridge Static Route.....	8-6
Figure 9-1.	Outgoing Packet Filtering Process.....	9-2
Figure 9-2.	Menu 21 - Filter Set Configuration	9-3
Figure 9-3.	Menu 21.1 - Filter Rules Summary	9-4
Figure 9-4.	Menu 21.1.1 - TCP/IP Filter Rule.....	9-7
Figure 9-5.	Menu 21.1.2 - Generic Filter Rule.....	9-10
Figure 9-6.	Menu 21.1.3 - IPX Filter Rule.....	9-12

Figure 10-1.	Menu 22 - SNMP Configuration	10-2
Figure 11-1.	Menu 23.2 - System Security - External Server.....	11-3
Figure 12-1.	Telnet Configuration on a TCP/IP Network.....	12-1
Figure 13-1.	Menu 24 - System Maintenance	13-1
Figure 13-2.	Menu 24.1 - System Maintenance - Status.....	13-2
Figure 13-3.	LAN Packet Which Triggered Last Call.....	13-4
Figure 13-4.	Menu 24.2 - System Maintenance - Change Terminal Baud Rate	13-5
Figure 13-5.	Examples of Error and Information Messages.....	13-6
Figure 13-6.	Menu 24.3.2 - System Maintenance - Syslog and Accounting.....	13-7
Figure 13-7.	Menu 24.4 - System Maintenance - Diagnostic.....	13-9
Figure 13-8.	Trace Display for a Successful IPCP Connection Via Manual Call	13-11
Figure 13-9.	Trace Display for a Failed IPCP Connection Via Manual Call.....	13-11
Figure 13-10.	Menu 24.7 - System Maintenance - Upload Firmware	13-13
Figure 13-11.	Menu 24.7.1 - Example of Uploading RAS Using PCPLUS	13-13
Figure 13-12.	Menu 24.7.2 - System Maintenance - Upload ROM File	13-14
Figure 13-13.	Menu 24.7.3 - System Maintenance - Upload WAN Port 2 Modem Firmware .	13-14
Figure 13-14.	Menu 24.7.4 - System Maintenance - Upload WAN Port 2 Modem Firmware .	13-15
Figure 13-15.	Menu 24.9 - System Maintenance - Call Control	13-16
Figure 13-16.	Menu 24.9.2 - Blacklist.....	13-17
Figure 13-17.	Menu 24.9.3 - Budget Management	13-18

List of Tables

Table 1-1.	LED Functions	1-3
Table 2-1.	Item Checklist	2-1
Table 2-2.	Main Menu Commands.....	2-8
Table 2-3.	Main Menu Summary.....	2-9
Table 2-4.	General Setup Menu Fields	2-13
Table 2-5.	Async WAN Port Setup Menu Fields	2-16
Table 2-6.	Advanced WAN Port Setup AT Commands Fields	2-19
Table 2-7.	Advanced WAN Port Setup Call Control Parameters	2-20
Table 3-1.	Subnet Mask Notation.....	3-2
Table 3-2.	Examples of IP Subnet Masks.....	3-3
Table 3-3.	Private Networks IP Addresses	3-4
Table 3-4.	DHCP Ethernet Setup Menu Fields	3-7
Table 3-5.	TCP/IP Ethernet Setup Menu Fields.....	3-8
Table 3-6.	Internet Account Information.....	3-9
Table 3-7.	Internet Access Setup Menu Fields	3-11
Table 3-8.	Single User Account Menu Fields.....	3-16
Table 3-9.	Remote Node Script Menu Fields	3-18
Table 4-1.	Remote Dial-in Users/Remote Nodes Comparison Chart	4-1
Table 4-2.	Default Dial-in Setup Fields	4-5
Table 4-3.	Edit Dial-in User Menu Fields	4-9
Table 5-1.	Remote Node Profile Menu Fields for Dial-up Line Applications.....	5-3
Table 5-2.	Remote Node PPP Options Menu Fields	5-10
Table 5-3.	Remote Node Profile Menu Fields for Leased Line Applications	5-13
Table 5-4.	Remote Node PPP Options Menu Fields for Leased Line Applications.....	5-19
Table 6-1.	Remote Node Network Layer Options for a TCP/IP Configuration.....	6-4
Table 6-2.	Edit IP Static Route Menu Fields	6-8

Table 7-1.	Novell IPX Ethernet Setup Fields.....	7-5
Table 7-2.	Remote Node Network Layer Options for Novell IPX Application	7-8
Table 7-3.	Edit IPX Static Route Menu Fields.....	7-10
Table 8-1.	Handle IPX Field Settings	8-2
Table 8-2.	Bridge Ethernet Setup Menu - Handle IPX Field Configuration.....	8-3
Table 8-3.	Remote Node Network Layers Menu Bridge Options.....	8-5
Table 8-4.	Default Dial-in Setup Field for Bridging Applications	8-6
Table 8-5.	Bridge Static Route Menu Fields	8-7
Table 9-1.	Abbreviations Used in the Filter Rules Summary Menu	9-4
Table 9-2.	Abbreviations Used If Filter Type Is IP.....	9-5
Table 9-3.	Abbreviations Used If Filter Type Is GEN	9-6
Table 9-4.	Abbreviations Used If Filter Type Is IPX	9-6
Table 9-5.	TCP/IP Filter Rule Menu Fields	9-8
Table 9-6.	Generic Filter Rule Menu Fields	9-10
Table 9-7.	IPX Filter Rule Menu Fields	9-13
Table 10-1.	SNMP Configuration Menu Fields.....	10-3
Table 11-1.	System Security - External Server Menu Fields	11-3
Table 13-1.	System Maintenance - Status Menu Fields	13-3
Table 13-2.	System Maintenance Menu Syslog Parameters.....	13-7
Table 13-3.	System Maintenance Menu Diagnostic Test Options	13-10
Table 14-1.	Troubleshooting the Start-Up of your <i>Prestige</i>	14-1
Table 14-2.	Troubleshooting a WAN Port Connection	14-2
Table 14-3.	Troubleshooting the LAN Interface	14-2
Table 14-4.	Troubleshooting a Connection to a Remote Node or ISP.....	14-3
Table 14-5.	Troubleshooting a Connection to a Remote User.....	14-4

Preface

About Your Router/Hub

Congratulations on your purchase of the *RM356D* PSTN Router/Hub.

The *RM356D* is a high-performance Router/Hub that offers a complete solution for your PSTN and WAN applications such as Internet access for the corporate office, multi-protocol LAN-to-LAN connections, telecommuting and remote access. Your *RM356D* Router/Hub is the ideal high-speed Internet Access solution for your whole office.

The *RM356D* is a universal router that can connect over PSTN (Public Switch Telephone Network) and ISDN (Integrated Service Digital Network) lines. The *RM356D* can accommodate both TCP/IP and Novell IPX protocols to provide multi-protocol routing and transparent bridging. Your *Prestige* is also compatible with routers from other manufacturers such as Ascend, Cisco, and 3Com.

Your *RM356D* is easy to install and to configure since you do not need to set any switch. All functions of the *RM356D* are software configurable via the SMT (System Management Terminal) Interface. The SMT Interface is a menu-driven software easily accessible from either a VT100 compatible terminal or a terminal emulation program on a PC.

Versatile and packed with a number of advanced features the *RM356D* is designed to provide the networking solutions adapted to your needs.

About This User's Manual

This user's manual covers all aspects of your *RM356D* operations and shows you how to get the best out of the multiple advanced features of your Router/Hub.

This manual consists of fourteen chapters designed to guide you through a correct configuration of your *RM356D* depending on your particular application.

Structure of this Manual

This manual is divided into five parts:

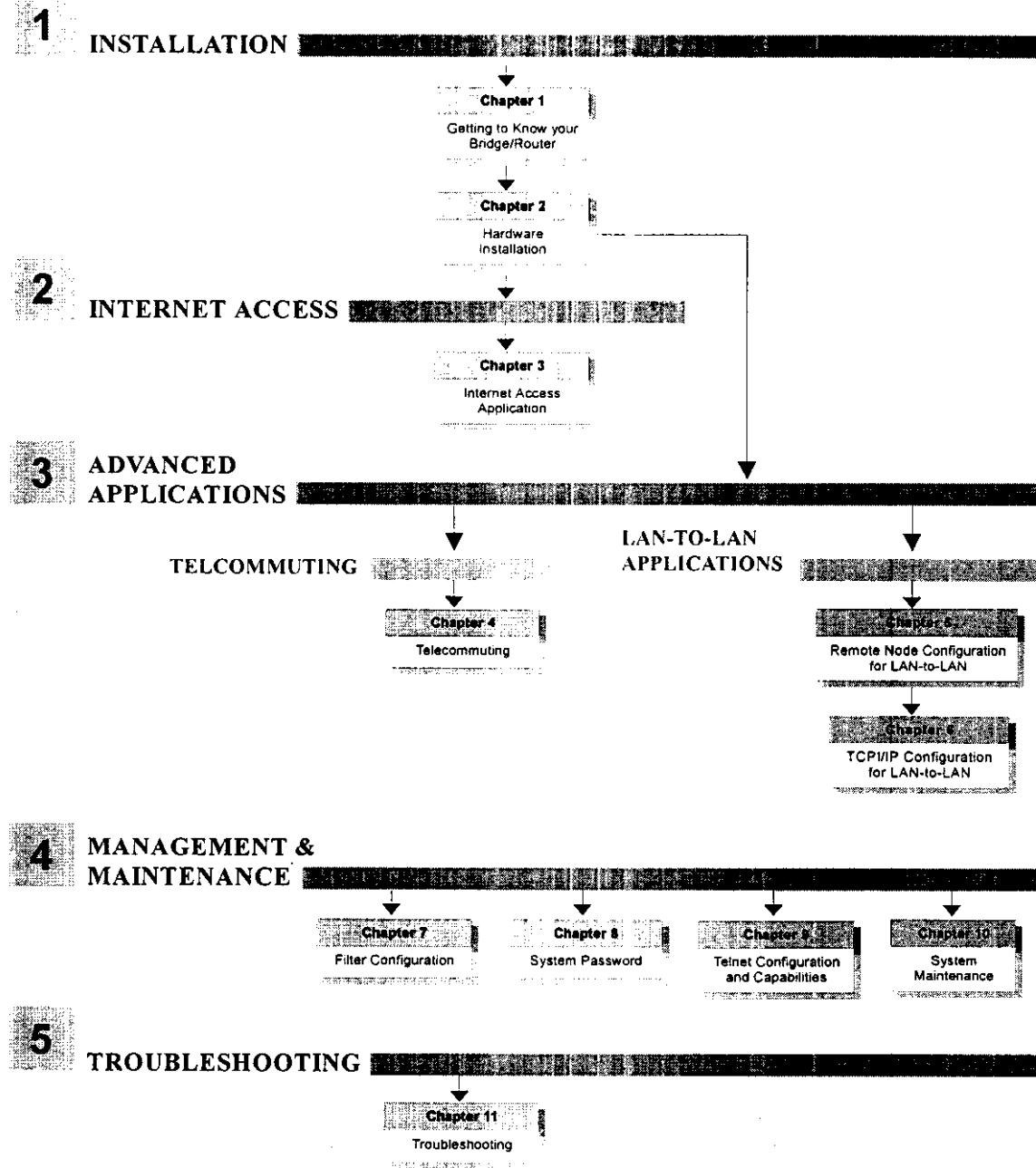
1. *Getting Started* (Chapters 1-2), is structured as a step-by-step guide to help you connect, install and setup your *RM356D* to operate on your network.
2. *The Internet* (Chapter 3), describes how to configure your *RM356D* to connect to the Internet.
3. *Setting Up Advanced Applications* (Chapters 4-8), describes how to use your *Prestige* for more advanced applications such as Telecommuting and LAN-to-LAN in TCP/IP, Novell IPX, and Bridging environments.
4. *Management & Maintenance* (Chapters 9-13), provides information on access control and logging features for network administrators.
5. *Troubleshooting* (Chapter 14), provides information about solving common problems.

Regardless of your particular application, it is important that you follow the steps outlined in *Chapters 1-2* to correctly connect your *RM356D* to your LAN. You can then refer the appropriate chapters of the manual depending on which applications you wish to use.

Orientation Map

The following *Orientation Map* is designed to guide you through a quick and correct installation of your *RM356D*. According to your particular application (Internet, Telecommuting, Multi-protocol LAN-to-LAN Connection), follow the path outlined in this *Orientation Map* to refer to the appropriate chapters in this manual. Read the instructions in each chapter carefully for a successful configuration of your *Prestige*.

Orientation Map



Chapter 1

Getting to Know Your Router/Hub

This chapter describes the key features and applications of your *RM356D* PSTN Router/Hub, equipped with a 4-port 10Tbase-T hub, 2 built-in 56 Kbps analog modems, and 1 serial port connection to external modem or ISDN TA.

1.1 *RM356D* PSTN Bridge Router

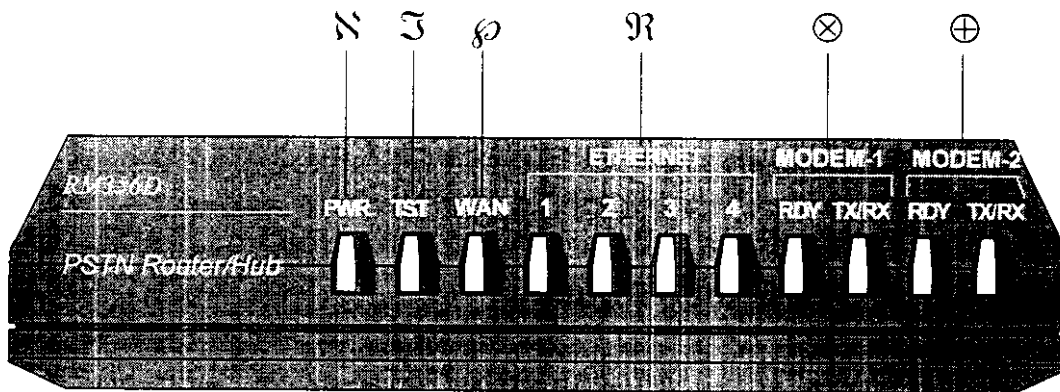
Congratulations on the purchase of your NETGEAR *RM356D* Bridge Router. Your *Prestige* integrates a 4-Port Router/Hub, Bridge and two high-speed 56K internal modems into a single package. In a modem-sized box, your *Prestige* offers inexpensive yet complete telecommunications and internetworking solutions for your home or branch office. The *Prestige* is ideal for everything from Internet browsing to receiving calls from Remote Dial-in Users to making LAN-to-LAN connections to Remote Nodes.

The *RM356D* features two 56 Kbps modem lines that can connect directly to your local PSTN (Public Switch Telephone Network) network thereby saving you the cost of buying additional external modems.

In addition, the *RM356D* offers one serial port that can connect to the PSTN network via an external modems or to the ISDN network by using ISDN-TA (ISDN Terminal Adapter).

1.2 Front Panel LEDs and Back Panel Ports

1.2.1 RM356D Front Panel



⏻ : PWR = Power LED

⏻ : TST = Test LED (Blinking)

⏻ : ETHERNET (1, 2, 3, 4) = 4-PORT 10Base-T HUB (Active Ethernet Port #)

⏻ : WAN = WAN port 1 Ready, Transmit/Receive

⏻ : MODEM-1 (RDY, TX/RX) = Internal Modem-1 (on WAN port 2) Ready, Transmit/Receive

⏻ : MODEM-2 (RDY, TX/RX) = Internal Modem-2 (on WAN port 3) Ready, Transmit/Receive

Figure 1-1. RM356D Front Panel LEDs

1.2.2 Front Panel LEDs

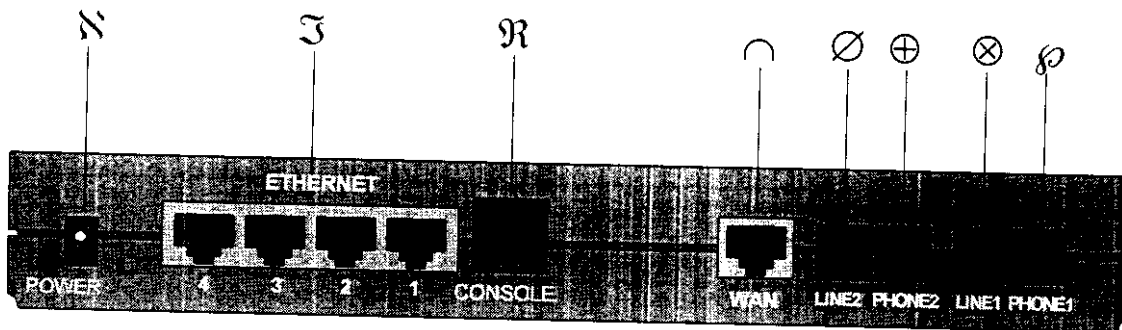
The LED indicator lights on the front panel of your *Prestige* indicate the Router/Hub functional status. The following Table 1-1 describes the LED functions:

Table 1-1. LED Functions

LEDs		Function	Indicator Status	Active	Description
PWR		Power LED	Green	On	The power AC adapter is connected to the <i>Prestige</i> .
TST		Test LED	Green	Blinking	The <i>Prestige</i> is functioning properly.
WAN (WAN 1)		Ready	Green	On	The modem or IDSN TA connected to WAN port 1 is in use.
		Transmit/Receive	Green	Blinking	Traffic is being transmitted or received on WAN port 1.
ETHER-NET	1,2,3,4	LAN Transmit LAN Receive	Green	On	The <i>Prestige</i> has successfully connected to LAN port 1,2,3,4 via the UTP Ethernet interface.
				Blinking	Traffic is being transmitted/received on LAN port 1,2,3,4.
MODEM-1 (WAN 2)	RDY	Ready	Green	On	The internal modem connected to WAN port 2 is in use.
	TX/RX	Transmit/Receive	Green	Blinking	Traffic is being transmitted or received on WAN port 2.
MODEM-2 (WAN 3)	RDY	Ready	Green	On	The internal modem connected to WAN port 3 is in use.
	TX/RX	Transmit/Receive	Green	Blinking	Traffic is being transmitted or received on WAN port 3.

1.2.3 RM356D Back Panel

Figure 1-2 helps you identify the rear panel ports of your *RM356D*. Refer to this diagram when attempting to make connections.



N : POWER = 16V-AC power outlet to connect the AC adapter.

E : ETHERNET = 4 x RJ-45 socket HUB to connect ETHERNET 10Base-T cables.

R : CONSOLE = RJ-45 connector to plug the RJ45-RS232 female adapter and connect to the Console or SMT.

O : PHONE1 = RJ-11 socket to connect a phone or fax to Modem port 1.

X : LINE1 = RJ-11 socket to connect the PSTN telephone line to Modem-1 (on WAN port 2).

⊕ : PHONE2 = RJ-11 socket to connect a phone or fax to Modem port 2.

⊗ : LINE2 = LINE1 = RJ-11 socket to connect the PSTN telephone line to Modem-2 (on WAN port 3).

C : WAN = RJ-45 socket to connect the RJ45-RS232 male adapter and plug a modem or ISDN TA to WAN port 1.

Figure 1-2. RM356D Back Panel Ports

1.3 Features of *RM356D*

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 quick and easy to install. Physically, it resembles an external modem except for the fact that it is a router and uses an Ethernet cable to connect to the host network.

Multiple WAN Ports

Your *RM356D* has three WAN ports (*WAN-1,2,3*). WAN port 1 can be connected to a dial-up/leased line modem or to an ISDN TA (Terminal Adapter). WAN port 2,3 are internally connected to two high-speed 56K modems that support dial-up configurations.

Leased Line/Dial Back-Up Support

Your *RM356D* supports a leased line connection to its serial port WAN port 1. The *Prestige* can also support dial back-up function for the leased line connection.

Multiple Networking Protocol Support

The *RM356D* is a multi-protocol router that supports TCP/IP, Novell IPX, and Transparent Bridging.

Dial-On-Demand

The Dial-On-Demand feature allows the *RM356D* to automatically place a call to a remote node whenever there the traffic coming from any workstation on the LAN is directed to that particular remote site.

Bandwidth-On-Demand

The Bandwidth-On-Demand feature provides flexible bandwidth when needed. The *RM356D* dynamically allocates bandwidth between the WAN ports, increasing or decreasing speeds as needed to allow for greater efficiency in data transfer.

By using the PPP/MP (Point-to-Point Protocol/Multilink Protocol), your *RM356D* can bundle three WAN ports connected to three different internal and external modems in order to use the maximum available bandwidth. The *RM356D* supports BAP (Bandwidth Allocation Protocol) and BACP (Bandwidth Allocation Control Protocol) to manage the number of links in multilink bundle.

Full Network Management

Your *RM356D* supports SNMP (Simple Network Management Protocol) and allows menu-driven network management via an RS-232 or Telnet connection. Your *Prestige* is also equipped with a Call Detail Record to help analyze and manage your telephone bill.

RADIUS

The RADIUS (Remote Authentication Dial-In User Service) feature allows you to use an external and central Unix-based server to support thousands of users.

PAP and CHAP Security

The *Prestige* supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). With PAP authentication enabled, the user sends the name and password in plain text. Generally, CHAP authentication is more secure since the password is scrambled prior to transmission. However, PAP is readily available on more platforms.

DHCP Support

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

Call Control

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

Data Compression

Your *Prestige* incorporates Stac data compression and CCP (Compression Control Protocol).

Networking Compatibility

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

1.4 Applications for RM356D

The RM356D offers complete solutions for your WAN applications such as Corporate Internet Access, Internet Single User Account, LAN-to-LAN Connections, Telecommuting and Remote Node Access.

Internet Access

The RM356D is the ideal high-speed Internet Access solution for the corporate and branch offices. Your RM356D supports the TCP/IP protocol, which is the language used for the Internet. It is also compatible with access servers manufactured by major vendors such as Cisco and Ascend. A typical Internet Access application is shown in Figure 1-3.

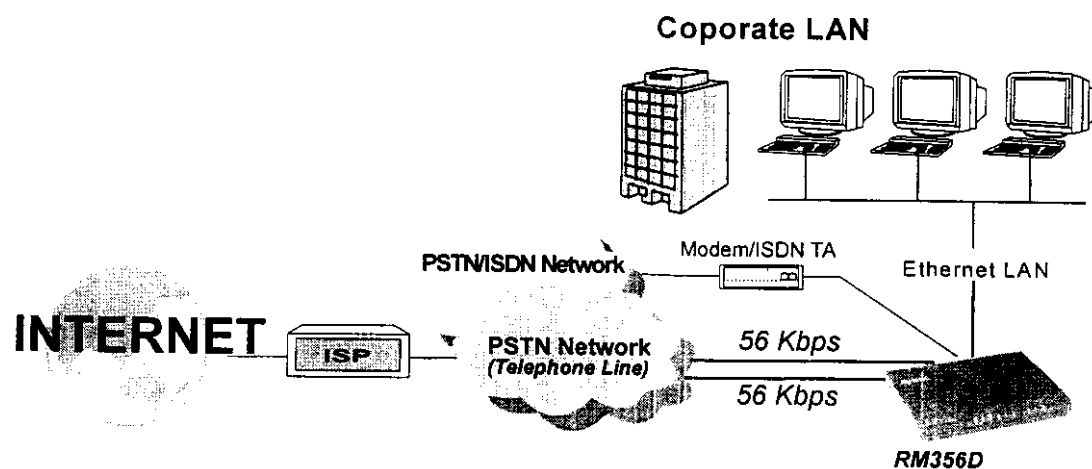


Figure 1-3. Internet Access Application

Internet Single User Account

For a small office environment, your *Prestige* offers a Single User Internet Account from an ISP (Internet Service Provider). This allows multiple users on the LAN (Local Area Network) to access the Internet concurrently for the cost of a single user. Single User Account address mapping can also be used for LAN to LAN connection.

Multiprotocol/Multiport LAN-to-LAN Connection

Your *Prestige* can dial to or answer calls from another remote access router connected to a different network. The *Prestige* supports TCP/IP, Novell IPX, and has the capability to bridge any Ethernet protocol. Your *Prestige* can also bundle several WAN ports in one LAN-to-LAN connection for greater bandwidth. A typical LAN-to-LAN application for your *RM356D* is to connect the Corporate Office LAN of your company with the Branch Office, as shown in Figure 1-4.

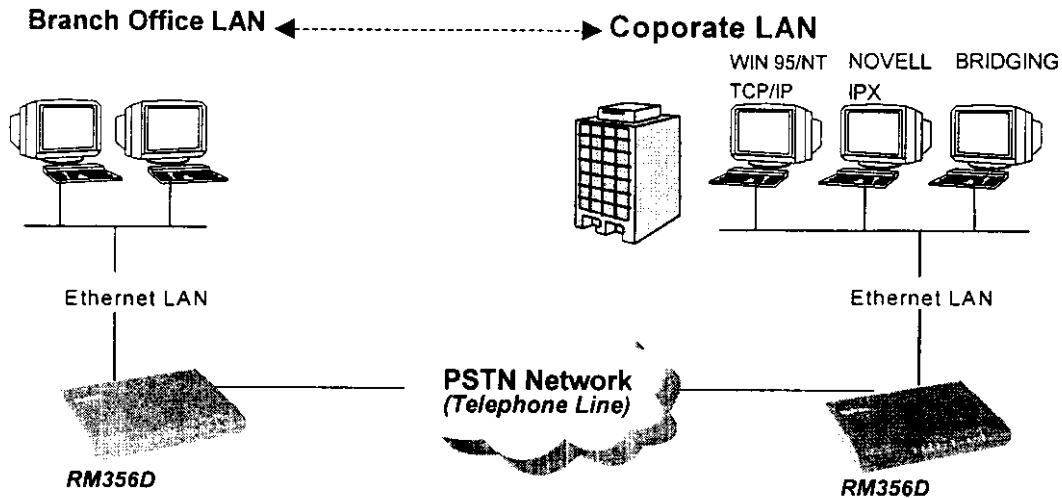


Figure 1-4. LAN-to-LAN Connection Application

Dial-On-Demand

Also, with the automatic Dial-On-Demand, your *RM356D* makes a connection only when data is transferred between the Corporate LAN and the Branch Office. Dial-On-Demand minimizes connection charges and user intervention.

Telecommuting Server / Remote Access

Your *Prestige* allows Remote Dial-in Users to dial-in and gain access to your LAN. This feature enables users that have workstations with remote access capabilities (for example, Windows 95), to dial in using a modem or an ISDN terminal adapter (TA) to access the network resources without physically being in the office. Figure 1-5 shows how a remote user or a telecommuter can connect to its corporate office via a modem or ISDN TA and the PSTN/ISDN network.

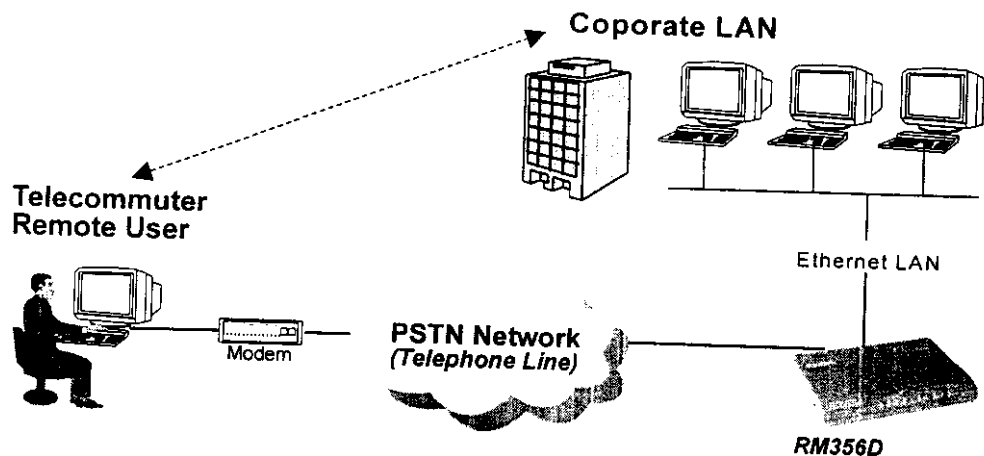


Figure 1-5. Telecommuting/Remote Access Application

RM356D allows up to three simultaneous remote-access connections or one PPP/MP bundled connection. PAP or CHAP password checking may be used to control the access from remote users to the corporate LAN. Also, call-back can be used to authenticate connections from remote users.

Chapter 2

Hardware Installation & Initial Setup

2.1 Unpacking your Router/Hub

Before you proceed further, check all items you received with your *Prestige* against this list to make sure nothing is missing. The complete package should include:

Table 2-1. Item Checklist

Package Contents	RM356D
RM356D PSTN Router/Hub	1
Power Adapter	1
RS-232 cable	1
25-pin female to 9-pin male adapter cable	1
LAN crossover cable (red tag)	1
LAN straight cable (white tag)	1
SMT RJ-45 to RS-232 female adapter cable	1
WAN RJ-45 to RS-232 male adapter cable	1
RJ-11 PSTN telephone line cable	2
Warranty Card	1
This RM356D User's Manual	1
Quick Start Guide	1

2.2 Additional Installation Requirements

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

- External Modems or ISDN TAs (Terminal adapters).
- An Ethernet 10Base-T connection to your computer.
- A computer equipped with communications software configured to the following parameters:
 - VT100 terminal emulation.
 - 9600 Baud rate.
 - No parity, 8 Data bits, 1 Stop bit.

After the *Prestige* has been successfully connected to your network, you can make future changes to the configuration by using a Telnet application.

2.3 Connect your *PSTN Router/Hub*

2.3.1 RM356D Connections

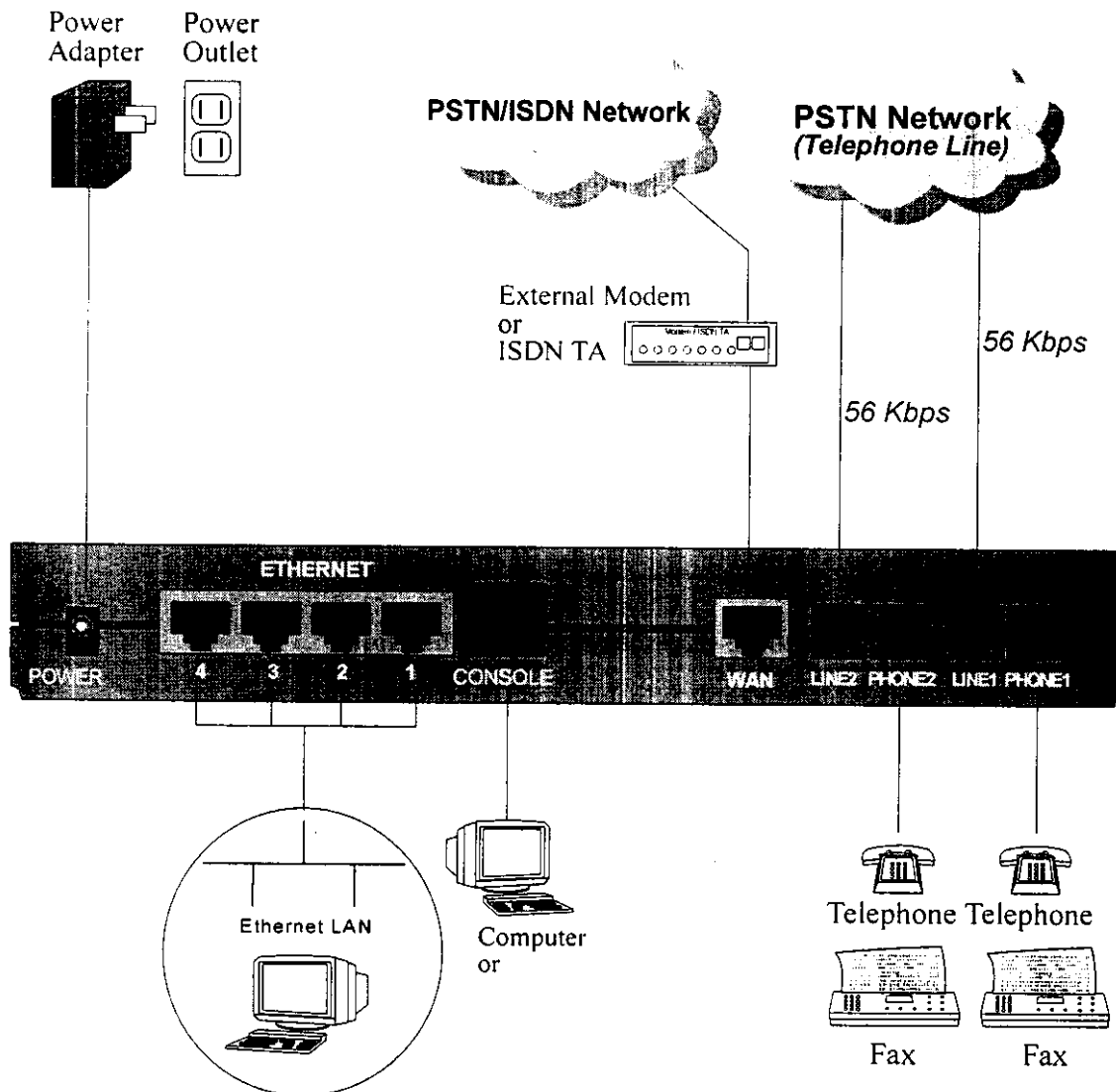


Figure 2-1. Connect RM356D

This section outlines how to connect your *RM356D* to the LAN and the WANs. Refer to Figure 1-2 to identify all of the ports on your device. Then see Figure 2-1 when you attempt to make the various connections.

Follow these steps designed to guide you through a quick and correct installation of your *RM356D*.



A Warning On Connection Cables

The SMT RS-232 cable, WAN modem line, and Ethernet cable are very similar to each other. It is important that you use the correct cable for each connection; otherwise, your *Prestige* could be damaged.

Step 1. Connect Your Computer and Your *Prestige*

For the initial setup and configuration of your *RM356D*, you must use RS-232 and communications software.

After your *Prestige* has been successfully installed, you can modify the configuration through a remote Telnet connection. See *Chapter 12 - Telnet Configuration and Capabilities* for detailed instructions on using Telnet to configure your *RM356D*.



Note on Connecting the RS-232 Cable to your *Prestige*

One RJ45 to RS-232 female adapter cable is included in your package. To make a RS-232 connection, first connect the RJ45 end of the cable to the CONSOLE port on the back panel of the *Prestige*. Connect the other end to the RS-232 cable attached to the serial port (COM1, COM2, or any other COM port) of your computer.

Step 2. Connect the Serial WAN Port

The *RM356D* has one serial WAN port (WAN port 1) which can be connected to a Dial-up modem, a Leased Line modem, or ISDN TA (Terminal Adapter). The serial WAN port uses a RJ45 connector. A cable is provided to convert RJ-45 to DB-25.

Step 3. Connect the Internal 56K Modem Ports

The *RM356D* has two modem ports (LINE 1,2) which can be connected directly to your local PSTN (Public Switch Telephone Network) via a telephone line. Use the RJ11 cables included in the package to connect the modem ports labeled LINE 1 and LINE 2 directly to the PSTN telephone line.

Step 4. Telephone/Fax Connection

The ports labeled PHONE 1 and PHONE 2 at the rear panel of your *RM356D* can be used to connect a telephone and fax that will share the same lines, LINE 1 and LINE 2 respectively, as the internal modems. Therefore, when the internal modem on LINE 1 or LINE 2 is not in use, you can dial-out and place a call or send a fax by using the telephone or fax connected to PHONE 1 or PHONE 2 ports of your *Prestige*.

Step 5. Connect an Ethernet Cable to your *Prestige*

The LAN ports 1,2,3, and 4 at the rear panel of your *Prestige* are used to connect to 10Base-T Ethernet networks. 10Base-T networks use Unshielded Twisted Pair (UTP) cable and RJ-45 connectors that look like a bigger telephone plug with 8 pins. Two types of gray Ethernet cables come with the package:

- Straight through cable (white tag): Connect your *Prestige* to your computer directly without a hub.
- Crossover cable (red tag): Connect your *Prestige* to another 10Base-T Switch/Hub.

Step 6. Connect the Power Adapter to your *Prestige*

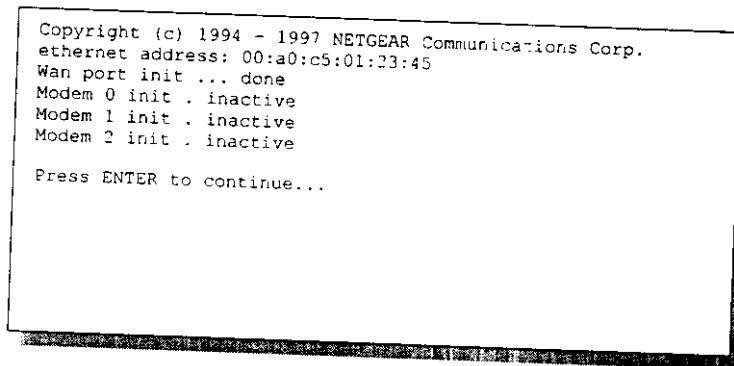
Plug a 16VAC 1200mA power adapter into the outlet labeled POWER on the rear panel of your *Prestige*.

2.4 Power On Your *Prestige*

At this point, you should have connected the computer, the external modem or ISDN TA (WAN), the telephone lines (LINE 1,2), the Ethernet cable, and the power supply. You can now power on your *Prestige* by plugging the AC adapter to the appropriate power outlet.

Step 1. Initialize SMT

When you power on your *Prestige*, the Router/Hub will perform several internal tests and will also perform a PSTN/ISDN line initialization. After this initialization, the *Prestige* will display the SMT (System Management Terminal) interface and ask you to press [Enter] to continue, as shown in Figure 2-2.



```
Copyright (c) 1994 - 1997 NETGEAR Communications Corp.  
ethernet address: 00:a0:c5:01:23:45  
Wan port init ... done  
Modem 0 init . inactive  
Modem 1 init . inactive  
Modem 2 init . inactive  
  
Press ENTER to continue...
```

Figure 2-2. Power-On Display

Step 2. Enter Password

The Login screen appears prompting you to enter the password, as shown in Figure 2-3.

For your first login, enter the default password 1234 to get into the Main Menu of the System Management Terminal (SMT). As you type a password, the screen displays an (X) for each character you typed.

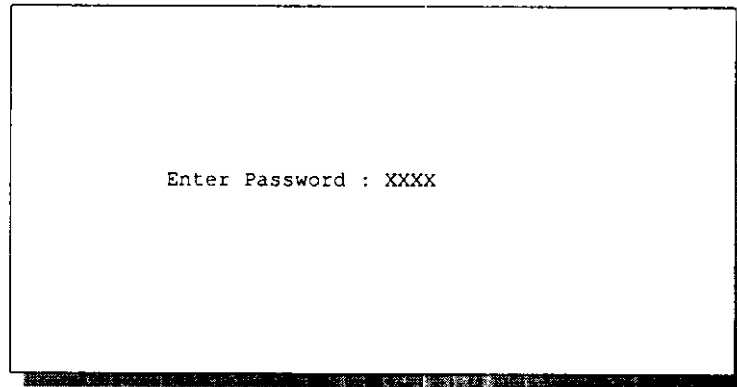


Figure 2-3. Login Screen

Note that once you are in the SMT and if there is no activity for longer than 5 minutes, your *Prestige* will automatically log you out and will display a blank screen. If you see a blank screen, press [Enter] to bring up the password screen.

2.5 Navigating the SMT Interface

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

Several operations that you should be familiar with before you attempt to modify the configuration are listed in Table 2-2.

Table 2-2. Main Menu Commands

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

The SMT displays the Main Menu, as shown in Figure 2-4.

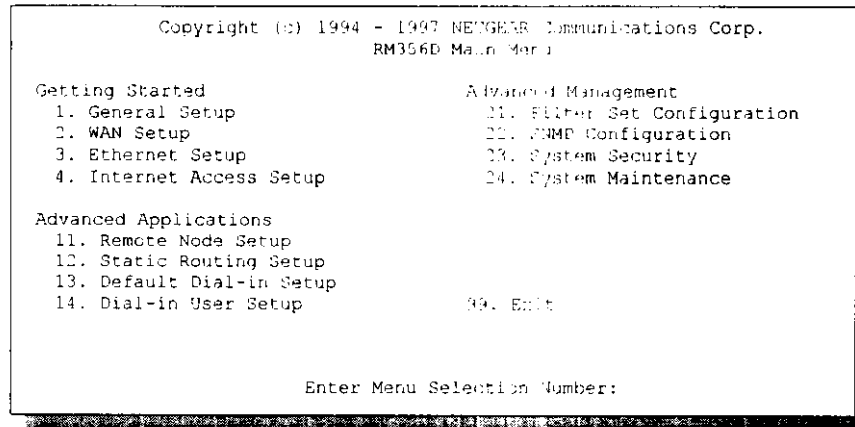


Figure 2-4. SMT Main Menu

System Management Terminal Interface Summary

Table 2-3. Main Menu Summary

#	Menu Title	Description
1	General Setup	Access this menu to setup general information and enable routing or bridging of specific protocols.
2	WAN Setup	Access this menu to setup WAN port configuration.
3	Ethernet Setup	Access this menu to setup Ethernet configuration.
4	Internet Access Setup	A quick and easy way to setup Internet connection.
11	Remote Node Setup	Access this menu to setup the Remote Node for LAN-to-LAN connection, including Internet connection. <i>Prestige</i> supports up to four Remote Nodes.
12	Static Routing Setup	Access this menu to setup static route for different protocols. There are four static routes for each protocol.
13	Default Dial-in Setup	Access this menu to setup default dial-in parameters so that your <i>Prestige</i> can be a dial-in server for the Remote Node and Remote Dial-in User.
14	Dial-in User Setup	Setup Remote Dial-in User. <i>Prestige</i> has eight Remote Dial-in Users.
21	Filter Set Configuration	Setup filters to be used in Menu 3 and Menu 11 to provide security, call control, etc.
22	SNMP Configuration	Access this menu to setup SNMP related parameters
23	System Security	Access this menu to setup security related parameters.
24	System Maintenance	Provides system status, diagnostics, firmware upload, etc.
99	Exit	To exit from SMT and return to the blank screen.

2.6 Configure the SMT Password

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

- Step 1.** Select option **[23. System Security]** in the Main Menu. This will open Menu 23 - System Security as shown in Figure 2-5.

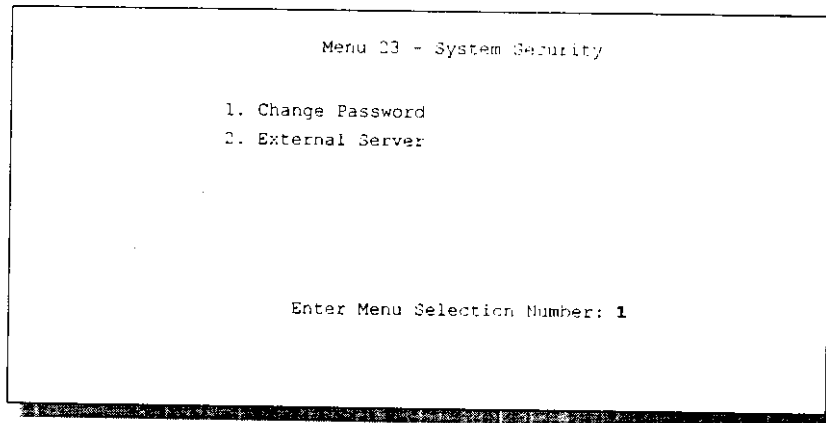
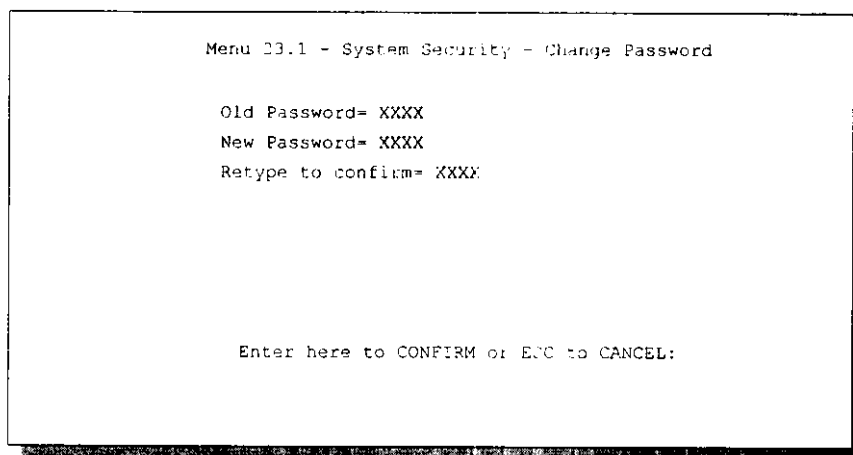


Figure 2-5. Menu 23 - System Security

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

- Step 3.** When the Submenu 23.1- System Security-Change Password appears, as shown in Figure 2-6, type in your previous system password, then press [Enter].



```
Menu 23.1 - System Security - Change Password

Old Password= XXXX
New Password= XXXX
Retype to confirm= XXXX

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

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

- Step 4.** Enter your new system password and press [Enter].
Step 5. Re-type your new system password for confirmation and press [Enter].

You will now need to enter this password every time you attempt to access the SMT. In addition, the password is required when a network administrator attempts to access your *Prestige* via a Telnet connection.



Note on Password Display

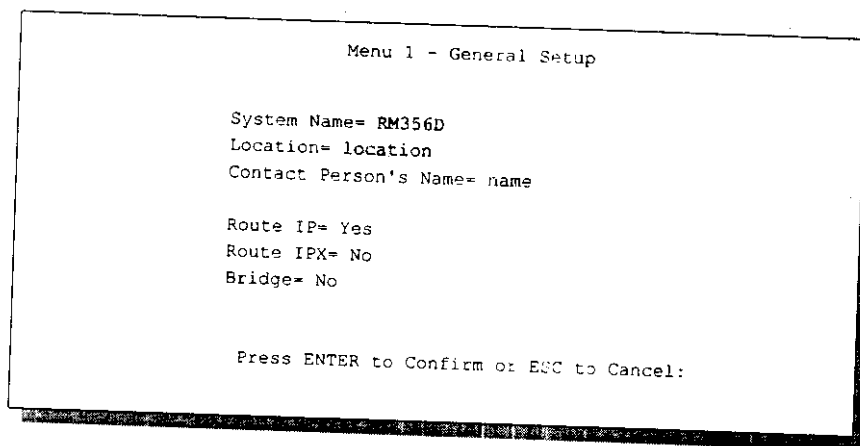
As you type a password, the screen displays a (X) for each character you type.

2.7 General Setup

The 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.** Select option [1. General Setup] in the Main Menu by typing 1 at the menu selection number prompt.
- Step 2.** The Menu 1 - General Setup screen appears, as shown in Figure 2-7. Fill in the required fields marked [?] and turn on the individual protocols for your particular application, as explained in Table 2-4.



```
Menu 1 - General Setup

System Name= RM356D
Location= location
Contact Person's Name= name

Route IP= Yes
Route IPX= No
Bridge= No

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

Figure 2-7. Menu 1 - General Setup

Table 2-4. General Setup Menu Fields

Field	Description	Example
System Name	Choose a descriptive name for identification purposes. This name can be up to 8 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted. This name can be retrieved remotely via SNMP, used for CHAP authentication, and will be displayed at the prompt in the Command Mode.	RM356D
Location (optional)	Enter the geographic location (up to 31 characters) of your <i>Prestige</i> .	location
Contact Person's Name (optional)	Enter the name (up to 8 characters) of the person in charge of this <i>Prestige</i> .	name
Protocols:	Turn on or off the individual protocols for your particular application. Unsupported protocols will display a [N/A] in their fields.	Press space-bar to toggle
Route IP	Set this field to [Yes] if you are configuring your <i>Prestige</i> for Internet Access.	[Yes/No]
Route IPX	Selecting [Yes] will let your <i>Prestige</i> route IPX protocol applications.	[Yes/No]
Bridge	Bridging is used for protocols that are not supported (for example, SNA) or not turned on in the previous Route fields.	[Yes/No]

**Note on Route IP, IPX Protocols and Bridge**

Your *RM356D* is a multi-protocol Router/Hub that can support any combinations of Route IP, Route IPX, and Bridge.

If Route IP is set to [Yes] and Bridge set to [Yes] your *Prestige* functions as a **Router & Bridge**.

If Route IP is set to [Yes] and Bridge set to [No] your *Prestige* functions as a **Router Only**.

If Bridge is set to [Yes] and Route IP set to [No] your *Prestige* function as a **Bridge Only**.

**Note on Bridge**

When bridging is enabled, your *Prestige* will forward any packet that it does not recognize.

Otherwise, the unrecognized packets are discarded. The disadvantage of bridging is that it usually generates large amounts of traffic.

2.8 WAN Setup

This section describes how to configure the WAN ports on your *RM356D* by using Menu 2- WAN Setup. The Menu 2 - WAN Setup is used for entering information about your Modem or ISDN TA connected to the serial port WAN Port 1 and the modem line connected internally to WAN port 2 or 3 (LINE 1,2). Select a WAN Port (# 1,2, or 3) that you wish to configure first. Then configure the WAN Port from Submenu 2.1. If advanced setup is required, go into Menu 2.2. When you are finished, press [Enter] in Menu 2.1. Your *Prestige* will save the information to ROM first; then use this information to initialize the Wan Port and the attached modem or ISDN TA.



Note on WAN Setup

Before you connect a leased line modem or ISDN TA to your *Prestige*, make sure to configure the device accordingly. To configure the modem or ISDN TA, refer to the instructions provided by the manufacturer

2.8.1 *RM356D* WAN Port Setup

RM356D supports three WAN port connections with Modems or ISDN TAs.

To configure the WAN ports on *RM356D*, follow these steps:

- Step 1.** Select option [2. WAN Setup] in the Main Menu by typing 2 at the menu selection number prompt.
- Step 2.** In Menu 2 - WAN Port Setup, as shown in Figure 2-8, enter the number (1,2, or 3) of the WAN port you wish to configure.
- Select option [1. Wan Port 1(External)] to setup the WAN port 1 with external modem or ISDN TA parameters.
 - Select options [2,3 Wan Port 2,3(Internal)] to configure the Internal 56K Modems on WAN Port 2 and 3.

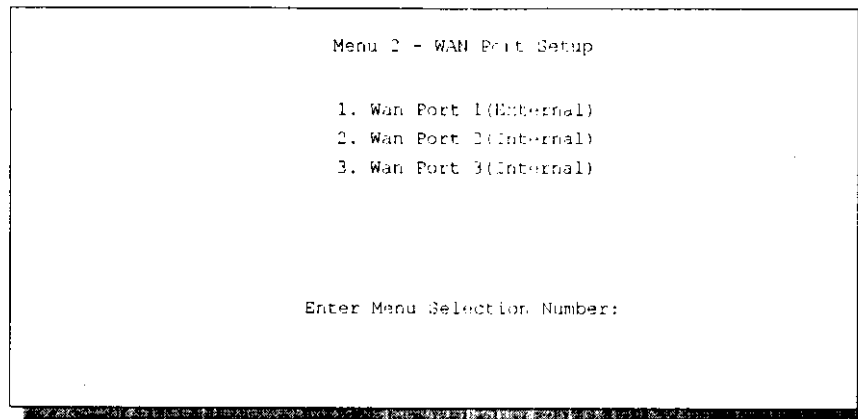


Figure 2-8. Menu 2 - WAN Port Setup

Step 3. This will bring up Menu 2.1 - Async WAN Port Setup, as shown in Figures 2-9a, 2-9b. In Menu 2.1 you can set the configuration parameters for the selected WAN port.

- Figure 2-9a shows how to configure WAN port 1 connected to an external modem or ISDN TA.

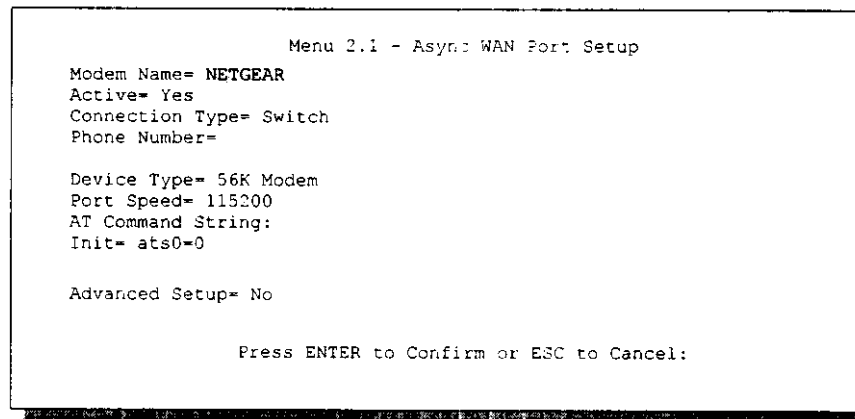


Figure 2-9a. Menu 2.1 - Async WAN Port Setup for Serial WAN Port 1

- Figure 2-9b displays Menu 2.1 when configuring WAN port 2 and 3 internally connected to the built-in 56K modem LINE 1 and LINE 2 respectively.

```

Menu 2.1 - Async WAN Port Setup

Modem Name= NETGEAR
Active= Yes
Connection Type= Switch (r.o.)
Phone Number=

Device Type= 56K Modem (r.o.)
Port Speed= 115200
AT Command String:
Init=ats0=0W1&fs95=1

Advanced Setup= No

Press ENTER to Confirm or ESC to Cancel:

```

Figure 2-9b. Menu 2.1 - Async WAN Port Setup for WAN Port 1,2 (LINE 1,2)

Table 2-5 describes how to configure the WAN port 1 with the external modem or ISDN TA parameters, and WAN port 2 and 3 with the internal 56K modem line parameters.

Table 2-5. Async WAN Port Setup Menu Fields

Field	Description	Example
Modem Name	Enter a descriptive name for the Modem or ISDN TA connected to this WAN Port.	NETGEAR
Active	Set to [Yes] to activate a WAN port, then your <i>Prestige</i> will initialize the WAN Port and the attached Modem or ISDN TA. When a WAN Port is deactivated, it has no effect on the operation of your <i>Prestige</i> , even though its profile is still kept in the database, and can be activated in the future.	Press space-bar to toggle [Yes/No]
Connection Type	For WAN Port 1 (Serial WAN port connected to external modem or ISDN TA), select the connection type for your particular application. Select [Switch] for Dial-up application or [Leased] for Leased Line Modem application.	Press space-bar to toggle [Switch/Leased]

Table 2-5. Async WAN Port Setup Menu Fields (continued)

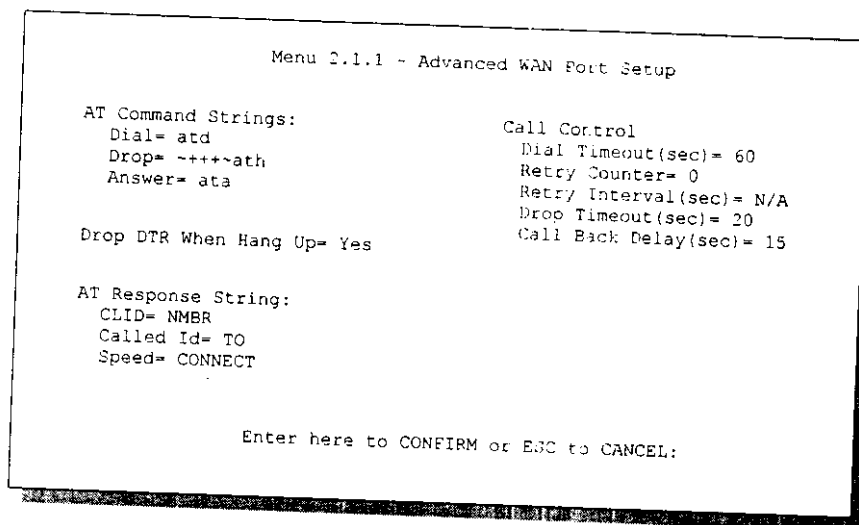
Connection Type	For WAN Port 2 and 3 (LINE 1 and LINE 2 ports with internal 56K modems), this field is read only (r.o.). The connection type is set to [Switch] for Dial-up line applications only.	[Switch (r.o.)]
Phone Number	Enter the telephone number assigned to your modem line by your telephone company. Note that your <i>Prestige</i> only accepts digits; do not include dashes and spaces in this field.	5551212 (example)
Device Type	For WAN Port 1 (Serial WAN port connected to external modem or ISDN TA), use the space bar to select one of the following devices: [Modem / ISDN TA / X.25 PAD / 56K Modem]. A Device Type is selected for the WAN Port such that a Remote Node only picks up a free device of the selected type to dial out. Only the WAN Ports of the same device type can be bundled. This field is not applicable if the Connection Type is set to [Leased].	Space-bar to toggle [Modem] [ISDN TA] [X.25 PAD] [56K Modem]
Device Type	For WAN Port 2 and 3 (LINE 1 and LINE 2 ports with internal 56K modems), this field is read only (r.o.). The device type is set to [56K Modem] which corresponds to the 56K modems built in your <i>RM356D</i> .	[56K Modem (r.o.)]
Port Speed	Use the space bar to select the maximum speed of your Modem or ISDN TA. Available speeds are: 9600 / 19200 / 38400 / 57600 / 115200 / 230000 bps Note that the port speed is set to 56Kps for WAN port 2 and 3 with internal modems.	115200 (default)
AT Command String: Init	Enter an AT command string to initialize the modem or ISDN TA attached to the WAN Port. When the Connection Type is set to [Switch], you must enter an AT command (ats0=0) to disable auto answer (i.e. ats0=0) or your <i>Prestige</i> will answer the incoming phone call. Note the default AT command string [at&s95=1] for dial-up applications with internal 56K modem.	(Default: ats0=0)
Advanced Setup	To edit the Advanced Setup for this Modem/ISDN TA, move the cursor to this field, use the space bar to select [Yes] and press [Enter]. This will bring you to Menu 2.1.1 - Advanced Setup.	[Yes/No]
When you complete this menu, press [Enter] to save your selections, or [Esc] to cancel. After you press [Enter], the <i>Prestige</i> uses the information you have saved to initialize the WAN Port and the connected Modem/ISDN TA.		

2.8.2 Advanced WAN Port Setup

The Advanced WAN Port Setup Menu allows you to configure the AT Commands for the external modem/ISDN TA connected to WAN port 1 and for the built-in 56K modems internally connected to WAN port 2 and 3. Also, this menu lets you configure the call control parameters. For all of *RM356D* WAN ports, follow the common Advanced WAN Port Setup procedure outlined in this section.

Step 1. In Menu 2.1, move the cursor to the Advanced Setup field and press the space bar to select [Yes], then press [Enter].

Step 2. When Menu 2.1.1 appears, fill in the appropriate AT commands and call control parameters for the external modem or ISDN TA connected to the WAN port 1 and for the internal modems on WAN port 2 and 3, as shown in Figure 2-10.



```
Menu 2.1.1 - Advanced WAN Port Setup

AT Command Strings:
Dial= atd
Drop= ~+++~ath
Answer= ata

Drop DTR When Hang Up= Yes

AT Response String:
CLID= NMBR
Called Id= TO
Speed= CONNECT

Call Control
Dial Timeout(sec)= 60
Retry Counter= 0
Retry Interval(sec)= N/A
Drop Timeout(sec)= 20
Call Back Delay(sec)= 15

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

Figure 2-10. Menu 2.1.1 - Advanced WAN Port Setup

Refer to Table 2-6 for details on how to fill in the AT commands fields.

Table 2-6. Advanced WAN Port Setup AT Commands Fields

Field	Description	Default
AT Command Strings:		
Dial	Enter the AT Command string to make a modem/ISDN TA connection.	[atd]
Drop	Enter the AT Command string to drop a modem/ISDN TA connection. [~] represents a one second wait.	[~++++~ath]
Answer	Enter the AT Command string to answer a phone call and make a modem/ISDN TA connection.	[ata]
Drop DTR When Hang Up	When [Yes] is selected, your <i>Prestige</i> will drop the DTR signal after sending out [AT Command String: Drop].	Toggle [Yes/No] (Default=[Yes])
AT Response Strings:		
CLID (Caller Line Identification)	Enter the keyword to capture Caller ID from the AT Response String. Your <i>Prestige</i> will capture CLID from the AT Response String, if they are available. The keyword just before CLID is recognized first; then captures CLID. CLID is required for <i>Prestige</i> callback function or CLID authentication. Not every modem supports CLID.	[NMBR]
Called ID	Enter the keyword to capture Called ID from AT Response String.	[TO]
Speed	Enter the keyword to capture the Connection Speed from AT Response String.	[CONNECT]
When you have completed this menu, press [Enter] to return to Menu 2.1.		

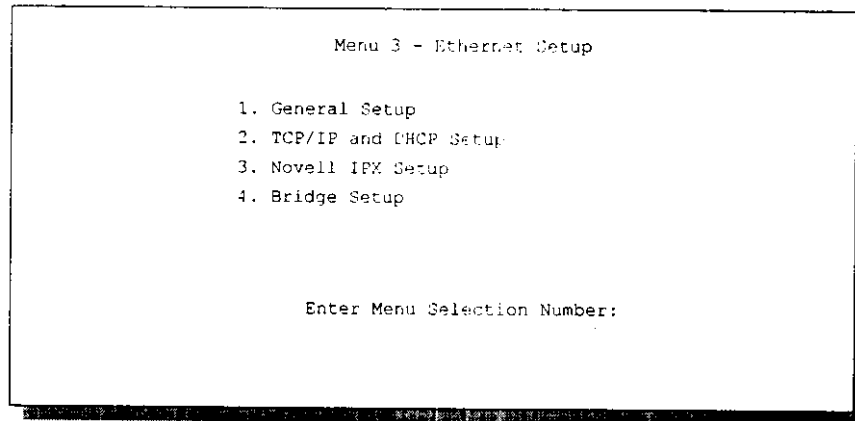
Table 2-7 below describes the call control parameters.

Table 2-7. Advanced WAN Port Setup Call Control Parameters

Field	Description	Default
Dial Timeout (sec)	The <i>Prestige</i> will timeout if it can not set up an outgoing modem call within the timeout value.	[60] seconds
Retry Counter	How many times a busy or no-answer phone number is retried before it is put on the blacklist.	[0] to disable the blacklist control
Retry Interval (sec)	Elapsed time after a call fails before another call may be retried. Applies before a phone number is blacklisted.	
Drop Timeout (sec)	The <i>Prestige</i> will timeout if it can not drop a call within the timeout value.	[20] seconds
Call Back Delay (sec)	Elapsed time between dropping a callback request call and dialing a callback call.	[15] seconds

2.9 General Ethernet Setup

This section describes the Ethernet Setup Menu that you will configure depending on the particular protocol TCP/IP, IPX, or Bridge you are using on your LAN. From the Main Menu, enter 3, then the Menu 3- Ethernet Setup displays as shown in Figure 2-11.



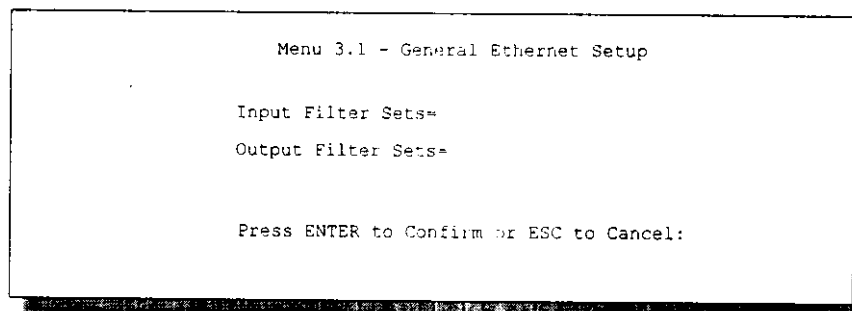
```
Menu 3 - Ethernet Setup

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

Enter Menu Selection Number:
```

Figure 2-11. Menu 3 - Ethernet Setup

This menu determines the type of the filter sets you wish to implement to monitor your Ethernet traffic. From Menu 3 - Ethernet Setup, enter 1 to go to Menu 3.1 -General Ethernet Setup.



```
Menu 3.1 - General Ethernet Setup

Input Filter Sets=
Output Filter Sets=

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

Figure 2-12. Menu 3.1 - General Ethernet Setup

Filters are not required for your *RM356D* to function properly. However, input and output filter sets may be useful to block certain packets, reduce traffic, and prevent a security breach.

If you have a usage for filters, read about *Chapter 9- Filter Set Configuration*, then return to this menu to define the appropriate filter sets.

2.10 Protocol Dependent Ethernet Setup

Depending upon the type of protocol TCP/IP, IPX, or Bridge you are using for your applications, you will be required to configure the Ethernet Setup accordingly.

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

Chapter 3

Internet Access Application

This chapter shows you how to configure your *RM356D* for Internet Access.

3.1 IP Addresses and the Internet

If you are setting up and configuring your network for Internet Access for the first time, read before proceeding. This section contains important information on how to assign IP addresses for your network.

About the Internet

Conventionally, the "Internet" (with a capital I) refers the large-scale interconnected networks across the world. The Internet uses exclusively the TCP/IP suite of protocols. The term "internet" (lower case i), however, refers to any interconnected networks using any protocol. An internet can be as simple as two hosts on a LAN, or it can be as complex as the Internet itself.

IP Addresses

Every machine on the Internet must have a unique address within that internet. An IP Address is required for TCP/IP protocol and usually assigned by your ISP (Internet Service Provider) The IP Address is the unique 32-bit number assigned to your *Prestige*. This address is typically expressed as a sequence of four 8-bit numbers (0-255) in dotted decimal notation (separated by decimal points), for example, 192.68.203.5.

Record the IP Address assigned by your network administrator or MIS specialist.

**Note on IP Address Assignment**

A unique 32-bit IP address is assigned to each host on the Internet. Similarly, every machine on an internet must have a unique IP address. Do not assign an arbitrary address to any machine on your network without prior consulting your network administrator.

IP Subnet Mask

A subnet mask is a 32-bit quantity that, when logically ANDed with an IP address, yields the network number. For instance, the subnet masks for class A, B and C without subnetting are 255.0.0.0, 255.255.0.0 and 255.255.255.0, respectively.

The subnet mask is used to split the IP network addresses to create more network numbers. More network numbers can be created by shifting some bits from the host ID to the network ID. For instance, to partition a class C network number 192.68.135.0 into two, you shift 1 bit from the host ID to the network ID. Thus the new subnet mask will be 255.255.255.128; the first subnet will have network number 192.68.135.0 with hosts 192.68.135.1 to 192.68.135.126 and the second subnet will have network number 192.68.135.128 with hosts 192.68.135.129 to 192.68.135.254.

It is recommended that you use the same subnet mask for all physical networks that share an IP network number. Table 3-1 below lists the additional subnet mask bits in dot decimal notations. To use Table 3-1, write down the original subnet mask and substitute the higher order 0s with the dot decimal of the additional subnet bits. For instance, to partition your class C network 204.247.203.0 with subnet mask 255.255.255.0 into 16 subnets (4 bits), the new subnet mask becomes 255.255.255.240.

Table 3-1. Subnet Mask Notation

Additional Subnet Mask Bits in Dot Decimal Notation	
Number of Bits	Dot Decimal Value
1	128
2	192

Table 3-1. Subnet Mask Notation (continued)

Number of Bits	Dot Decimal Value
3	224
4	240
5	248
6	252
7	254
8	255

Table 3-2 lists some examples of IP subnet masks and the number of hosts that are allowed. Consult your network administrator or MIS specialist if you are unsure of this value.

Table 3-2. Examples of IP Subnet Masks

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

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

Private IP Addresses

If your networks are isolated from the Internet (for example, only between your two branch offices) you can assign arbitrarily 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, as shown in Table 3-2.

For this reason, it is recommended that you choose your private network number from the list provided in Table 3-3.

Table 3-3. Private Networks IP Addresses

Private IP Addresses
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

Assigning IP Addresses

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 on IP Address Assignment

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

3.2 Route IP Setup

The first step in configuring your *Prestige* for Internet Access is to enable the Route IP function in Menu 1 - General Setup.

To edit Menu 1, select the menu option [1. General Setup] in the Main Menu and press [Enter]. When Menu 1 appears, fill in the required fields marked [?] and set the Route IP field to [Yes], as shown in Figure 3-1.

```
Menu 1 - General Setup

System Name= RM356D
Location= location
Contact Person's Name= name
Route IP= Yes
Route IPX= No
Bridge= No

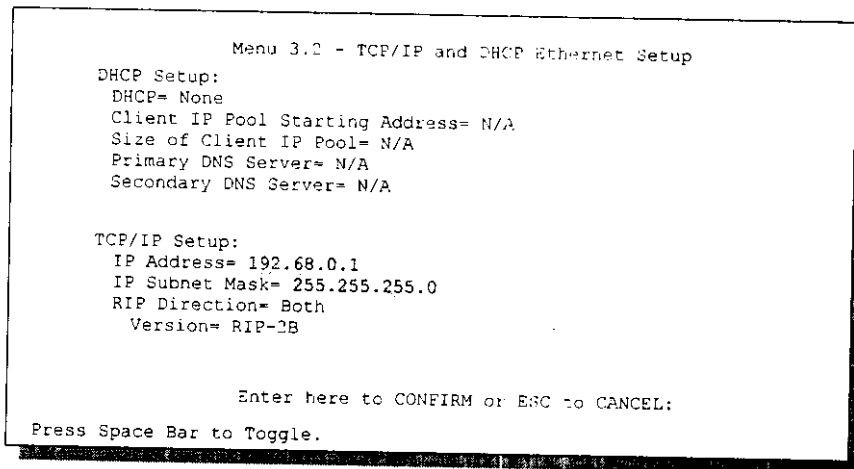
Press ENTER to Confirm or ESC to Cancel:
```

Figure 3-1. Menu 1 - General Setup

3.3 TCP/IP Ethernet Setup and DHCP

You will now configure in Menu 3.2 the Ethernet port of your *Prestige* for a TCP/IP connection.

To edit Menu 3.2, select the menu option **[3. Ethernet Setup]** in the Main Menu. When Menu 3 appears, select the submenu option **[2. TCP/IP and DHCP Setup]** and press **[Enter]**. The screen now displays Menu 3.2 - TCP/IP and DHCP Ethernet Setup, as shown in Figure 3-2.

A screenshot of a text-based menu interface. The title is "Menu 3.2 - TCP/IP and DHCP Ethernet Setup". It is divided into two sections: "DHCP Setup:" and "TCP/IP Setup:". The DHCP section lists "DHCP= None", "Client IP Pool Starting Address= N/A", "Size of Client IP Pool= N/A", "Primary DNS Server= N/A", and "Secondary DNS Server= N/A". The TCP/IP section lists "IP Address= 192.68.0.1", "IP Subnet Mask= 255.255.255.0", "RIP Direction= Both", and "Version= RIP-2B". At the bottom, it says "Enter here to CONFIRM or ESC to CANCEL:" and "Press Space Bar to Toggle.".

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

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

TCP/IP Setup:
  IP Address= 192.68.0.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
  Version= RIP-2B

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

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

Follow the instructions in Table 3-4 on how to configure the DHCP fields.

Table 3-4. DHCP Ethernet Setup Menu Fields

Field	Description	Example
DHCP	This field determines the mode of DHCP (Dynamic Host Configuration Protocol) support. If set to [None], DHCP will not be used. If it is set to [Server], your <i>Prestige</i> will act as a DHCP server, capable of automatically assigning IP addresses to Windows 95, Windows NT, and other systems that support the DHCP client.	[None] (default)
If DHCP=Server:	When DHCP is used, the following four items need to be set:	[Server]
Client IP Pool Starting Address	DHCP can assign IP addresses to hosts dynamically instead of requiring that each system have a fixed IP address. IP addresses are allocated from a block of addresses, usually assigned by your Internet provider. The Client IP Pool Starting Address gives the first address in the reserved block, which is also used as the LAN network address of the <i>Prestige</i> itself. This address will also serve as the default gateway for DHCP clients.	
Size of Client IP Pool	Gives the size of the block of addresses reserved for DHCP address assignment. The <i>Prestige</i> itself uses the first address in the block, and the remaining addresses in the pool are assigned to clients.	
Primary DNS Server Secondary DNS Server	These two fields are used by DHCP clients (such as Windows 95 and Windows NT systems) for Domain Name Servers. Usually your Internet provider will provide one or more name service hosts.	



Note on DHCP

Once you have determined the IP address range for your local network, you may want to use DHCP to assign addresses to individual hosts on the network, as an alternative to manually configuring the IP setting for each host.

Table 3-5 contains instructions on how to configure your *Prestige* for TCP/IP Ethernet Setup.

Table 3-5. TCP/IP Ethernet Setup Menu Fields

Field	Description	Example
TCP/IP Setup		
IP Address	Enter the IP address of your <i>Prestige</i> in dotted decimal notation (four 8-bit numbers, between 0 and 255, separated by periods)Note that every machine on the TCP/IP network must have a unique IP address.	192.68.135.5 (example)
IP Subnet Mask	An IP address consists of two parts, the network ID and the host ID. The IP Subnet Mask is used to specify the network ID portion of the address, expressed in dotted decimal notation. Your <i>Prestige</i> will automatically calculate this mask based on the IP address that you assign. Unless you have special need for subnetting, use the default subnet mask.	255.255.255.0 (default)
RIP Direction	This parameter determines how your <i>Prestige</i> handles RIP (Routing Information Protocol). If set to [Both] (default), your <i>Prestige</i> will broadcast its routing table on the LAN, and incorporate RIP broadcasts by other routers into the routing table. If set to In Only, your <i>Prestige</i> will not broadcast its routing table on the LAN, if set to Out Only, your <i>Prestige</i> will broadcast the routing table but ignores any RIP broadcast packets that it receives. If set to None, your <i>Prestige</i> will not participate in any RIP exchange with other routers. Version: The default is [RIP-2B] Note: Usually, you should use the default RIP [Both], and let RIP propagate the routing information automatically.	[Both] (default)
When you have completed this menu, press [Enter] at the prompt [Press ENTER to Confirm...] to save your selections, or press [Esc] at any time to cancel.		

3.4 Internet Access Configuration

Menu 4 of the SMT allows you to configure Internet Access on one screen. Before you configure your *Prestige* for Internet Access, you need to collect your Internet account information from your ISP (Internet Service Provider).

Use Table 3-6 to record your Internet Account Information.

Table 3-6. Internet Account Information

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

From the Main Menu, enter option [4. Internet Access Setup] to go to Menu 4 - Internet Access Setup, as displayed in Figure 3-3.

```

Menu 4 - Internet Access Setup
ISP's Name= ?
ISP Gateway IP Addr=
Connection Type= Switch
Leased Ports= N/A
Pri Phone #= ?
Sec Phone #=
My Login=
My Password= *****
Single User Account= No
Local IP Addr= N/A
Server IP Addr= N/A
Edit Script Options= No
Device Type= 56K Modem

Enter here to CONFIRM or ESC to CANCEL:

```

Figure 3-3. Menu 4 - Internet Access Setup

Table 3-7 contain instructions on how to configure your *Prestige* for Internet Access.

Table 3-7. Internet Access Setup Menu Fields

Field	Description	Observation
ISP's Name	Enter the name of your Internet Service Provider. (This information is for identification purposes only.)	Myisp
ISP IP Addr	Enter the IP Address of the remote gateway at the ISP's site. If you do not have this data, just leave it blank.	(optional)
Connection Type Leased Ports	Select [Switch] if a Dail-up modem is used to connect to your ISP. Select [Leased] if a Leased Line Modem is used to connect to your ISP. If [Leased] is selected in Connection Type, this field displays the WAN port that supports Leased Line connections. This field is read only (r.o.), since only the serial port WAN port 1 supports, enter the WAN Port numbers in the Leased Line connection. Note: The Connection Type of WAN Port 1 also must be specified as [Leased] in Menu 2.1 - Async WAN Port Setup.	Space-bar to toggle [Switch/Leased] [1 (r.o.)]
Pri(mary) Phone #	The first number your <i>Prestige</i> will dial to connect to the ISP. Once connected, your <i>Prestige</i> will use the BACP (Bandwidth Allocation Control Protocol) to establish the second B-channel if PPP/MP is enabled, and the ISP also supports MP and BACP.	(required)
Sec(ondary) Phone #	If the Primary Phone number is busy or does not answer, your <i>Prestige</i> will call the Secondary Phone number if available.	(optional)
My Login Name	Enter the login name assigned to you by your ISP.	(required)
My Password	Enter the password associated with the login name above. Note that this login name/password pair is only for your <i>Prestige</i> to connect to the ISP's gateway. When you use TCP/IP applications (for example, FTP) to access the Internet from your workstation, you will need a separate login name and password for each server.	(required)

Table 3-7. Internet Access Setup Menu Fields (continued)

Field	Description	Observation
Single User Account	See Section 3.5 for a more detailed discussion on the Single User Account feature.	[Yes/No]
Edit Script Option	To edit the parameters, select [Yes] and press [Enter]. This will bring you to Menu 4.1 - Remote Node Script Options. This field is not applicable if the Connection Type is [Leased].	Space-bar to toggle
Device Type	A Remote Node only picks up a free device of the selected Device Type to dial out. This field is not applicable if the Connection Type is [Leased]. Selections:[Modem/ISDN TA/X.25 PAD/56K Modem]	
Press [Enter] at the message [Press ENTER to Confirm ...] to confirm your selections, or press [Esc] at any time to cancel your selections.		

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

3.5 Single User Account

Typically, if there are multiple users on the LAN wanting to concurrently access the Internet, they will have to subscribe to multiple IP addresses or a Class C sub-network from the ISP. In either case, these two approaches will cost more than a single user account.

The Single User Account (SUA) feature allows customers to have the same benefits as having a Class C address, but still only pay for one IP address, thus saving significantly on subscription fees. (Check with your ISP before you enable this feature).

Figure 3-4 illustrates a typical Single User Account topology.

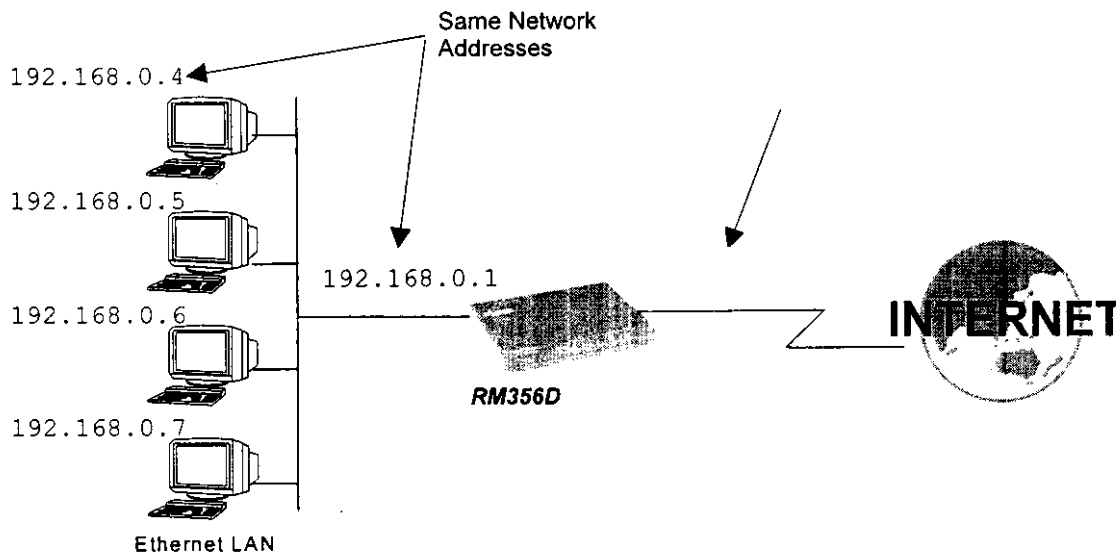


Figure 3-4. Single User Account Topology

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

The IP address for the SUA can be either fixed or dynamically assigned by the ISP (or other remote node). In addition, you can also configure a server (for example, a Web server) on your local network and make it accessible by outside users.

If you do not set a server IP address, SUA offers the additional benefit of firewall protection. With SUA, even if no server is defined, all incoming inquiries will be filtered out by your *Prestige* even if you do have a server on your network. This can prevent intruders from probing your system.

Your *Prestige* accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. For more information on IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

3.5.1 Advantages of SUA

In summary:

- SUA is an ideal cost-effective solution for small offices with less than 20 hosts using a LAN to concurrently access the Internet or other remote TCP/IP network.
- SUA can provide one server address to be accessed by Remote Dial-in Users, thus controlling the incoming packets.
- SUA can provide firewall protection if you do not configure a server IP address. All incoming inquiries will be filtered out by your *Prestige* protecting the servers on your network.
- UDP and TCP datagrams can be routed. In addition, ICMP echo can also be routed.

Figure 3-4 shows an example of a small office connected to the Internet via a SUA using the *Prestige*. Note that if you enable the SUA feature, your local IP address **MUST** be selected from the list of IP addresses for private networks as defined by the IANA.

3.5.2 Configuration for Single User Account

The steps for configuring your *Prestige* for Single User Internet Access are identical to conventional Internet Access (See configuration instructions in Table 3-7) with the exception that you need to fill in three extra fields in Menu 4 - Internet Access Setup, as shown in Figure 3-5.

```
Menu 4 - Internet Access Setup

ISP's Name= ?
ISP Gateway IP Addr=
Connection Type= Switch
Leased Ports= N/A
Pri Phone #= ?
Sec Phone #=
My Login=
My Password=
Single User Account= Yes
Local IP Addr=
Server IP Addr=
Edit Script Options= No
Device Type= 56K Modem

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

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

To enable the SUA feature in Menu 4, move the cursor to the [Single User Account] field and select [Yes] (or [No] to disable SUA). Then follow the instructions on how to configure the SUA fields in Table 3-8.

Table 3-8. Single User Account Menu Fields

Field	Description
Single User Account	Select [Yes] to enable SUA.
Local IP Addr.	If your ISP assigns you a dynamic IP address, enter [0.0.0.0] here. If your ISP assigns you a static IP address, enter that IP address here.
Server IP Addr.	If you want to make a single server (for example, a Web server) accessible to outside users, enter that server's IP address here.
Press [Enter] at the message [Press ENTER to Confirm ...] to save your selections, or press [Esc] at any time to cancel your selections.	

At this point, your *Prestige* will ask if you wish to test the Internet connection. If you select [Yes], the ISP will be called, and the connection tested. If the test fails, note the error message that you receive and take the appropriate troubleshooting steps.

3.6 Configuring Backup ISP Accounts

Sometimes it may be desirable to configure more than one ISP account for backup purposes. The SUA feature can be enabled for all of these accounts, making it convenient to switch Internet Service Providers in the event of a failure.

3.6.1 Configure a Backup ISP

To configure a backup ISP Account, follow these steps:

Step 1. Configure your primary ISP using Menu 4, as described earlier in this chapter.

Step 2. Enter Menu 11, then select the number of an unused remote node.

- Step 3.** In Menu 11.1, choose a name for your backup ISP account, then set the Active field to [No], and enter your outgoing login name, password, and phone number(s). The Remote IP Address field should be set to [1.1.1.1].
- Step 4.** In Menu 11.3, set the remote node's subnet mask to [0.0.0.0], and set RIP to [None].
- Step 5.** Save the new configuration.

3.6.2 To Switch ISP

Once you have done this, if you need to switch from your primary ISP to a backup ISP follow these steps:

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

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

3.7 Editing Script Options

For some ISP, login script handshaking is required after a call connection. The *Prestige* provides four set of programming scripts for this purpose. Each set of script is composed of an 'expect' string and a 'send' string. After capturing of the string in the field of 'expect', the *Prestige* will send out the string in the field of 'send'. If both of Expect and Send fields are empty, the *Prestige* will terminate script handshaking. The Script Options display as shown in Figure 3-6.

```

Menu 11.4 - Remote Node Script

Active= No

Set 1:
  Expect=
  Send=
Set 2:
  Expect=
  Send=
Set 3:
  Expect=
  Send=
Set 4:
  Expect=
  Send=

Set 5:
  Expect=
  Send=
Set 6:
  Expect=
  Send=

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

Figure 3-6. Menu 11.4 - Remote Node Script

The following Table 3-9 describes each field in Menu 11.4 - Remote Node Script.

Table 3-9. Remote Node Script Menu Fields

Field	Description	Option
Active	Press the space bar to toggle between [Yes] and [No]. When a Remote Node Script is deactivated, it has no effect on the operation of your <i>Prestige</i> , even though it is still kept in the database, and can be activated in the future.	Press space bar to toggle [Yes/No]
Set 1-6: Expect	Enter an Expect string to capture. After capturing the Expect string, the <i>Prestige</i> will send out the string in the [Send] field.	
Set 1-6: Send	Enter a string to send out after the Expect string is captured.	

Chapter 4

Telecommuting

You can configure your *Prestige* to receive calls from Remote Dial-in Users (for example, Telecommuters) and Remote Nodes. There are several differences between Remote Dial-in Users and Remote Nodes, as summarized in Table 4-1.

Table 4-1. Remote Dial-in Users/Remote Nodes Comparison Chart

Remote Dial-in Users	Remote Nodes
Your <i>Prestige</i> will only answer calls from Remote Dial-in Users.	Your <i>Prestige</i> can make calls to or answer calls from the Remote Node.
All Remote Dial-in Users share one common set of parameters, as defined in the Default Dial In Setup (Menu 13).	Each Remote Node can have its own set of parameters such as Bandwidth On Demand, Protocol, Security, etc.
Remote Dial-in Users are individual users who dial in to your <i>Prestige</i> directly from their workstations.	Remote Nodes represent networks and are used for LAN-to-LAN connections.

This chapter discusses how to setup Default Dial-in parameters for both Remote Node and Remote Dial-in Users. The following sections give two examples of how your *Prestige* can be configured as a dial-in server for either or both.

By default, your *Prestige* allows information for up to eight users to be kept. If more than eight remote dial-in users can access your *Prestige*, you can use a separate RADIUS server to provide remote authentication services. For details on using a separate RADIUS server, see the *Using RADIUS Authentication* section in *Chapter 11 - System Security*.

4.1 Telecommuting

Telecommuting enables people to work at remote sites and yet still have access to the resources in the business office. Typically, a telecommuter will use a client workstation with TCP/IP or IPX and dial-out capabilities (for example, a Windows 95 PC or a Macintosh) connected to a Modem or an ISDN Terminal Adapter (ISDN TA). For telecommuters to call in to your LAN, you need to configure a Dial-In User Profile for each telecommuter. Additionally, you need to configure the Default Dial-In Setup to set the operational parameters for all dial-in users. You can configure up to eight Remote Dial-in Users for your *Prestige*.

An example of Remote Dial-in User application, telecommuting, is shown in Figure 4-1.

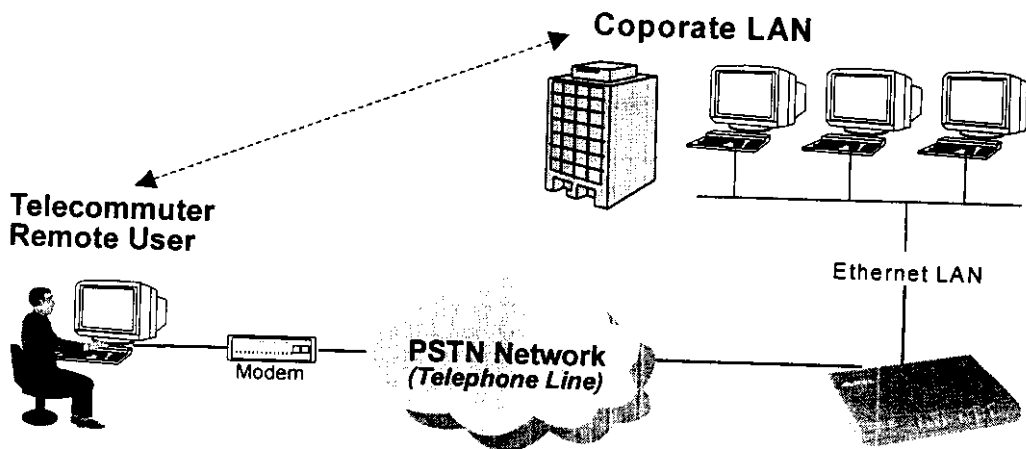


Figure 4-1. Example of Remote User: Telecommuter

4.2 Dial-In Server Application

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

An example of your *Prestige* being used as a dial-in server is shown in Figure 4-2.

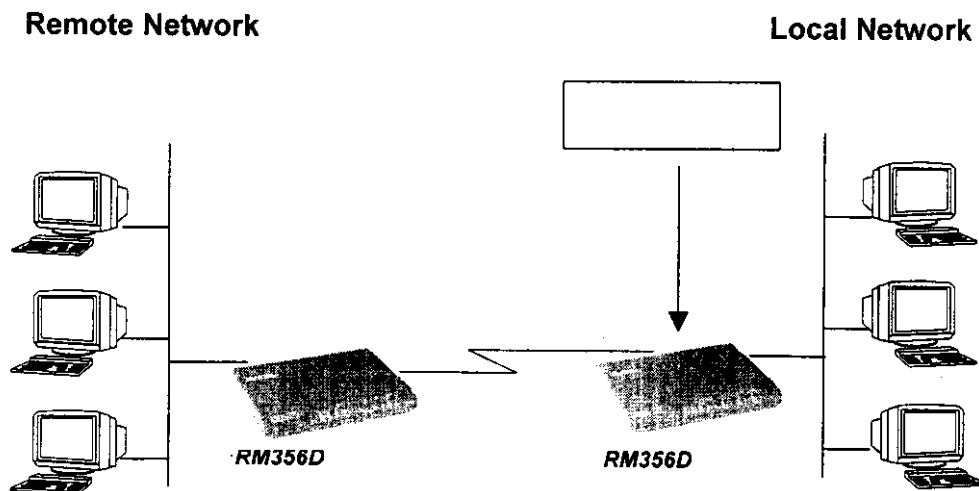


Figure 4-2. Example of a Dial-in Server Application

4.3 Default Dial-In Setup

This section covers the default dial-in parameters. The parameters in Menu 13 affect incoming calls from all Remote Dial-in Users and Remote Nodes before authentication is completed. Once authentication is completed, and if it matches a Remote Node, your *Prestige* will use parameters from that particular Remote Node.

```

Menu 13 - Default Dial-in Setup

Telco Options:                      IP Address Supplied By:
  CLID Authen= None                 Dial-in User= Yes
                                   IP Pool= No
                                   IF Start Addr= N/A
                                   IF Count(1,3)= N/A

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

Session Options:
  Callback Budget Management:
    Allocated Budget(min)=
    Period(hr)=
  Input Filter Sets=
  Output Filter Sets=
  Idle Timeout= 300

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

```

Figure 4-3. Menu 13 - Default Dial-in Setup

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

Table 4-2 describes and contains information on how to configure each parameter in Menu 13 - Default Dial-in Setup.

Table 4-2. Default Dial-in Setup Fields

Field	Description	Option
Telco Options: CLID Authen	This field sets the CLID authentication parameter for all incoming calls. There are three options for this field: ● None - No CLID is required. ● Required - Must provide CLID, or call is disconnected. ● Preferred - If the CLID is available then CLID will be used to do authentication. If the CLID is not available the call will continue.	[None] [Required] [Preferred]
PPP Options: Recv. Authen	This field sets the authentication protocol used for incoming calls. User names and passwords are configured in the next section (Remote users/Dial-in Users Setup). Options for this field are: ● CHAP/PAP - Your <i>Prestige</i> will try CHAP first, but PAP will be used if CHAP is not available. ● CHAP - Use CHAP only. ● PAP - Use PAP only. ● None - Your <i>Prestige</i> tries to acquire CHAP/PAP first, but no authentication is required if CHAP/PAP is not available.	[CHAP/PAP] [CHAP] [PAP] [None]
PPP Options: Mutual Authen	Some vendors (for example, Cisco) implement a type of mutual authentication. That is, the node that initiates the call will request a user name and password from the far end that they are dialing to. If the Remote Node that is dialing in implements this type of authentication, set this field to Yes.	[Yes/No]
PAP Login	This field will only be enabled if the Mutual Authen. Field is set to [Yes]. Enter in the login name to be used to respond to the far end's PAP authentication request. This field does not apply to CHAP authentication.	
PAP Password	This field will only be enabled if the Mutual Authen. Field is set to [Yes]. Enter in the PAP password to be used to respond to the far end's authentication request. This field does not apply to CHAP authentication.	

Table 4-2. Default Dial-in Setup Fields (continued)

Field	Description	Option
Multiple Link Options: Max Port	Enter the maximum number of ports in a connection between your <i>Prestige</i> and the Remote Dial-in User.	Default = 1
Callback Budget Management: Allocated Budget (min)	This field will set a budget callback time for all the Remote Dial-in Users. The default for this field is [0] for no budget control.	Default = 0
Callback Budget Management: Period (hr)	This field will set the time interval to reset the above callback budget control.	
Dial-In IP Address Supplied By: Dial-in User	If set to [Yes], it tells your <i>Prestige</i> to allow a remote host to specify its own IP address. This is to prevent the remote host from using an invalid IP address and potentially disrupting the whole network. If set to [No], the remote host must use the IP address assigned by your <i>Prestige</i> from the IP pool, configured below.	(Default = Yes) [Yes/No]
Dial-In IP Address Supplied By: IP Pool	This field tells your <i>Prestige</i> to provide the remote host with an IP address from the pool. This field is required if Dial-In IP Address Supplied By: Dial-in User is set to [No]. You can configure this field even if Dial-in User is set to [Yes], in which case your <i>Prestige</i> will accept the IP address if the remote peer specifies one; otherwise, an IP address is assigned from the pool.	[Yes/No] (Default = No)
IP Pool: IP Start Addr	This field is active only if you selected [Yes] in the Dial-In IP Address Supplied By: IP Pool field. The IP pool contains contiguous IP addresses and this field specifies the first one in the pool.	
IP Count (1-3)	In this field, enter the number ([1], [2], or [3]) of the addresses in the IP Pool. For example, if the starting address is 192.168.135.5 and the count is [2], then the pool will have 192.68.135.5 and 192.68.135.6	[1], [2], [3]

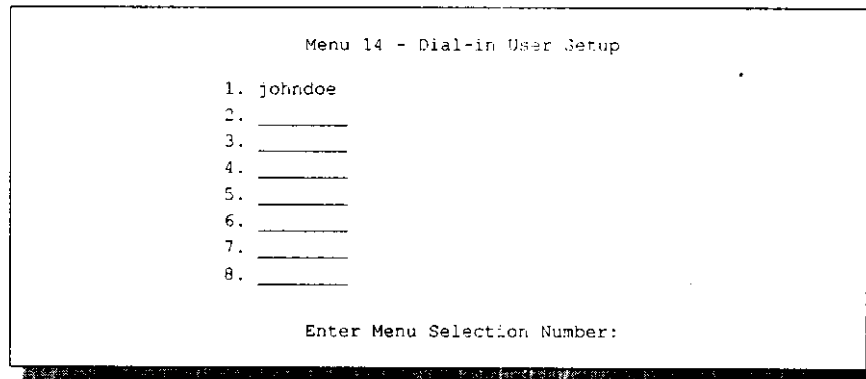
Table 4-2. Default Dial-in Setup Fields (continued)

Field	Description	Option
Dial-In IPX Net. Num. Supplied By: IPX Pool	This field tells your <i>Prestige</i> to provide the remote host with an IPX network number from the pool. Otherwise, your <i>Prestige</i> will generate a random IPX network number.	[Yes/No] (Default = No)
IPX Start Net. Num.	This field is active only if you selected [Yes] in the Dial-In IPX Net. Num. Supplied By: IPX Pool field. The IPX pool contains contiguous IPX network numbers and this field specifies the first one in the pool.	
IPX Count (1,16)	In this field, enter the number ([1] - [16]) of network numbers in the IPX Pool. For example, if the starting number is 12345678, and the count is [2], then the IPX pool will have 12345678 and 12345679.	[1] to [16]
Session Options: Input Filter Sets Output Filter Sets	In these fields, you need to select the filter set(s) to filter the incoming and outgoing traffic between your <i>Prestige</i> and the Remote Dial-in User. Keep in mind that these filter set(s) will only apply to all Remote Dial-in Users but not the Remote Nodes. You can choose from 12 different filter sets. In addition, you can link up to 4 filter sets together for further customization (for example, 1, 5, 9, 12). Note that spaces and [-] symbol, are accepted in this field. For more information on customizing your filter sets, see <i>Chapter 9 - Filter Configuration</i>. The default is blank, i.e., no filters.	Default = blank
Session Options: Idle Timeout	This value is the number of idle seconds that elapses before the dial-in user is automatically disconnected. Idle Timeout is the period of time when there is no data traffic between the dial-in user or Remote Node and your <i>Prestige</i>. This field will only be used if the Recv. Authen field is set to [None] and the call is not mapped to any Remote Node or Remote Dial-in User or your <i>Prestige</i> calls back to the Remote Dial-in User.	
Once you have completed filling in Menu 13 - Default Dial-in Setup, press [Enter] at the message [Press ENTER to Confirm...] to save your selections, or press [Esc] at any time to cancel your selections.		

4.4 Dial-In Users Setup

The following steps describe the setup procedure for adding a Remote Dial-in User.

- Step 1.** From the Main Menu, enter option 14 to go to Menu 14 - Dial-in User Setup, as shown in Figure 4-4.

A screenshot of a terminal window showing the 'Menu 14 - Dial-in User Setup' screen. The screen displays a list of eight numbered options, with the first option '1. johndoe' filled in. Below the list, it prompts the user to 'Enter Menu Selection Number:'.

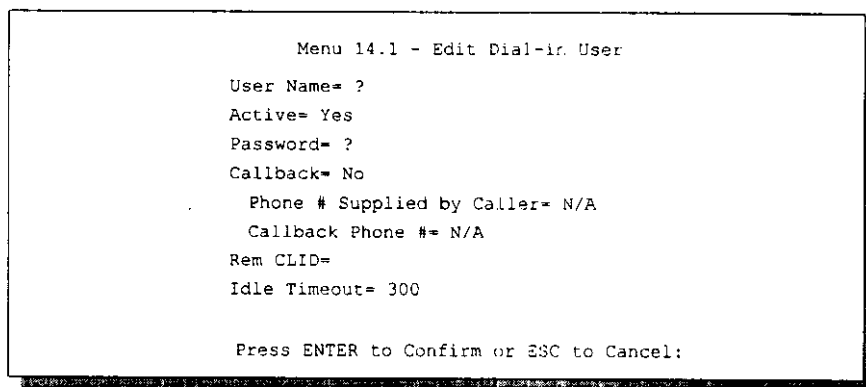
```
Menu 14 - Dial-in User Setup

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

Enter Menu Selection Number:
```

Figure 4-4. Menu 14 - Dial-in User Setup

- Step 2.** Select one of eight users by number, this will bring you to Menu 14.1 - Edit Dial-in User, as shown in Figure 4-5.

A screenshot of a terminal window showing the 'Menu 14.1 - Edit Dial-in User' screen. The screen displays various user configuration fields with their current values. At the bottom, it prompts the user to 'Press ENTER to Confirm or ESC to Cancel:'.

```
Menu 14.1 - Edit Dial-in User

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

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

Figure 4-5. Menu 14.1 - Edit Dial-in User

Table 4-3 provides instructions on how to fill in the Edit Dial-In User fields.

Table 4-3. Edit Dial-in User Menu Fields

Field	Description	Option
User Name	This is a required field. This will be used as the login name for authentication. Choose a descriptive word for login, for example, [johndoe].	
Active	You can disallow dial-in access to this user by setting this field to [Inactive]. When set to [inactive], the user record is still kept in the database for later activation. Deactivated users are displayed with a [-] (minus sign) at the beginning of the name in Menu 14.	[Active] [Inactive]
Password	Enter the password for the Remote Dial-in User.	
Callback	This field determines if your <i>Prestige</i> will allow call back to the Remote Dial-in User upon dial-in. If this option is enabled, your <i>Prestige</i> will be able to call back to the Remote Dial-in User if they request it. In such a case, your <i>Prestige</i> will disconnect the initial call from this user and dial back to the specified callback number (see below). • [No] - The default is [no callback]. • [Optional] - The user can choose to disable callback. • [Mandatory] - The user can not disable callback.	Default=No [No] [Optional] [Mandatory]
Phone # Supplied by Caller	This option allows the Remote Dial-in User to specify the call back telephone number on a call-by-call basis. This is useful for when your <i>Prestige</i> returns a call back to a mobile user at different numbers (for example, a Sales Rep. in a hotel). • If the setting is [Yes], the user can specify and send to the <i>Prestige</i> the callback number of his/her choice. • Note that the default is [No], that is your <i>Prestige</i> always calls back to the fixed callback number.	Default=No [Yes] [No]
Callback Phone #	If [Phone # Supplied by Caller] is [Yes], then this is a required field. Otherwise, a [N/A] will appear in the field. Enter the telephone number to which your <i>Prestige</i> will call back.	

Table 4-3. Edit Dial-in User Menu Fields (continued)

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

4.5 More on CLID

CLID allows your *Prestige* to authenticate the caller before a call is answered, thus saving the cost of a connection. Your *Prestige* uses the caller ID in call setup message to match against the CLID in the database.



Note on CLID and Modems

For your *Prestige* to use the CLID authentication, it is necessary that your modem also support caller CLID.

Besides authentication, another application of CLID is to combine it with callback. For instance, your company pays for the connection charges for telecommuting employees and you use your *Prestige* as the dial in server. You can turn on both the CLID authentication and call back options for the dial-in users. By doing so, all usage are charged to the company instead of the employees, and your accounting department can avoid the hassles of accountability and reimbursement.

Chapter 5

Remote Node Configuration for LAN-to-LAN

A Remote Node represents both a remote gateway and the internet behind it, across a WAN connection. A Remote Node is required for placing calls to or answering calls from a remote network. Note that when you use Menu 4 to configure the Internet, your *Prestige* will automatically add a Remote Node for you. Once a Remote Node is configured properly, traffic to the remote LAN will trigger your *Prestige* to make a call automatically (i.e., Dial On Demand). Similarly, calls from the remote LAN will be answered automatically and security will be checked.

In this chapter, we will discuss the parameters that are protocol independent. The protocol-dependent configuration will be covered in subsequent chapters. For TCP/IP, see *Chapter 6*. For IPX, see *Chapter 7*. For Bridging, see *Chapter 8*.

5.1 Remote Node Setup

This section describes the configuration of protocol-independent parameters for the Remote Node.

5.1.1 Remote Node Profile

To configure the Remote Node parameters, follow these steps:

- Step 1.** From the Main Menu, select menu option [11. Remote Node Setup]
- Step 2.** When Menu 11 appears, as shown in Figure 5-1, enter the number of the Remote Node (1-4) that you wish to configure.

```

Menu 11 - Remote Node Setup

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

Enter Node # to Edit:

```

Figure 5-1. Menu 11 - Remote Node Setup

Step 3. When Submenu 11.1. - Remote Node Profile appears, select the connection type depending on your particular application (dial-up line or leased line application). Move the cursor to the Connection Type field and use the space bar to toggle (Switch/Leased). Set the Connection Type to one of the following values:

- [Switch]: for Dial-up Line Application, as shown in Figure 5-2.
- [Leased]: for Leased Line Application. Selecting [Leased] will bring you to the Submenu 11.1.2 - Remote Node Profile for leased line application.

```

Menu 11.1 - Remote Node Profile

Rem Node Name= ?      Device Type= 56K Modem
Active= Yes           Route= IP
Connection Type= Switch Bridge= No
Call Direction= Both Edit PPP Options= No
Incoming:             Rem IP Addr= ?
  Rem Login= ?        Edit IP/IPX/Bridge= No
  Rem Password= ?     Edit Script Options= No
  Rem CLID=           Telco Option:
  Call Back= No       Allocated Budget(min)= 0
Outgoing:             Period(hr)= 0
  My Login= ?         Session Options:
  My Password= ?      Input Filter Sets=
  Authen= CHAP/PAP    Output Filter Sets=
  Pri Phone #= ?      Call Filter Sets=
  Sec Phone #=        Idle Timeout(sec)= 300

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

```

Figure 5-2. Menu 11.1 - Remote Node Profile for Dial-up Line Applications

Table 5-1 contains the instructions on how to configure the Remote Node Menu for Dial-up Line applications.

Table 5-1. Remote Node Profile Menu Fields for Dial-up Line Applications

Field	Description	Options
Rem Node Name	This is a required field [?]. Enter a descriptive name for the Remote Node, for example, SJHQ. This field can support up to eight characters. This name must be unique from any other Remote Node name or Remote Dial-in User name.	
Active	Press the space bar to toggle between [Yes] and [No]. When a Remote Node is deactivated, it has no effect on the operation of your <i>Prestige</i>, even though it is still kept in the database, and can be activated in the future. Deactivated nodes are displayed with a minus sign (-) at the beginning of the name in Menu 11.	Press space bar to toggle [Yes/No]
Connection Type	Use the space bar to toggle between [Switch] and [Leased]. After [Leased] is selected, moving the cursor to the next field will bring you to Submenu 11.1.2 for a Leased Line Modem application.	Press space bar to toggle [Switch/Leased]
Call Direction	● If this parameter is set to [Both], your <i>Prestige</i> can both place and receive calls to/from a Remote Node. ● If set to Incoming, your <i>Prestige</i> will not place a call to a Remote Node. ● If set to Outgoing, your <i>Prestige</i> will drop any call from a Remote Node. Several other fields in this menu depend on this parameter. For example, in order to enable [Call Back], the Call Direction must be [Both].	[Both] [Incoming] [Outgoing]

Table 5-1. Remote Node Profile Menu Fields for Dial-up Line Applications (continued)

Field	Description	Options
Incoming: Rem Node Login Name	Enter the login name that this Remote Node will use when it calls into your <i>Prestige</i> . The login name in this field combined with the Rem Node Password will be used to authenticate the incoming calls from this node.	
Incoming: Rem Node Password	Enter the password used when this Remote Node calls into your <i>Prestige</i> .	
Incoming: Rem CLID	This field is active only if [Call Direction] is either [Both] or [Incoming]. Otherwise, an [N/A] appears in the field. This is the Calling Line ID (the telephone number of the calling party) of this Remote Node. If you enable the CLID Authen field in Menu 13 - Default Dial In, your <i>Prestige</i> will check this number against the CLID in the incoming call. If they do not match and the CLID Authen is Required, the call will be rejected.	[Both] [Incoming] [N/A]
Incoming: Call Back	This field will be valid only if [Call Direction] is [Both]. Otherwise, an [N/A] appears in the field. This field determines whether or not your <i>Prestige</i> will call back after receiving a call from this Remote Node. If this option is enabled, your <i>Prestige</i> will disconnect the initial call from this node and call it back at the Outgoing Primary Phone Number (see below).	[Enable] [Disable]
Outgoing: My Login Name	This is a required field [?] if [Call Direction] is either [Both] or [Outgoing]. Enter the login name for your <i>Prestige</i> when it calls this Remote Node.	

Table 5-1. Remote Node Profile Menu Fields for Dial-up Line Applications (continued)

Field	Description	Options
Outgoing: My Password	This is a required field [?] if [Call Direction] is either [Both] or [Outgoing]. Enter the password for your <i>Prestige</i> when it calls this Remote Node.	
Outgoing: Authen	This field sets the authentication protocol used for outgoing calls. Your <i>Prestige</i> supports two authentication protocols: PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). ● PAP sends the user name and password in plain text. ● CHAP scrambles the password before it is sent over the wire. Generally speaking, CHAP is more secure than PAP; however, PAP is readily available on more platforms. The recommendation is to use CHAP whenever possible. Turning off the authentication is STRONGLY discouraged. Options for this field are: ● CHAP/PAP - Your <i>Prestige</i> will try CHAP when CHAP is requested by the Remote Node or PAP when PAP is requested by the Remote Node. ● CHAP - use CHAP only. ● PAP - use PAP only.	[CHAP/PAP] [CHAP] [PAP]

Table 5-1. Remote Node Profile Menu Fields for Dial-up Line Applications (continued)

Field	Description	Options
Outgoing: Pri(primary) Sec(ondary) Phone Numbers	Both the Primary Phone number and the Secondary Phone number refer to the number that your <i>Prestige</i> will dial to connect to the Remote Node. Your <i>Prestige</i> will always call the Remote Node using the Primary Phone number first. If the Primary Phone number is busy or does not answer, your <i>Prestige</i> will call the Secondary Phone number if available. Once connected, your <i>Prestige</i> will use the BACP (Bandwidth Allocation Control Protocol) to establish the second B-channel if Multilink PPP is enabled, and the Remote Node supports MP and BACP. Some areas require dialing the pound sign # before the phone number for local calls. A # symbol may be included at the beginning of the Primary Phone number or Secondary Phone number as required.	
Device Type	Use the space bar to choose the following selections: Modem / ISDN TA / X.25 PAD / 56K Modem. A Remote Node only picks up a free device of the selected Device Type to dial out. Only the devices of the same device type will be bundled.	[Modem] [ISDN TA] [X25 PAD] [56K Modem]
Route	This field determines the protocols that your <i>Prestige</i> will route. The choices for this field are determined by the features enabled on your <i>Prestige</i> .	
Bridge	Bridging is used for protocols that are not supported or not turned on in the previous Route field by your <i>Prestige</i>, for example, SNA. When bridging is enabled, your <i>Prestige</i> will forward any packet that it does not recognize to this Remote Node; otherwise, the unrecognized packets are discarded. The disadvantage of bridging is that it usually generates large amounts of traffic.	Press space bar to toggle [Yes/No]

Table 5-1. Remote Node Profile Menu Fields for Dial-up Line Applications (continued)

Field	Description	Options
Edit PPP Options	To edit the PPP options for this Remote Node, move the cursor to this field, use the space bar to select [Yes] and press [Enter] . This will bring you to Menu 11.2 - Remote Node PPP Options. For more information on configuring PPP options, see the section Editing PPP Options.	Press space bar to toggle [Yes] then press [Enter]
IP Addr	This is a required field [?] if [Route] is set to [IP]. Enter the IP address of this Remote Node.	
Edit IP/IPX/Bridge Options	To edit the parameters, select [Yes] and press [Enter]. This will bring you to Menu 11.3 - Remote Node Network Layer Options. For more information on this screen, refer to the chapter pertaining to your specific protocol.	Press space bar to toggle [Yes] then press [Enter]
Edit Script Option	To edit the parameters, select [Yes] and press [Enter]. This will bring you to Menu 11.4 - Remote Node Script Options.	[Yes] then press [Enter]
Telco Options: Allocated Budget (min) Period (hr)	This field will set a budget outgoing call time for the Remote Node. The default for this field is [0] for no budget control. This field will set the time interval to reset the above outgoing call budget control.	Default = 0
Session Option: Input Filter Sets, Output Filter Sets and Call Filter Sets	In these fields, select which filter set(s) you would like to implement to filter the incoming and outgoing traffic between this Remote Node and your <i>Prestige</i> . You can choose from 12 different filter sets. In addition, you can link up to 4 filter sets together for further customization (for example, 1, 5, 9, 12). Note that spaces are accepted in this field. For more information on customizing your filter sets, see <i>Chapter 9</i> . The default is blank, that is, no filters defined.	Default=Blank

Table 5-1. Remote Node Profile Menu Fields for Dial-up Line Applications (continued)

Field	Description	Options
Session Option: Idle Timeout (sec)	This value specifies the number of idle seconds that elapses before the Remote Node is automatically disconnected. Idle seconds is the period of time where no data is passed between the Remote Node and your <i>Prestige</i> . Administrative packets such as RIP are not counted as data. The default is 300 seconds (5 minutes).	Default=300sec
Once you have completed filling in Menu 11.1.1 - Remote Node Profile, press [Enter] at the message [Press ENTER to Confirm...] to save your selections, or press [Esc] at any time to cancel your selections.		

5.1.2 Bandwidth on Demand

The Bandwidth on Demand (BOD) feature allows you to bundle two or three WAN Ports in one connection. The additional ports are added and subtracted dynamically according to traffic demand. The *Prestige* uses the Bandwidth Allocation Control Protocol (BACP) and the Multilink Protocol (MP) to implement bandwidth on demand.

The configuration of bandwidth on demand is based on the Minimum and Maximum Ports of a Remote Node. If Minimum and Maximum Ports are 1, BOD is disabled. Otherwise, BOD is enabled.

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

The Target Utility for a second port specifies the line utilization range at which you want your *Prestige* to add or subtract bandwidth. The parameters are separated by a -. For example, 10-20 means the add threshold is 20 kbps and the subtract threshold is 10 kbps. Your *Prestige* will perform bandwidth on demand only if it initiates the call. Addition and subtraction are based on the value set in the BOD Calculation field. If this field is set to Transmit or Receive, then traffic in either direction will be calculated to determine if a link should be added or dropped. Transmit will

only use outgoing traffic to make this determination. and Receive will only use incoming traffic to make this determination.

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

Similarly, a third port will be brought up or dropped based on the target utility for the third port. The target utility for the third port is based on the Target Utility for the second port and Bandwidth Increment for Additional Ports. For example, when Bandwidth Increment for an Additional Port is 5 (Kbps) and the Target Utility for a second Port is 10-20; then the Target Utility for a third port is 15-25.

See Menu 11.2 - Remote Node PPP Options in Figure 5-3 for a detailed description of BOD fields and instructions on how to configure the PPP Options.

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 and select **[Yes]**, then press **[Enter]**. Menu 11.2 appears as shown in Figure 5-3.

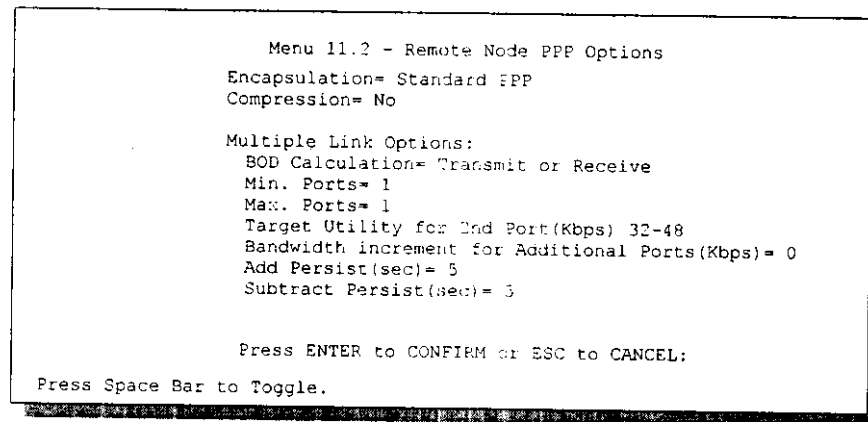


Figure 5-3. Menu 11.2 - Remote Node PPP Options

Table 5-2 describes the Remote Node PPP Options Menu, and contain instructions on how to configure the PPP options fields.

Table 5-2. Remote Node PPP Options Menu Fields

Field	Description	Option
Encapsulation	Select CCP (Compression Control Protocol) for the PPP or MP link. There are two options in this field. ● Standard PPP - Standard PPP options will be used. ● CISCO PPP - Cisco PPP options will be used.	[Standard PPP] [CISCO PPP]
Compression	Turn on the Stac Compression. The default for this field is Off.	[On/Off] (Default = Off)
Multiple Link Options:		
BOD Calculation	Select the direction of the traffic you wish to calculate in order to determine when to add or subtract a link. The default for this field is [Transmit or Receive].	Default = Transmit or Receive
Min. Ports	Enter the minimum number of ports for this Remote Node when a packet triggers a connection.	
Max. Ports	Enter the maximum number of ports for this Remote Node when a packet triggers a connection.	
Target Utility for 2 nd Port (kbps)	Enter the two thresholds separated by a [-] for subtracting and adding the second port.	Default=10-20
Bandwidth Increment for Additional Ports (Kbps)	Enter the Bandwidth Increment to define the two thresholds for subtracting and adding the third port.	

Table 5-2. Remote Node PPP Options Menu Fields (continued)

Field	Description	Option
Add Persist	This parameter specifies the number of seconds where traffic is above the adding threshold before the <i>Prestige</i> will bring up the second channel.	Default = 5 sec
Subtract Persist	This parameter specifies the number of seconds where traffic is below the subtraction threshold before your <i>Prestige</i> drops the second channel.	Default = 5 sec
Once you have completed filling in Menu 11.2 - Remote Node PPP Options, press [Enter] at the message [Press ENTER to Confirm...] to save your selections, or press [Esc] at any time to cancel your selections.		

5.2 Leased Line Connection

The Leased Line Modem Connection feature allows you to connect the serial port WAN Port 1 to a Leased Line Modem (Async). The Connection Type of WAN port 1 must be selected as [Leased] in Menu 2.1 - Async WAN Port Setup.



Note on PPP Echo Request/Reply

In a Leased Line Connection, a [PPP Echo Request] packet is sent periodically to every link (WAN Port). This is to verify if the link is up. When your *Prestige* receives a [PPP Echo Request] packet, it will send another [PPP Echo Reply] packet back to the sender through the same link. When [PPP Echo Reply] packets are not received for several times, your *Prestige* will drop the link.



Note on Backup Function for Leased Line

You can also enable a Backup function for a Leased Line connection. When all the links in a Leased Line Connection drop, your *Prestige* will pick up any available [Switch] WAN port to place a phone call to establish a Backup connection. When any link (WAN port) in the Leased Line Connection becomes available again, your *Prestige* will drop the backup connection. The Backup function is usually enabled in a Leased Line Connection for LAN-to-LAN applications.

5.2.1 Leased Line Remote Node Profile

From Submenu 11.1.2, select [Leased] in the Connection Type field to go to Submenu 11.1.2 - Remote Node Profile for Leased Line application, as shown below in Figure 5-4.

```

Menu 11.1 - Remote Node Profile

Rem Node Name= ?      Route= IP
Active= Yes           Bridge= No
Connection Type= Leased
Leased Ports= 1 (r.o.)
Incoming:              Edit PPP Options= No
  Rem Login= ?         Rem IP Addr= ?
  Rem Password= ?      Edit IP/IPX/Bridge= No
Outgoing:              Session Options:
  My Login= ?          Input Filter Sets=
  My Password= ?       Output Filter Sets=
  Authen= CHAP/PAP     Idle Timeout(sec)= 300
Backup Line Call Direction= Both
Device Type= 56K Modem
Pri Backup Phone #- ?
Sec Backup Phone #-

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

```

Figure 5-4. Menu 11.1 - Remote Node Profile for Leased Line Applications

Table 5-3 describes each field in Menu 11.1.2 - Remote Node Profile for Leased Line applications.

Table 5-3. Remote Node Profile Menu Fields for Leased Line Applications

Field	Description	Option
Rem Node Name	This is a required field [?]. Enter a descriptive name for the Remote Node, for example, SJHQ. This field can support up to eight characters. This name must be unique from any other Remote Node name or Remote Dial-in User name.	
Active	Press the space bar to toggle between [Yes] and [No]. When a Remote Node is deactivated, it has no effect on the operation of your <i>Prestige</i> , even though it is still kept in the database, and can be activated in the future. Deactivated nodes are displayed with a minus sign [-] at the beginning of the name in Menu 11.	Press space bar to toggle [Yes/No]

Table 5-3. Remote Node Profile Menu Fields for Leased Line Applications (continued)

Field	Description	Option
Connection Type: [Leased]	Use space bar to toggle [Switch/Leased], and select [Leased] and press [Enter].	[Leased]
Leased Port(s)	If [Leased] is selected in Connection Type, this field displays the WAN port that supports Leased Line connections. This field is read only (r.o.), since only the serial port WAN port 1 supports, enter the WAN Port numbers in the Leased Line connection. Note: The Connection Type of WAN Port 1 also must be specified as [Leased] in Menu 2.1 - Async WAN Port Setup.	[1 (r.o.)]
Incoming: Rem Node Login Name (*for backup line only)	Enter the login name that this Remote Node will use when it calls into your <i>Prestige</i> . The login name in this field combined with the Rem Node Password will be used to authenticate the incoming calls from this node.	
Incoming: Rem Node Password (*for backup line only)	Enter the password used when this Remote Node calls into your <i>Prestige</i> .	
Outgoing: My Login Name (*for backup line only)	This is a required field [?] if [Call Direction] is either [Both] or [Outgoing]. Enter the login name for your <i>Prestige</i> when it calls this Remote Node.	
Outgoing: My Password (*for backup line only)	This is a required field [?] if [Call Direction] is either [Both] or [Outgoing]. Enter the password for your <i>Prestige</i> when it calls this Remote Node.	

Table 5-3. Remote Node Profile Menu Fields for Leased Line Applications (continued)

Field	Description	Option
Outgoing: Authen (*for backup line only)	This field sets the authentication protocol used for outgoing calls. Your <i>Prestige</i> supports two authentication protocols: PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). ● PAP sends the user name and password in plain text. ● CHAP scrambles the password before it is sent over the wire. Generally speaking, CHAP is more secure than PAP; however, PAP is readily available on more platforms. The recommendation is to use CHAP whenever possible. Turning off the authentication is STRONGLY discouraged. Options for this field are: ● CHAP/PAP - Your <i>Prestige</i> will try CHAP when CHAP is requested by the Remote Node or PAP when PAP is requested by the Remote Node. ● CHAP - use CHAP only. ● PAP - use PAP only.	CHAP/PAP CHAP PAP [CHAP/PAP] [CHAP] [PAP]

Table 5-3. Remote Node Profile Menu Fields for Leased Line Applications (continued)

Field	Description	Option
Backup Line Call Direction	When the Backup Line function is enabled and if all links (WAN Ports) in a Leased Line Modem connections drop, your <i>Prestige</i> will pick up an available Dial-up WAN port to trigger a backup connection. ● If this parameter is set to [Both], your <i>Prestige</i> can both place and receive calls to/from a Remote Node. ● Set this parameter to [None] to de-activate the Backup Line function. ● If set to Incoming, your <i>Prestige</i> will not place a call to a Remote Node. ● If set to Outgoing, your <i>Prestige</i> will drop any call from a Remote Node.	Press space bar to toggle [Both/None/Outgoing/Incoming] [Both] (default) [None] [Incoming] [Outgoing]
Device Type (*for backup line only)	Use the space bar to choose the following selections: Modem / ISDN TA / X.25 PAD / 56K Modem. Your <i>Prestige</i> only picks up a free device of the selected Device Type to dial up.	[Modem] [ISDN TA] [X25 PAD] [56K Modem]
Pri(mary) Backup Phone # (*for backup line only)	Enter the primary telephone number that your <i>Prestige</i> will dial when the Backup Line function is triggered.	
Sec(ondary) Backup Phone # (*for backup line only)	Enter the secondary telephone number that your <i>Prestige</i> will dial when the Backup Line function is triggered.	

Table 5-3. Remote Node Profile Menu Fields for Leased Line Applications (continued)

Field	Description	Option
Route	This field determines the protocols that your <i>Prestige</i> will route. The choices for this field are determined by the features enabled on your <i>Prestige</i> .	
Bridge	Bridging is used for protocols that are not supported or not turned on in the previous Route field by your <i>Prestige</i> , for example, SNA. When bridging is enabled, your <i>Prestige</i> will forward any packet that it does not recognize to this Remote Node; otherwise, the unrecognized packets are discarded. The disadvantage of bridging is that it usually generates large amounts of traffic.	Press space bar to toggle [Yes/No]
Edit PPP Options	To edit the PPP options for this Remote Node, move the cursor to this field, use the space bar to select [Yes] and press [Enter]. This will bring you to Menu 11.2 - Remote Node PPP Options. For more information on configuring PPP options, see the section Editing PPP Options.	Press space bar to toggle [Yes] then press [Enter]
Rem IP Addr	This is a required field [?] if [Route] is set to [IP]. Enter the IP address of this Remote Node.	
Edit IP/IPX/Bridge Options	To edit the parameters, select [Yes] and press [Enter]. This will bring you to Menu 11.3 - Remote Node Network Layer Options. For more information on this screen, refer to the chapter pertaining to your specific protocol.	Press space bar to toggle [Yes] then press [Enter]
Rem Password	This is a required field [?] if [Route] is set to [IP]. Enter the password used when this Remote Node calls into your <i>Prestige</i> .	

Table 5-3. Remote Node Profile Menu Fields for Leased Line Applications (continued)

Field	Description	Option
Session Option: Input Filter Sets, Output Filter Sets and Call Filter Sets	In these fields, select which filter set(s) you would like to implement to filter the incoming and outgoing traffic between this Remote Node and your <i>Prestige</i>. You can choose from 12 different filter sets. In addition, you can link up to 4 filter sets together for further customization (for example, 1, 5, 9, 12). Note that spaces are accepted in this field. For more information on customizing your filter sets, see <i>Chapter 9</i>. The default is blank, that is, no filters defined.	Default=Blank
Session Option: Idle Timeout (sec)	This value specifies the number of idle seconds that elapses before the Remote Node is automatically disconnected. Idle seconds is the period of time where no data is passed between the Remote Node and your <i>Prestige</i>. Administrative packets such as RIP are not counted as data. The default is 300 seconds (5 minutes).	Default=300sec
Once you have completed filling in Menu 11.1.2 - Remote Node Profile for Leased Line Connection, press [Enter] at the message [Press ENTER to Confirm...] to save your selections, or press [Esc] at any time to cancel your selections.		

5.2.2 Editing Leased Line PPP Options

To edit the remote node PPP Options in the case of a Leased Line connection, move the cursor to the **[Edit PPP Options]** field in Menu 11.2 - Remote Node Profile, and use the space bar to toggle and select **[Yes]**, then press **[Enter]**. Menu 11.2 appears as shown in Figure 5-5.

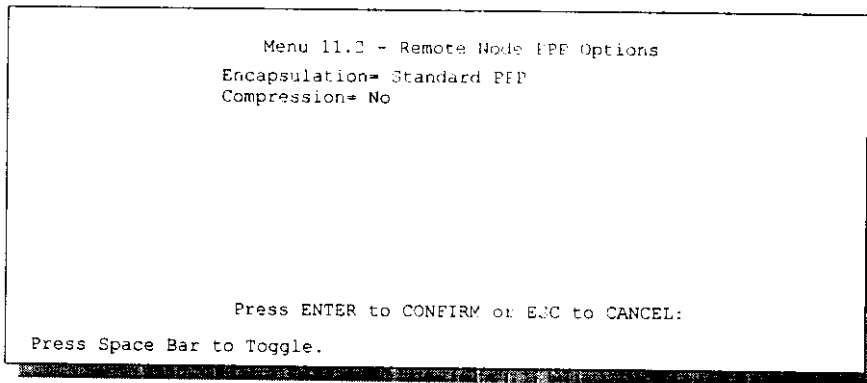


Figure 5-5. Menu 11.2 - Remote Node PPP Options for Leased Line Applications

Table 5-4 describes the Remote Node PPP Options Menu for Leased Line applications, and contains instructions on how to configure the PPP options fields.

Table 5-4. Remote Node PPP Options Menu Fields for Leased Line Applications

Field	Description	Option
Encapsulation	Select CCP (Compression Control Protocol) for the PPP or MP link. There are two options in this field. - Standard PPP - Standard PPP options will be used. - CISCO PPP - Cisco PPP options will be used.	[Standard PPP] [CISCO PPP]
Compression	Turn on the Stac Compression. The default for this field is Off.	[On/Off] (Default = Off)

Chapter 6

TCP/IP Configuration for LAN-to-LAN

This chapter shows you how to configure your *Prestige* for TCP/IP. Depending on your particular applications, you will need to configure different menus. For instance, Internet access is the most common application of TCP/IP. For this application, you should configure Menu 4. We will illustrate the configuration for LAN-to-LAN applications in the following sections.

6.1 LAN-to-LAN Application

A typical LAN-to-LAN application is to use your *Prestige* to call from a branch office to the headquarters, as depicted in the following Figure 6-1.

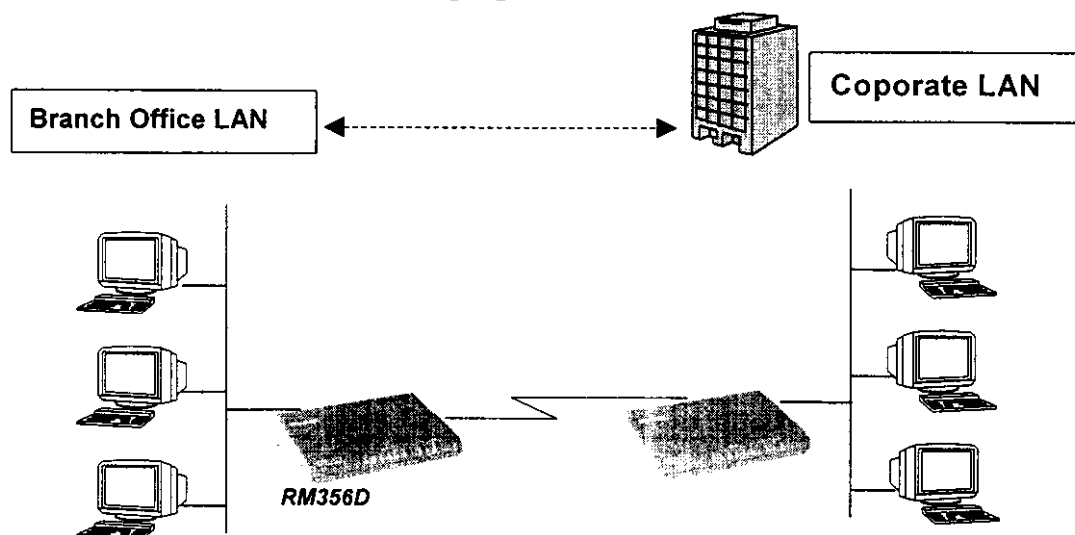


Figure 6-1. LAN-to-LAN Application with TCP/IP

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 configure Static Routes if some services reside beyond the immediate remote LAN.

6.1.1 Remote Node Setup

Follow the procedure in *Chapter 5 - Remote Node Configuration for LAN-to-LAN* to fill the protocol-independent parameters in Menu 11 - Remote Node Profile. For the protocol-dependent parameters, follow the instructions below. If you are configuring your *Prestige* to receive an incoming call, you also need to set the default dial-in parameters in Menu 13.

To edit Menu 11.3 - Remote Node Network Layer Options shown in Figure 6-2, follow these steps:

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

```
Menu 11.3 - Remote Node Network Layer Options

IP Options:
Rem IP Addr: 0.0.0.0
Rem Subnet Mask= 0.0.0.0
My WAN Addr= 0.0.0.0
Single User Account= No
  Server IP Addr= N/A
Metric= 2
Private= No
RIP Direction= Both
Version= RIP-2B

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

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

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

Figure 6-2. Menu 11.3- Remote Node Network Layer Options for a TCP/IP Application

The following diagram in Figure 6-3 explains the Sample IP Addresses to help understand the field of My Wan Address in Menu 11.3.

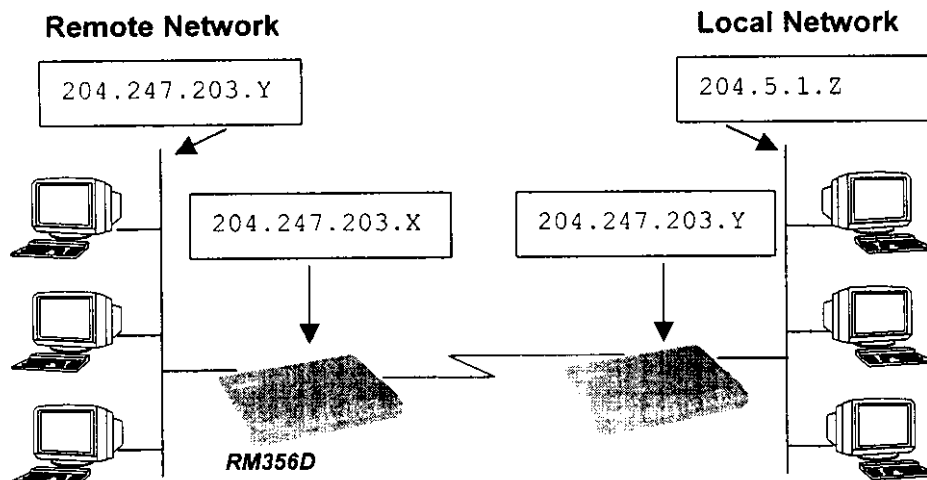


Figure 6-3. Sample IP Addresses for a LAN-to-LAN Connection with TCP/IP

The following Table 6-1 describes the Remote Node Profile and Remote Node Network Layer Options for a TCP/IP configuration.

For more details on the IP Options fields, refer to *Chapter 3 - Internet Access Application*.

Table 6-1. Remote Node Network Layer Options for a TCP/IP Configuration

Field	Description	Option
Route	Make sure [IP] is among the protocols in the Route field.	[IP] ([IP/IPX/IP+IPX])
IP Address	Enter the IP address of the gateway at the remote site (in this case, headquarters). If the remote router is using a different IP address than the one entered here, your <i>Prestige</i> will drop the call.	
Edit IP/IPX/Bridge	Press the space bar to change it to [Yes] and press [Enter] to go to Menu 11.3 - Remote Node Network Layer Options Menu.	[Yes] ([Yes/No])
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 hosts on both ends of the PSTN/ISDN link to have separate addresses from the LAN, and that the addresses must have the same network number. If this is the case, enter the IP address assigned to the WAN port of your <i>Prestige</i>. Note that this is the address assigned to your local <i>Prestige</i>, not the remote router. (See Figure 6-3 for an explanation of My WAN Addr. With Sample IP Addresses)	
Single User Account	This field should be set to [Yes] to enable the Single User Account (Network Address Translation) feature for this site. Use the space bar to toggle between [Yes] and [No]. See <i>Chapter 3 - Internet Access Application</i> for more information on the Single User Account feature.	[Yes/No]
Server IP address	If you are using the Single User Account feature and you want to make a server on your LAN (for example, a Web server) accessible to outside users, enter that servers IP address here.	

Table 6-1. Remote Node Network Layer Options for a TCP/IP Configuration (continued)

Field	Description	Option
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of [1] for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between [1] and [16]. In practice, [2] or [3] is usually a good number.	[1] to [16]
Private	This parameter determines if the <i>Prestige</i> will include the route to this Remote Node in its RIP broadcasts. If set to [Yes], this route is kept private and not included in RIP broadcast. If [No], the route to this Remote Node will be propagated to other hosts through RIP broadcasts.	[Yes/No]
RIP	This parameter determines how your <i>Prestige</i> handles RIP (Routing Information Protocol), and the default is [Both]. If set to [Both], your <i>Prestige</i> will broadcast its routing table on the WAN, and incorporate RIP broadcasts by the other router into its routing table. If set to [In Only], your <i>Prestige</i> will not broadcast its routing table on the WAN. If set to [Out Only], your <i>Prestige</i> will broadcast its routing table but ignores any RIP broadcast packets that it receives. If set to [None], your <i>Prestige</i> will not participate in any RIP exchange with other routers. Usually, you should leave this parameter at its default of [Both] and let RIP propagate the routing information automatically.	(Default=Both) [Both] [In Only] [Out Only] [None]
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 selections, or press [Esc] at any time to cancel your selections.		

6.1.2 Static Route Setup

On a directly connected internet, RIP usually handles the routing automatically. However, RIP cannot propagate across isolated networks, as in the case before a connection is made between the two subnetworks using one Class C IP address. Without a route, no packets can be forwarded to their destinations. A static route is used to resolve this problem by providing your *Prestige* with some static routing information. As a matter of fact, when you configure the Internet Access or a Remote Node, a static route is implicitly created by your *Prestige*. An example is given below. In the example, stations on the 204.5.1.0/24 subnetwork can access the remote stations using the static route. The route will have a destination of 204.5.1.64/26 with the gateway address being that of the Remote Node (204.5.1.150).

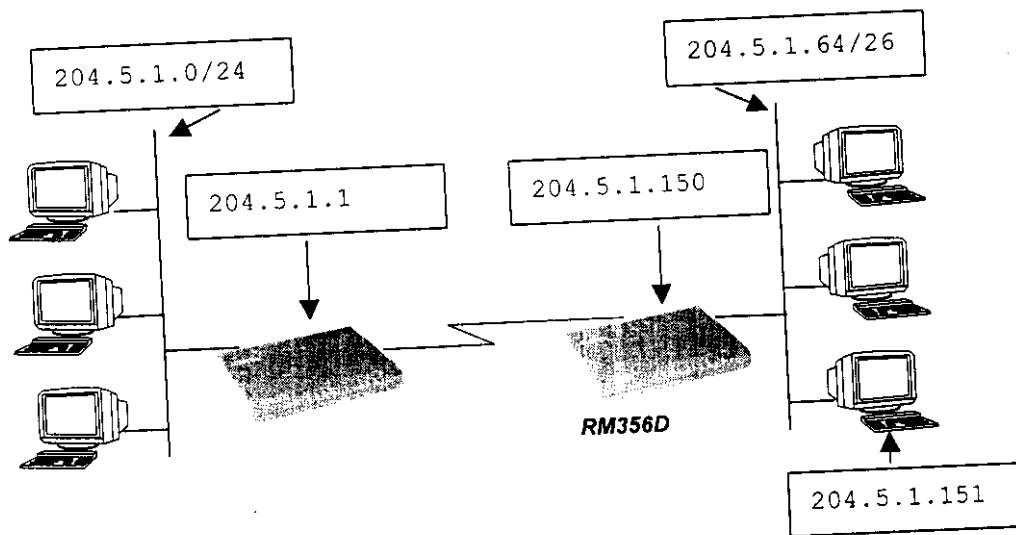


Figure 6-4. Example of Static Routing Topology

Note that in normal circumstances, your *Prestige* will have adequate routing information after you configure the Internet access and Remote Nodes; you do not need to configure additional static routes. You will need to configure static routes only for unusual cases (for example, subnetting).

To create an additional static route for IP, use Menu 12, Static Route Setup, as displayed in Figure 6-5.

```
Menu 12 - Static Route Setup

IP Static Route
1. ispl (ISP)
2. _____
3. _____
4. _____

Bridge Static Route
21. _____
22. _____
23. _____
24. _____

IPX Static Route
11. _____
12. _____
13. _____
14. _____

Enter Selection Number:
```

Figure 6-5. Menu 12 - Static Route Setup

From Menu 12, select one of the four possible IP Static Routes (no. 1-4), this will open Menu 12.2 - Edit IP Static Route, as shown in Figure 6-6.

```
Menu 12.1 - Edit IP Static Route

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

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

Figure 6-6. Menu 12.1 - Edit IP Static Route

Table 6-2 describes the fields for Menu 12.1 - Edit IP Static Route Setup.

Table 6-2. Edit IP Static Route Menu Fields

Field	Description
Route Name	Enter a descriptive name for this route. This is for identification purpose only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the subnet mask for this destination. Follow the discussion on IP subnet mask in this chapter.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your <i>Prestige</i> that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your <i>Prestige</i> ; over PSTN/ISDN, the gateway must be the IP address of one of the Remote Nodes.
Metric	Same meaning as those in the Remote Node Setup (See Table 6-3).
Private	Same meaning as those in the Remote Node Setup (See Table 6-3).

Chapter 7

Novell IPX Configuration for LAN-to-LAN

This chapter shows you how to configure your *Prestige* for IPX protocol. Depending on your particular applications, you will need to configure different menus. We will illustrate the configuration for some applications in the following sections.

7.1 IPX Network Environment

7.1.1 Frame Type

The stations on an IPX network (both clients and servers) can run on four different frame types existing on one physical Ethernet cable. These frame types include 802.2, 802.3, Ethernet II (DIX), and SNAP.

7.1.2 Network Numbers

External Network Number

Whenever you are setting up an IPX routing environment, it is important to correctly configure the network numbers on the LAN. On any IPX network, there is an external network number that is, the number associated with the frame type on the Ethernet cable to which the stations on the network are joined.

Internal Network Number

In addition to this external network number, each NetWare server has its own internal network number. It is important to remember that every network number has to be unique for that entire internetwork. So if a server station had an internal network number of [00000011], there is no other network number (internal or external) of [00000011] anywhere on the entire network.

7.2 Prestige Operating in IPX Environment

There are two different scenarios in which you would connect your *Prestige* to a LAN:

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

Figure 7-1 illustrates a typical LAN(Client)-to-LAN(Server) connection in an IPX environment.

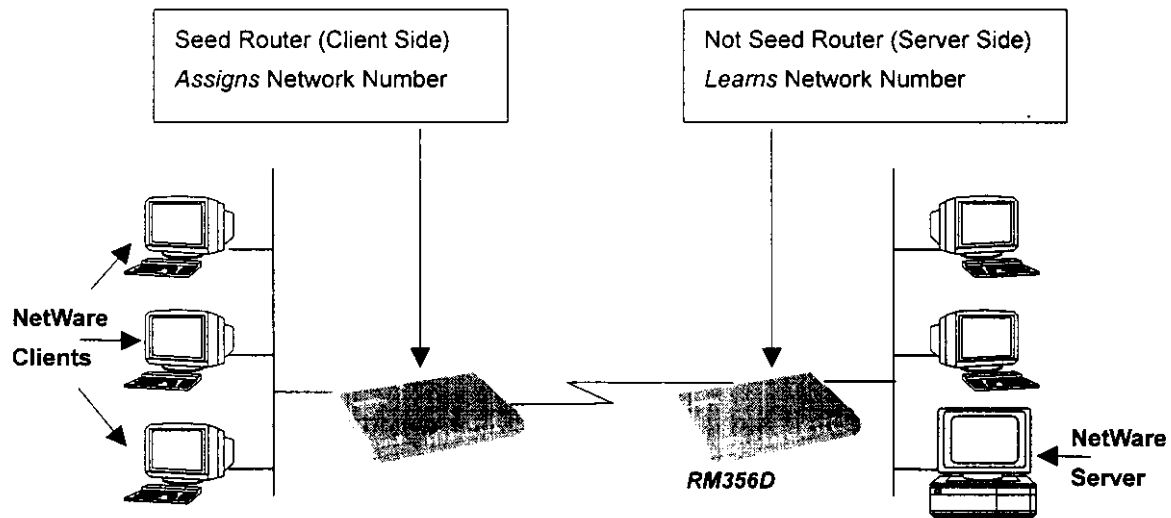


Figure 7-1. Prestige Operating in IPX Environment

7.2.1 *Prestige* on LAN with Server

When your *Prestige* is being connected to a LAN with an existing NetWare server station, you will not need to configure your *Prestige* as a seed router, and hence the network number parameter in the Ethernet Setup Menu for your *Prestige*. Your *Prestige* will learn the network number of the network it is attached to through the regular RIP broadcasts sent by the server and add this route to its routing table.

7.2.2 *Prestige* on LAN without Server

If your *Prestige* is connected to a LAN without an existing NetWare server station, then it needs to create a unique external network number to apply to that frame on the LAN. Your *Prestige* must then be configured as a Seed Router, and the network number can be configured in the Ethernet Setup Menu. The network number must be unique and not used anywhere else on the entire internetwork.

7.3 IPX Spoofing

Your *Prestige* comes with several pre-defined call filters designed to prevent certain IPX packets from triggering a call to a Remote Node. These filters should inform your *Prestige* which packets should be ignored as traffic.

When you are routing IPX packets, the default call filters are defined as follows:

- Block periodical SAP and RIP response messages.
- Block NetWare serialization packets.
- Allow SAP and RIP inquiry packets.

These call filters prevent your *Prestige* from making a call to the Remote Node, thus preventing the expense of an unnecessary phone call.

7.4 IPX Ethernet Setup

The first step is to set up your *Prestige* on the LAN. From Menu 3 - Ethernet Setup, select option [3. Novell IPX Setup] to go to Menu 3.3 - Novell IPX Ethernet Setup as shown in Figure 7-2.

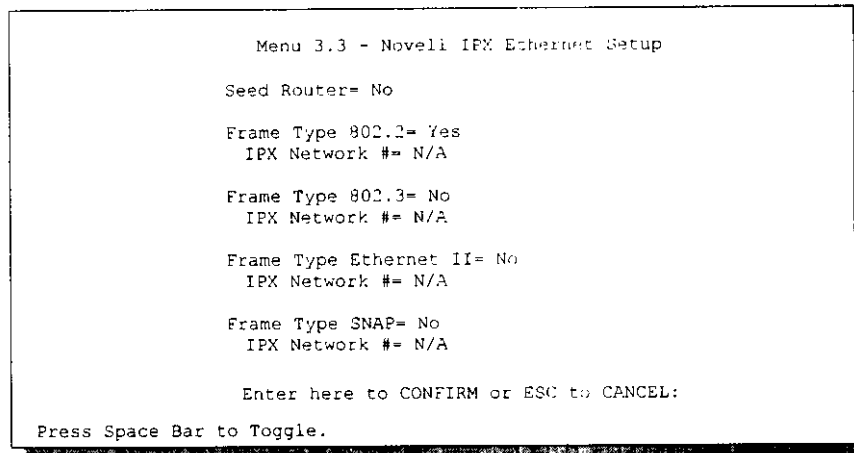


Figure 7-2. Menu 3.3 - Novell IPX Ethernet Setup

The following Table 7-1 describes the Novell IPX Ethernet Setup Menu.

Table 7-1. Novell IPX Ethernet Setup Fields

Field	Description	Options
Seed Router	Determine if your <i>Prestige</i> is to act as a seed router. This value depends on the existing network. If there is a NetWare server providing the network number, select No. If there is no NetWare server providing the network number, select Yes.	[Yes/No]
Frame Type	For every frame type that your <i>Prestige</i> needs to support, you need to set the corresponding field to Yes. The frame type(s) selected here must be the same frame type(s) as the server or client stations on that network. Otherwise, the devices will not be able to communicate. You can select one or more options listed in this field.	[802.2] [802.3] [Ethernet II] [SNAP]
IPX Network #	If you selected your <i>Prestige</i> to act as a seed router, you need to provide a unique network number to be associated with the network that your <i>Prestige</i> has joined. Keep in mind that this number must not be used anywhere else on the entire internetwork.	
Press [Enter] at the message [Press ENTER to Confirm ...] to save your selections, or press [Esc] at any time to cancel your selections.		

7.5 LAN-to-LAN Application with Novell IPX

A typical LAN-to-LAN application is to use your *Prestige* to call from a branch office to the corporate headquarters, such that all of the stations on the branch office network have access to the server at the headquarters, as depicted in Figure 7-3.

For the branch office, you need to configure a Remote Node in order to dial out to headquarters.

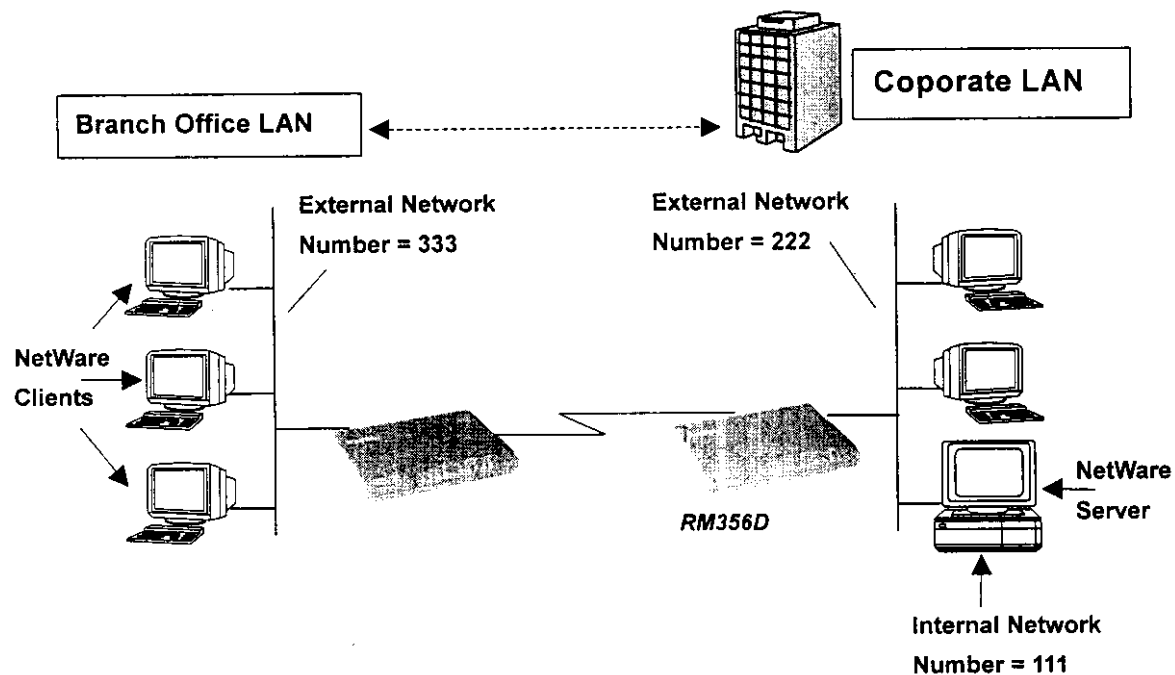


Figure 7-3. LAN-to-LAN Application with Novell IPX

7.5.1 Remote Node Setup

Follow the procedure in *Chapter 5* to define the protocol-independent parameters in Menu 11.1 - Remote Node Profile. For the protocol-dependent parameters in Menu 11.3 - Remote Node Network Layer Options, follow the ensuing instructions. If your *Prestige* is configured to receive an incoming call, you can also configure the default dial-in parameters in Menu 13.

To edit Menu 11.3 - Remote Node Network Layer Options shown in Figure 7-4, follow these steps:

- Step 3.** 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 4.** Move the cursor to the [Edit IP/IPX/Bridge] field, then press the space bar to toggle and set the value to [Yes], and press [Enter] to edit Menu 11.3 - Network Layer Options.

```

Menu 11.3 - Remote Node Network Layer Options

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

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

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

Enter here to CONFIRM or ESC to CANCEL:

```

Figure 7-4. Menu 11.3 - Remote Node Network Layer Options for Novell IPX Application

The Table 7-2 describes the IPX protocol-dependent parameters of the Remote Node Setup.

Table 7-2. Remote Node Network Layer Options for Novell IPX Application

Field	Description	Option
Route	Make sure [IPX] is among the protocols in the Route field.	
Edit IP/IPX/Bridge	Press the space bar to change it to [Yes] and press [Enter] to go to the Network Layer Options Menu.	
Dial-On-Query	This field is necessary for your <i>Prestige</i> on the client side LAN. When set to [Yes], any Get Service SAP or RIP broadcasts coming from the LAN will trigger your <i>Prestige</i> to make a call to that Remote Node. If it is set to [No], your <i>Prestige</i> will not make the outgoing call.	[Yes/No]
Rem LAN Net #	In this field, enter the internal network number of the NetWare server on the remote side LAN. Your <i>Prestige</i> will create a route to access this server.	
My WAN Net #	In this field, you can type in the WAN network number of the device that you are connecting to. This number will be used for negotiation between your <i>Prestige</i> and the remote device. If you leave this field as [00000000], your <i>Prestige</i> will select the greater WAN network number between the two devices.	[00000000] (default)
Hop Count	This field indicates the number of intermediate networks that must be passed through to reach the Remote Node.	[1] (default)
Tick Count	This field indicates the time-ticks required to reach the Remote Node.	[2] (default)
W/D Spoofing (min)	This field is used for the <i>Prestige</i> on the server side LAN. Your <i>Prestige</i> can spoof a response to a server's WatchDog request after the connection is dropped. In this field, type in the time (number of minutes) that you want your <i>Prestige</i> to spoof the WatchDog response.	
SAP/RIP Timeout (min)	This field indicates the amount of time that you want your <i>Prestige</i> to maintain the SAP and RIP entries learned from this Remote Node in its internal tables after the connection has been dropped. If this information is retained, then your <i>Prestige</i> will not have to get the SAP information when the line is brought back up. Enter the time (number of minutes) in this field.	
Once you have completed filling in the Network Layer Options Menu, press [Enter] to return to Menu 11.1. Then press [Enter] at the message [Press Enter to Confirm] to save your selections, press [Esc] to cancel.		

7.5.2 Static Route Setup

If your LAN-to-LAN application has NetWare servers on both sides of the link, then all NetWare client stations will have access to a server on their LAN as shown in Figure 7-5.

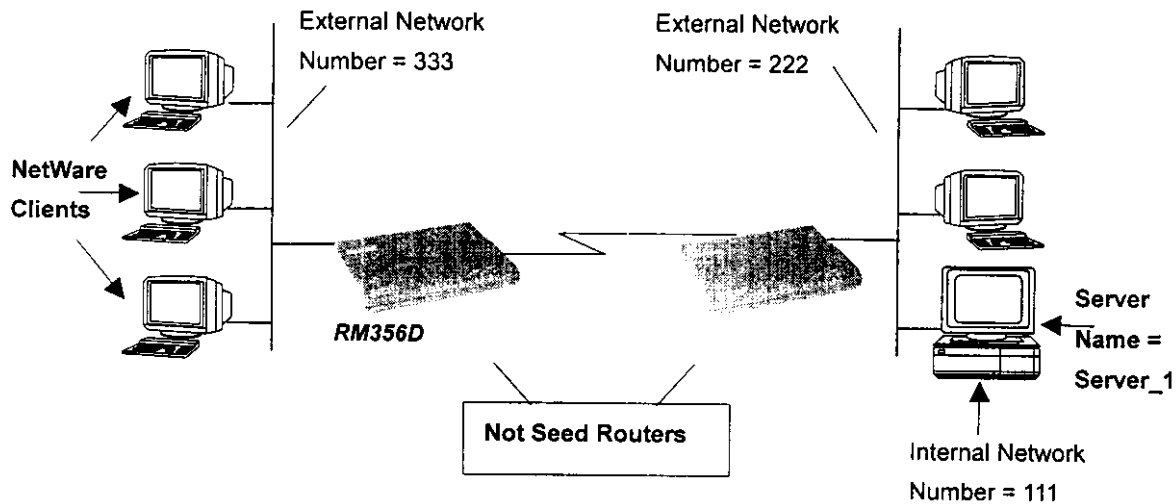


Figure 7-5. Netware Servers on Both Sides of the Link

This may present a problem if you desire your client station to access a server at a remote site. For example, in the diagram of Figure 7-5, suppose that a client station on the network on the left wishes to access the NetWare server on the right (internal network number = 111). However, the SAP broadcasts will receive a response from the server on the left (internal network number = 444). A static route is used to resolve this problem by providing your *Prestige* with some static routing information to access the remote server.

From Menu 12, select one of the four possible IPX Static Routes (no. 11-14), this will open Menu 12.2 - Edit IPX Static Route, as shown in Figure 7-6.

```

Menu 12.2 - 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

Table 7-3 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 in the name that has been configured for the server. This name must be the exact name configured in the NetWare server.
Network #	This field contains the internal network number of the remote server that you wish to access. Do not use [00000000] or [FFFFFFF] for this field.
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 (1-4) of the Remote Node that is linked to this static route. That is, the Remote Node that you wish to route the packet to.
Hop Count and Tick Count	These two fields have the same meaning as those in the Remote Node Setup.
Once you have completed filling in the menu, press [Enter] at the message [Press Enter to Confirm] to save your selections, or press [Esc] to cancel to cancel your selections.	

Chapter 8

Bridge Configuration for LAN-to-LAN

This chapter shows you how to configure the Bridging options for your *Prestige*. Depending on your particular applications, you will need to configure different menus. We will illustrate the configuration for some applications in the following sections.

8.1 IPX Spoofing

Your *Prestige* comes with several pre-defined call filters designed to prevent certain IPX packets from triggering a call to a Remote Node. These filters should inform your *Prestige* which packets should be ignored as traffic.

When you are routing IPX packets, the default call filters are defined as follows:

- Block periodical SAP and RIP response messages.
- Block SAP and RIP inquiry packets if set to Handle IPX as Server.
- Allow SAP and RIP inquiry packets if set to Handle IPX as Client or None.

These call filters prevent your *Prestige* from making a call to the Remote Node, thus preventing the expense of an unnecessary phone call.

8.2 Bridge Ethernet Setup

Bridging is used to forward packets of unsupported protocols whose destination is not on the local Ethernet to the WAN.

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

Table 8-1 describes the [Handle IPX] field settings.

Table 8-1. Handle IPX Field Settings

Handle IPX Setting	Description
None	Nothing is done to IPX traffic.
Client	All RIP and SAP (Service Advertising Protocol) periodical response packets will not trigger the call.
Server	No RIP or SAP packets will trigger the call. In addition, during the time when the ISDN line is down, your <i>Prestige</i> will reply to the servers watchdog messages on behalf of remote clients. The period of time that your <i>Prestige</i> 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.

From Menu 3 - Ethernet Setup, enter option [4. Bridge Setup] and Menu 3.5 - Bridge Ethernet Setup displays as shown in Figure 8-1.

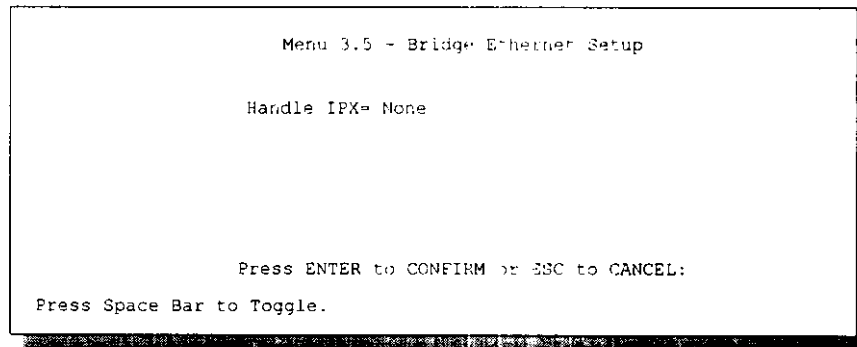


Figure 8-1. Menu 3.5 - Bridge Ethernet Setup

Table 8-2 describes how to configure the [Handle IPX] field in Menu 3.5.

Table 8-2. Bridge Ethernet Setup Menu - Handle IPX Field Configuration

Handle IPX Field (Menu 3.5)	Description
None	When there is no IPX traffic on the LAN or when you do not want to apply any special handling for IPX.
Client	When there are only client workstations on the LAN
Server	When there are only IPX servers on the LAN.
Client + Dial-On-Broadcast in Menu 12 set to [Yes]	When there are both clients and servers on the LAN, and the local clients will access the remote servers, set to Client and the Menu 12 to [Yes] to allow the client queries to trigger the call. If they do not, set it to [Server].

8.3 LAN-to-LAN Application

A typical LAN-to-LAN application is to use your *Prestige* to call from one office to another office such that stations on one network have access to stations on the remote side and vice versa. You will need to configure a Remote Node in order to dial out to another office.

8.3.1 Remote Node Setup

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

To edit Menu 11.3 - Remote Node Network Layer Options shown in Figure 8-2, follow these steps:

- Step 1.** In Menu 11.1, make sure the [Bridge] field is set to [Yes].
- Step 2.** Move the cursor to the [Edit IP/IPX/Bridge] field, then press the space bar to toggle and set the value to [Yes], and press [Enter] to edit Menu 11.3 - Network Layer Options.

```
Menu 11.3 - Remote Node Network Layer Options

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

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

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

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

Figure 8-2. Menu 11.3 - Remote Node Network Layer Options for Bridging Configuration

Table 8-3 describes the protocol-dependent parameters for the Bridge options in the Remote Node Profile and Network Layers menus.

Table 8-3. Remote Node Network Layers Menu Bridge Options

Field	Description
Bridge	Make sure this field is set to [Yes].
Edit IP/IPX/Bridge	Press the space bar to change it to [Yes] and press [Enter] to go to the Network Layer Options Menu.
Dial-On-Broadcast	This field is necessary for your <i>Prestige</i> on the caller side LAN. When set to [Yes], any broadcasts coming from the LAN will trigger your <i>Prestige</i> to make a call to that Remote Node. If it is set to [No], your <i>Prestige</i> will not make the outgoing call.
Ethernet Addr Timeout (min)	In this field, enter the time (number of minutes) that you wish your <i>Prestige</i> to retain the Ethernet Addr information in its internal tables while the line is down. If this information is retained, then your <i>Prestige</i> will not have to re-negotiate the protocol and 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 selections, or press [Esc] to cancel.	

8.3.2 Default Dial-In Setup for Bridge

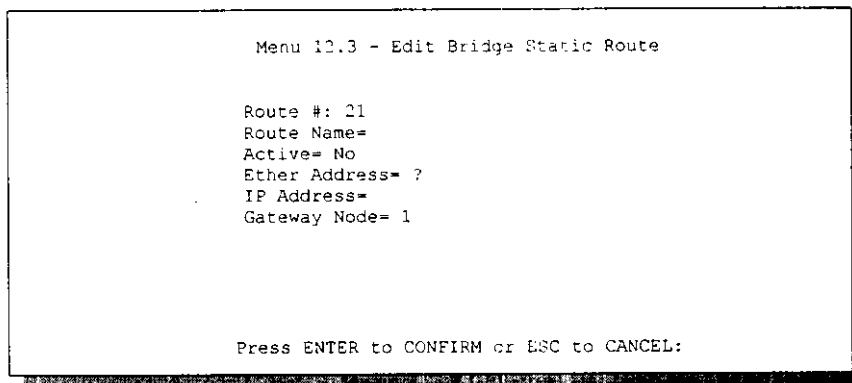
There is only one dial-in parameter [PPP Options: Recv. Authen] in Menu 13 - Default Dial-In Setup that you need to fill out for Bridging applications, as shown in Table 8-4.

Table 8-4. Default Dial-in Setup Field for Bridging Applications

Field	Description
(Menu 13) PPP Options: Recv. Authen	Make sure this field is set to [Yes].
Once you have completed filling in this menu, press [Enter] at the message [Press Enter to Confirm] to save your selections, or press [Esc] to cancel your selection.	

8.3.3 Bridge Static Route Setup

You can configure Bridge static routes for your Bridging applications in Menu 12.3, as shown in Figure 8-3.



```
Menu 12.3 - Edit Bridge Static Route

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

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

Figure 8-3 Menu 12.3 - Edit Bridge Static Route

The following Table 8-5 describes the Bridge Static Route Menu.

Table 8-5. Bridge Static Route Menu Fields

Field	Description
Route Name	For identification purposes enter a name for the bridge static route.
Active	Indicates whether the static route is active or not.
Ether Address	Enter the MAC address of the destination device that you wish to bridge your packets to.
IP Address	If available, enter the IP address of the destination device that you wish to bridge your packets to.
Gateway Node	Enter the number (1-4) of the Remote Node that is linked to this static route. When an incoming packet's destination Ether (MAC) address matches the value entered above, then it will trigger a call to this Remote Node.
Once you have completed filling in this menu, press [Enter] at the message [Press Enter to Confirm] to save your selections, or press [Esc] to cancel your selection.	

Chapter 9

Filter Configuration

About Filtering

Your *Prestige* uses filters to decide whether or not to allow passage of a data packet and/or to make a call over the Modem or ISDN TA line. There are three types of filters involved:

- Incoming Data Filters
- Outgoing Data Filters
- Call Filters.

Data filters screen the data to determine if the packet should be allowed to pass. Call filters are used to determine if a call should be placed.

Outgoing packets must pass through the data filters before they encounter the call filters. Call filters are divided into two groups

- Default Call Filters
- User-defined Call Filters.

Your *Prestige* has default call filters that filter out administrative packets (for example, RIP and SAP packets). Your *Prestige* applies the default filters first and then the user-defined call filters if applicable as the outgoing packet filtering process illustrates in Figure 9-1.

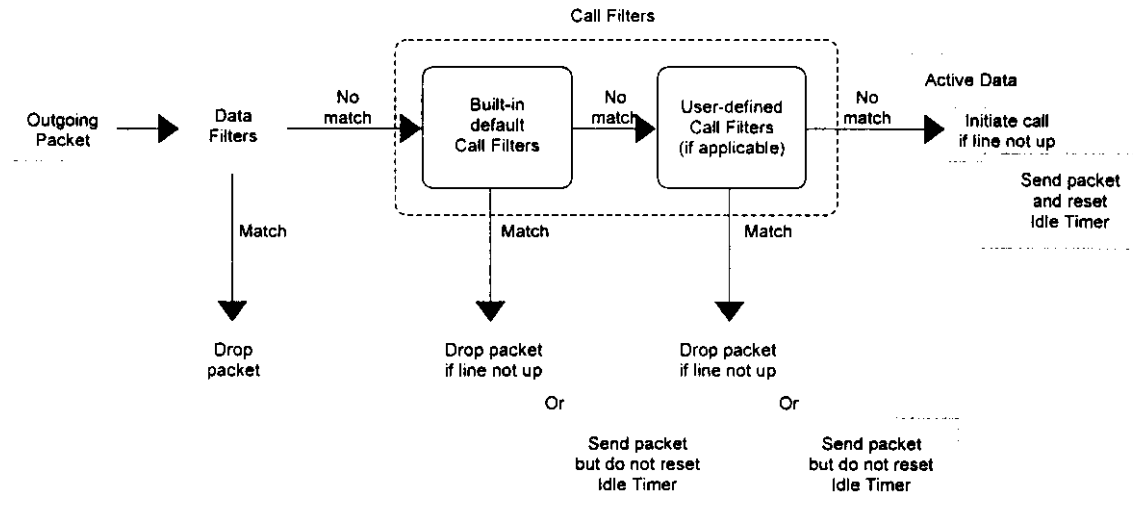


Figure 9-1. Outgoing Packet Filtering Process

For incoming packets, your *Prestige* applies data filters only. Packets are processed depending upon whether a match is made. Your *Prestige* allows you to customize the filter sets that you wish to use. The following sections describe how to configure filter sets.

The Filter Structure of the *Prestige*

You can configure up to twelve filter sets with six rules in each set, allowing you to customize up to 72 filter rules (12 x 6).

When implementing these filter sets, you can link up to four of the filter sets together to screen the data packet. Therefore, with each filter set having up to six rules, you can have a maximum of 24 rules active for a single filtering application.

9.1 Configuring a Filter Set

In order to distinguish between the 12 filter sets, each filter set should have a name or some sort of Comments. You can edit these Comments in the following way:

- Step 1.** From the Main Menu, select option [2]. Filter Set Configuration].
- Step 2.** When Menu 21 - Filter Set Configuration appears, you can choose among 12 filter sets. Select the filter set you wish to configure (no. 1-12), then press [Enter].
- Step 3.** This will bring you to the Edit Comments field. Whatever the comments are for that filter set will be displayed in this field. You can edit the comments you wish to use to identify that filter set.

Once you have completed filling in Edit Comments field, press [Enter] at the message: [Press ENTER to confirm], or press [Esc] at any time to cancel your selections.

The new information will now be displayed in the read-only section of Menu 21 - Filter Set Configuration as shown in Figure 9-2.

Menu 21 - Filter Set Configuration			
Filter Set #	Comments	Filter Set #	Comments
1	_____	7	_____
2	_____	8	_____
3	_____	9	_____
4	_____	10	_____
5	_____	11	_____
6	_____	12	_____

Enter Filter Set Number to Configure=

Edit Comments=

Press ENTER to CONFIRM or ESC to CANCEL:

Figure 9-2. Menu 21 - Filter Set Configuration

Step 4. Once you press [Enter] to confirm your changes, Menu 21.1 - Filter Rules Summary appears.

Filter Rules Summary Menu

The information displayed in the Menu 21.1 - Filter Rules Summary is read-only. From here, you can examine the parameters of each rule that you have configured for that filter set.

Figure 9-3 displays Menu 21.1 - Filter Rules Summary.

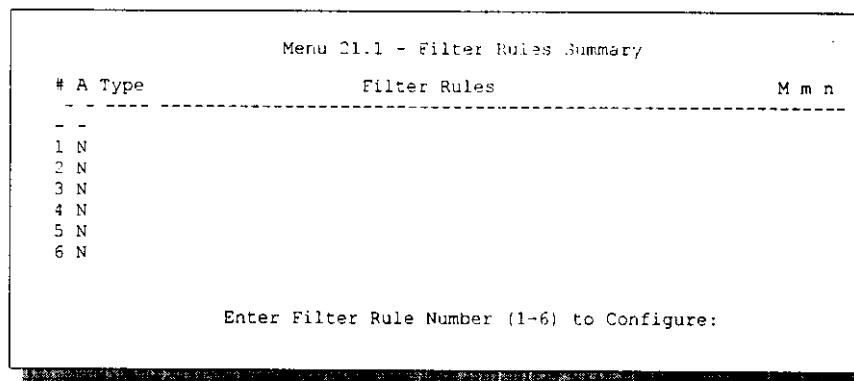


Figure 9-3. Menu 21.1 - Filter Rules Summary

The following Table 9-1 contains 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 can display GEN for generic, IP for TCP/IP, or IPX for Novell IPX.	[GEN] for Generic [IP] for TCP/IP [IPX] for Novell IPX

Table 9-1. Abbreviations Used in the Filter Rules Summary Menu (continued)

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

The protocol dependent filter rules abbreviation are listed as follows:

- If the filter type is IP (TCP/IP), the following abbreviations listed in Table 9-2 will be used.

Table 9-2. Abbreviations Used If Filter Type Is IP

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

- If the filter type is GEN (generic), the following abbreviations listed in Table 9-3 will be used.

Table 9-3. Abbreviations Used If Filter Type Is GEN

Abbreviation	Description
Off	Offset
Len	Length

- If the filter type is IPX (Novell IPX), the following abbreviations listed in Table 9-4 will be used.

Table 9-4 Abbreviations Used If Filter Type Is IPX

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

For more information on configuring the filter rule parameters, refer to the next section.

To configure a specific filter rule, simply select the number of the filter rule (1-6) you wish to configure and press [Enter]. This will take you to Menu 21.1.1 - TCP/IP Filter Rule in next section.

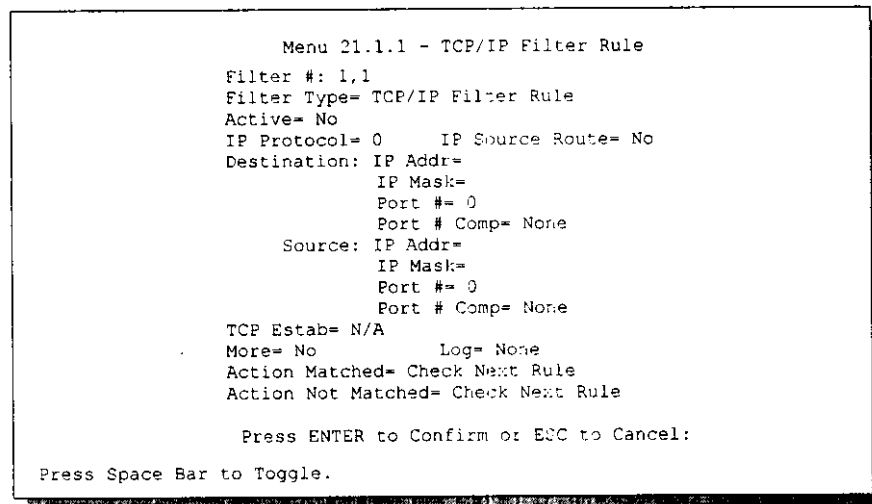
9.2 Configuring a Filter Rule

There are four types of filter rules that you can configure. Some of the parameters will differ depending on the type of rule. When you first enter the Filter Rule Menu, you will be presented with Menu 21.1.1 - TCP/IP Filter Rule. If you wish to configure another type of filter rule, you need to select the appropriate type (by pressing [Space bar]) under the Filter Type field and press [Enter]. This will bring you to the corresponding menu.

9.2.1 TCP/IP Filter Rule

This section will show you how to configure a TCP/IP filter rule for your *Prestige*.

Figure 9-4 displays Menu 21.1.1 TCP/IP Filter Rule.



```
Menu 21.1.1 - TCP/IP Filter Rule
Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= No
IP Protocol= 0      IP Source Route= No
Destination: IP Addr=
               IP Mask=
               Port #= 0
               Port # Comp= None
Source: IP Addr=
         IP Mask=
         Port #= 0
         Port # Comp= None
TCP Estab= N/A
More= No      Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

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

Figure 9-4. Menu 21.1.1 - TCP/IP Filter Rule

The following Table 9-5 describes how to configure your TCP/IP filter rule.

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

Field	Description	Option
Active	In this field, you can make the filter rule active or inactive.	[Yes/No]
IP Protocol	Protocol refers to the IP specific number of the protocol. The range for this value should be between 0 and 255. For example, 6 refers to the TCP protocol.	[0-255]
IP Source Route	Determine, Yes or No, whether to check the source route.	[Yes/No]
Destination: IP Addr	In this field, enter the destination IP Address of the packet you wish to filter. The address is usually written in dotted decimal notation such as a.b.c.d where a, b, c, and d are numbers between 0 and 255.	[a.b.c.d] where a,b,c,d=[0-255]
Destination: IP Mask	In this field, enter the IP mask that will be used to mask the bits of the IP Address given in Destination: IP Addr.	IP Address
Destination: Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535.	[0-65535]
Destination: Port # Comp	In this field, you can select what comparison quantifier you wish to use to compare to the value given in Source: Port #.	[None/Less/Greater/Equal/Not Equal]
Source: IP Addr	In this field, enter the source IP Address of the packet you wish to filter. The address is usually written in dotted decimal notation such as a.b.c.d where a, b, c, and d are numbers between 0 and 255.	IP Address [a.b.c.d] where a,b,c,d=[0-255]
Source: IP Mask	In this field, enter the IP mask that will be used to mask the bits of the IP Address given in 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.	[0-65535]
Source: Port # Comp	This field is dependent upon the IP Protocol field. This field will be inactive (N/A) unless the value in that field is 6 (TCP protocol). In this field you determine what type of	[Yes/No]

Field	Description	Option
	TCP packets to filter. There are two options:[Yes] - filter match only established TCP connections. [No] - filter match both initial and established TCP connections.	
TCP Estab	This field is dependent upon the IP Protocol field. This field will be inactive (N/A) unless the value in that field is 6 (TCP protocol). In this field you determine what type of TCP packets to filter. There are two options: Yes - filter match only established TCP connections. No - filter match both initial and established TCP connections.	[Yes/No]
More	In this field, you can determine if you want to pass the packet through the next filter rule before an action is taken. If More is [Yes], then Action Matched and Action Not Matched will be N/A.	[Yes / N/A]
Log	In this field, you can determine if you wish to log the results of packets attempting to pass the filter rule. These results will be displayed on the System Log. There are 4 options for this field: ● None - No packets will be logged. ● Action Matched - Only packets that match the rule parameters will be logged. ● Action Not Matched - Only packets that do not match the rule parameters will be logged. ● Both - All packets will be logged.	[None] [Action Matched] [Action Not Matched] [Both]
Action Matched	If the conditions for the filter rule are met, you can specify what to do with the packet.	[Check Next Rule] [Forward] [Drop]
Action Not Matched	If the conditions for the filter rule are not met, you can specify what to do with the packet.	[Check Next Rule] [Forward] [Drop]
Once you have completed filling in Menu 21.1.1 - TCP/IP Filter Rule, press [Enter] at the message [Press Enter to Confirm] to save your selections, or press [Esc] to cancel. This data will now be displayed on Menu 21.1 - Filter Rules Summary.		

9.2.2 Generic Filter Rule

This section will show you how to configure the protocol-independent parameters for a Generic filter rule for your *Prestige*. (For information on the protocol-dependent fields, refer to the previous section, TCP/IP Filter Rule and the following section, Novell IPX Filter Rule.)

Figure 9-5 displays Menu 21.1.2 - Generic Filter Rule

```
Menu 21.1.2 - Generic Filter Rule

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

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

Figure 9-5. Menu 21.1.2 - Generic Filter Rule

Table 9-6 describes the fields in the Generic Filter Rule Menu.

Table 9-6. Generic Filter Rule Menu Fields

Field	Description	Default
Offset	Offset refers to the value of the byte that you want to use as your starting offset. That is, in the data packet, at what point do you want to begin the comparison. The range for this field is from 0 to 255.	Default = 0
Length	This field refers to the length (in bytes) of the data in the packet that your <i>Prestige</i> should use for comparison and masking. The starting point of this data is determined by Offset. The range for this field is 0 to 8.	Default = 0

Table 9-6. Generic Filter Rule Menu Fields (continued)

Field	Description	Default
Mask	In this field, specify (in Hexadecimal) the value that your <i>Prestige</i> should logically qualify [and] the data in the packet. Since Length is given in bytes, you need to enter in twice the length hexadecimal numbers for this field. For example, if Length were 4, then a valid Mask must have 8 hexadecimal numbers, like 1155ABF8.	
Value	In this field, specify (in Hexadecimal) the value that your <i>Prestige</i> should use to compare with the masked packet. The value should align with Offset. Since Length is given in bytes, you need to enter in twice the length hexadecimal numbers for this field. For example, if Length were 4, then a valid Value must have 8 hexadecimal numbers, like 1155ABF8. If the result from the masked packet matches Value, then the packet is considered matched.	
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 selections, or press [Esc] to cancel. This data will now be displayed on Menu 21.1 - Filter Rules Summary.		

9.2.3 Novell IPX Filter Rule

This section will show you how to configure the protocol-dependent parameters for an IPX filter.

Figure 9-6 displays Menu 21.1.3 - IPX Filter Rule.

```
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 9-6. Menu 21.1.3 - IPX Filter Rule

Table 9-7 describes the IPX Filter Rule.

Table 9-7. IPX Filter Rule Menu Fields

Field	Description
IPX Packet Type	Enter the IPX packet type value of the packet you wish to filter. This value should be two hex-bytes.
Destination/Source Network #	Enter the four hex-byte destination/source network numbers of the packet that you wish to filter.
Destination/Source Node #	Enter in the six hex-byte value for the destination/source node number of the packet you wish to filter.
Destination/Source Socket #	Enter the destination/source socket number of the packets that you wish to filter. This should be a 4-byte hex value.
Destination/Source Socket # Comp	You can select what comparison quantifier you wish to use to compare to the value given in Destination Socket # and Source Socket #.
Operation	This field is only active if one of the Socket # fields is 0452 or 0453 indicating SAP and RIP packets. There are seven options for this field which determines the operation for the IPX packet. ● None. ● RIP Request. ● RIP Response. ● SAP Request. ● SAP Response. ● SAP Get Nearest Server Request. ● SAP Get Nearest Server Response
Once you have completed filling in Menu 21.1.3 - IPX Filter Rule, press [Enter] at the message [Press Enter to Confirm] to save your selections, or press [Esc] to cancel. This data will now be displayed on Menu 21.1 - Filter Rules Summary.	

Chapter 10

Simple Network Management Protocol

SNMP

About SNMP

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

10.1 Configuring Your *Prestige* For SNMP Support

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

- Step 1.** From the Main Menu, select option [22. SNMP Configuration]
- Step 2.** This will bring you to Menu 22 - SNMP Configuration, as shown in Figure 10-1.

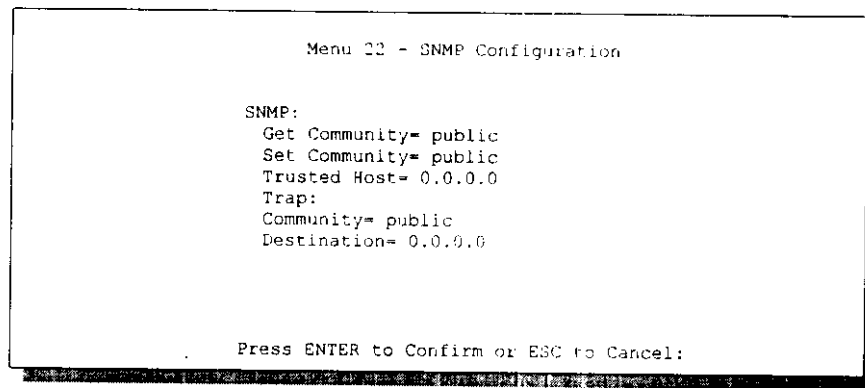


Figure 10-1. Menu 22 - SNMP Configuration

- Step 3.** You will then be prompted to enter the setup information. The following Table 10-1 describes the specific parameters involved in the configuration. The parameters you will have to fill in will be indicated in bold type.

Table 10-1. SNMP Configuration Menu Fields

Field	Description	Default
Get Community	You can determine the Get Community setting for your <i>Prestige</i> in this field. The value entered into this field will be used to authenticate the community field for the incoming Get- and GetNext- requests from the management station.	public
Set Community	In this field, enter the Set Community for your <i>Prestige</i> . The value entered in this field will be used to authenticate the community field for the incoming Set- requests from the management station.	public
Trusted Host	Enter the IP address of the trusted host SNMP management station. If this field is configured, then your <i>Prestige</i> will only respond to SNMP messages coming from this address. If you leave the field blank (default), then your <i>Prestige</i> will respond to all SNMP messages it receives, regardless of origin.	blank
Trap: Community	In this field, enter the community name that is sent with each trap to the SNMP manager. This should be treated like a password and match what the SNMP manager is expecting.	public
Trap: Destination	This field contains the IP address of the station that you wish to send your SNMP traps to.	blank
Once you have completed filling in Menu 22 - SNMP Configuration, press [Enter] at the message [Press Enter to Confirm] to save your selections, or press [Esc] to cancel.		

If you are unsure how to configure the fields for the SNMP configuration, consult your network administrator or MIS specialist.

Chapter 11

System Security

Your *Prestige* incorporates a number of security measures to prevent unauthorized access to your network. For example, your *Prestige* supports both PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol) in authenticating a Remote Node.

By default, your *Prestige* can store information about up to eight different users. If more dial-up users are necessary, an external RADIUS (Remote Authentication Dial In User Service) server can be used to provide centralized user security.

In addition, your *Prestige* also implements a user password to get into the SMT screen. You will have three attempts to enter the correct system password. If you do not do so, the SMT will kick you out. In addition, your *Prestige* will only support one user in the SMT at one time.

11.1 Using RADIUS Authentication

Your *Prestige* router has a built-in dial-up user list, which can hold up to eight users.

For multiple (>8) dial-in users, your *Prestige* supports an external authentication server (UNIX or NT server station) which may provide password storage and usage accounting for thousands of users.

11.1.1 Installing a RADIUS Server

To use RADIUS authentication, you will need to have a UNIX- or NT-based machine on your network to act as a [radiusd] server, as well as a copy of the [radiusd] server program itself.

You can obtain a copy of the RADIUS software, along with documentation for the server, at

<http://www.livingston.com/Tech/FTP/pub-le-radius.shtml>

or at

<ftp://ftp.livingston.com/pub/le/radius/>

Follow the included instructions to install the server on your UNIX- or NT-based server.

Once you have installed the server, you will need to edit the [dictionary] file in the RADIUS configuration directory (which will usually be [/etc/raddb]). Using any text editor, add the following lines to the [dictionary] file:

NETGEAR proprietary attributes

ATTRIBUTE	NETGEAR-Callback-Option	192 integer	
VALUE	NETGEAR-Callback-Option	None	0
VALUE	NETGEAR-Callback-Option	Optional	1
VALUE	NETGEAR-Callback-Option	Mandatory	2

Callback phone number source

ATTRIBUTE	NETGEAR-Callback-Phone-Source	193 integer	
VALUE	NETGEAR-Callback-Phone-Source	Preconfigured	0
VALUE	NETGEAR-Callback-Phone-Source	User	1

These changes allow the RADIUS server to be used with NETGEAR CLID authentication, as described in the section below.

11.1.2 Configuring the *Prestige* for RADIUS Authentication

To configure your *Prestige* to use the RADIUS server set up in the previous section, select option 23, System Security, from the Main Menu. This will bring you to Menu 23 - System Security. Then from this menu, select option 2, External Server to bring you to Menu 23.2 - System

Security - External Server as shown in Figure 11-1.

```

Menu 23.2 - System Security - External Server

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

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

```

Figure 11-1. Menu 23.2 - System Security - External Server

The fields in the System Security - External Server Menu are listed in Table 11-1.

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

Field	Description	Default
Active	Determines whether the external security facility is enabled. If this field contains No, only the built-in dial-up user list will be used. If this field contains Yes, the built-in dial-up user list will be searched first, then the external authentication server.	
Type	Determines the type of the external authentication server. At present only the RADIUS type is supported.	
Server Address	The IP address of your network's UNIX or NT-based RADIUS server.	
Port #	The IP port address used by the authentication server. The default value of [1645] should be used.	[1645]
Key	A "password" used to identify your <i>Prestige</i> as a valid client of the RADIUS authentication service.	

**Note to the Key Password Field**

The Key password should be stored in the [client] file in the RADIUS server's [/etc/raddb] directory. Lines of the following form should be added to the [client] file:

```
# Client Name      Key
#-----
192.168.0.1       1234
```

The Client Name field in the file gives the IP address of your *Prestige* router, and the Key field should be the same as the Key field in Menu 23.2.

After a RADIUS server has been configured, your *Prestige* will use it to authenticate all users that it can not find in its internal Dial-Up User List (see Menu 14)

11.1.3 Adding Users to the RADIUS Database

Your *Prestige* only uses the RADIUS database for user authentication; except for [Password], [Dialback-No], and the NETGEAR extensions [NETGEAR-Callback-Option] and [NETGEAR-Callback-Phone-Source] (described below), most standard RADIUS attribute fields are ignored by your *Prestige*.

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

```
joeuser      Password = "joepassword"
```

Similarly, each user should have a user name/password record in the [users] database.

11.1.4 Using RADIUS Authentication for CLID

To use RADIUS for CLID authentication, create a user record in the [users] file, where the user name (the first field) is the telephone number, and the password (the second field) is always [NETGEAR-CLID] (case-sensitive). The regular user name is put in a User-Name field. The

following is an example of a CLID user record:

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

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

11.2 Configure the SMT Password

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

- Step 1.** From the Main Menu, select option [23. System Security]
- Step 2.** From Menu 23 - System Security, you can select option [1. Change Password]. This will bring you to Menu 23.1 –
- Step 3.** In Menu 23.1 - System Security - Change Password, type in your previous system password and press [Enter].
- Step 4.** Type in your new system password and press [Enter].
- Step 5.** Re-type your new system password for confirmation purposes and press [Enter].

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

Chapter 12

Telnet Configuration and Capabilities

12.1 About Telnet Configuration

When you first configure your *Prestige*, it must be done via a computer connected to the RS-232 port. However, once your *Prestige* has been initially configured, you can use [telnet] to configure the device remotely as shown in Figure 12-1.

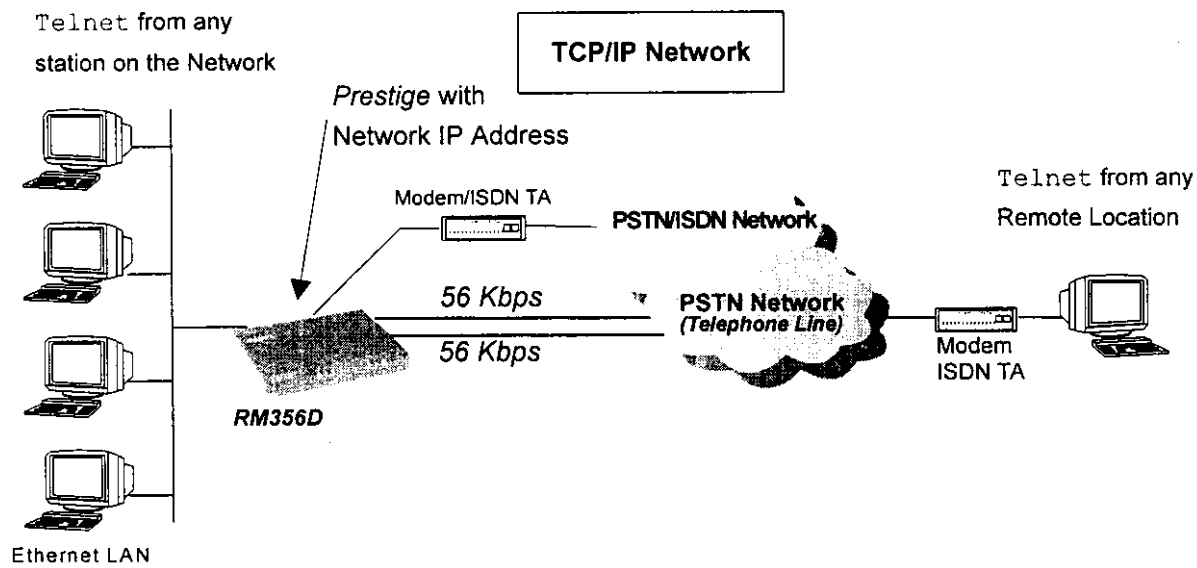


Figure 12-1. Telnet Configuration on a TCP/IP Network

In order to configure your *Prestige* in this way, you need to have assigned an IP Address to your PSTN Router/Hub and have connected it to your network. If your *Prestige* is configured for IPX routing but not IP in Menu 1, [telnet] will still be available provided you assign the *Prestige* an IP address.

12.2 Telnet Capabilities

12.2.1 Single Administrator

To prevent confusion and discrepancy on the configuration, your *Prestige* will only allow one terminal connection at any time. Your *Prestige* also gives priority to the RS-232 connection over [telnet]. If you have already connected to your *Prestige* via [telnet], you will be logged out if another user is connecting to the *Prestige* via the RS-232 cable. Only after the other administrator has been disconnected will you be able to [telnet] to your *Prestige* again.

12.2.2 System Timeout

When you are connected to your *Prestige* via [telnet], there is a system timeout of 5 minutes (300 seconds). If you are not configuring the device and leave it inactive for this timeout period, then your *Prestige* will automatically disconnect you.

Chapter 13

System Maintenance

Your *Prestige* provides diagnostic tools that you can use to maintain your device. Some of these tools include updates on system status, WAN Port status, log and trace capabilities and upgrades to the system software. This chapter will describe how to use these tools in greater detail.

System maintenance options are available in Menu 24 - System Maintenance, as shown in Figure 13-1.

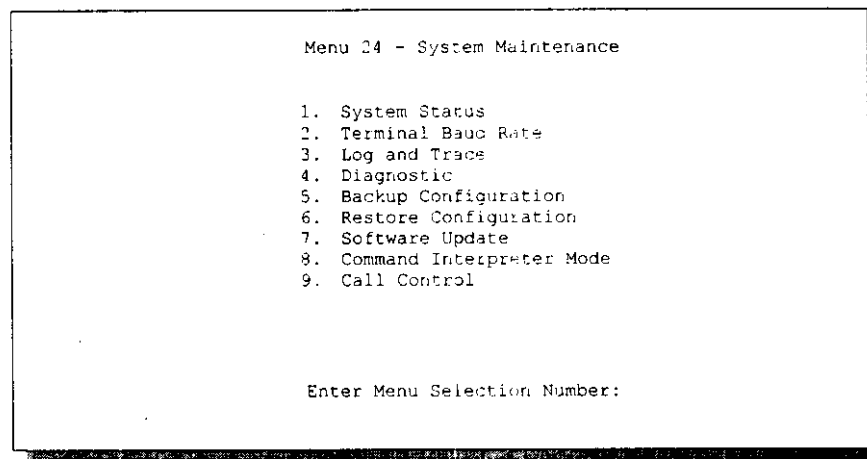


Figure 13-1. Menu 24 - System Maintenance

13.1 System Status

System Status is a tool that can be used to monitor your *Prestige*. Specifically, it will give you information on the status of your system software version, WAN Port, number of packets sent and number of packets received, as shown in Figure 13-2.

```

Menu 24.1 -- System Maintenance - Status

Port   Status   Kbps   TXPkts   RXPkts   Errors   Up Time
1      Idle     0Kbps   0         0         0       0:00:00
2      Down    0Kbps   0         0         0       0:00:00
3      Down    0Kbps   0         0         0       0:00:00

Total Outcall Time:      0:00:00

Ethernet:
  Status: 10M/Full Duplex
  TX Pkts: 26
  RX Pkts: 0
  Collisions: 0
  Name: RM356D
  RAS S/W Version: V1.6(e01) | 2/6/98
  Ethernet Address: 00:a0:c5:01:23:45

LAN Packet Which Triggered Last Call:

Press Command:

CMDS: 1-Drop Port1 2-Drop Port2 3-Drop Port3 8-Drop All 9-Rst Cnt ESC-Exit

```

Figure 13-2. Menu 24.1 - System Maintenance - Status

Follow the procedure below to go to the System Status Menu.

Step 1. Select option 24 from the Main Menu to access Menu 24 - System Maintenance.

Step 2. From Menu 24, select option [1. System Status].

Step 3. There are five possible commands in Menu 24.1 - System Maintenance - Status.

- Entering 1 or 2 or 3 will disconnect the call on the specified WAN port;
- Entering 8 will disconnect the calls on all WAN ports,
- Entering 9 will reset the counters; and [Esc] will exit this screen.

The following Table 13-1 describes the fields present in Menu 24.1 - System Maintenance - Status.

It should be noted that items 1-17 in this Table 13-1 are READ-ONLY and are meant to be used for diagnostic purposes.

Table 13-1. System Maintenance - Status Menu Fields

Field	Description
1. Port	Shows statistics for all WAN port respectively. These are the information displayed for each port from items 6 to 11 in this table.
2. Status	Shows the Remote Node the port is currently connected to or the status of the port ([Idle], [Calling], or [Answering]).
3. Kbps	The current connecting speed.
4. TXPkts	The number of transmitted packets on this port.
5. RXPkts	The number of received packets on this port.
6. Error	The number of error packets on this port.
7. Up Time	Time this port has been connected to the current Remote Node.
8. Total Outgoing call Time	Shows the total outgoing call time for all WAN ports since the system has been powered up.
9. Ethernet	Shows the current status of the LAN connection on your <i>Prestige</i>
10. Status	Shows the current status of the LAN
11. TX Pkts	The number of transmitted packets to LAN.
12. RX Pkts	The number of received packets from LAN
13. Collision	Number of collisions.

Table 13-1. System Maintenance - Status Menu Fields (continued)

Field	Description
14. Name	Displays the system name of your <i>Prestige</i> . This information can be modified in Menu 1 - General Setup.
15. RAS S/W Version	Refers to the version of the current RAS software.
16. Ethernet Address	Refers to the Ethernet MAC address assigned to your <i>Prestige</i> .
17. LAN Packet Which Triggered Last Call	Shows the first 48 octets of the LAN packet that triggered the last outgoing call. There are three different types of packets: IP, IPX, and RAW. By viewing the packet information, you can determine which station has sent a packet to cause your <i>Prestige</i> to make an outgoing call.

Figure 13-3 shows two examples of LAN Packets: the first of an ICMP Ping packet (Type: IP) triggering the call and the second with a SAP broadcast packet (Type: Raw) triggering the call. With this information, you can determine the source IP address of the packet or the source MAC address of the packet.

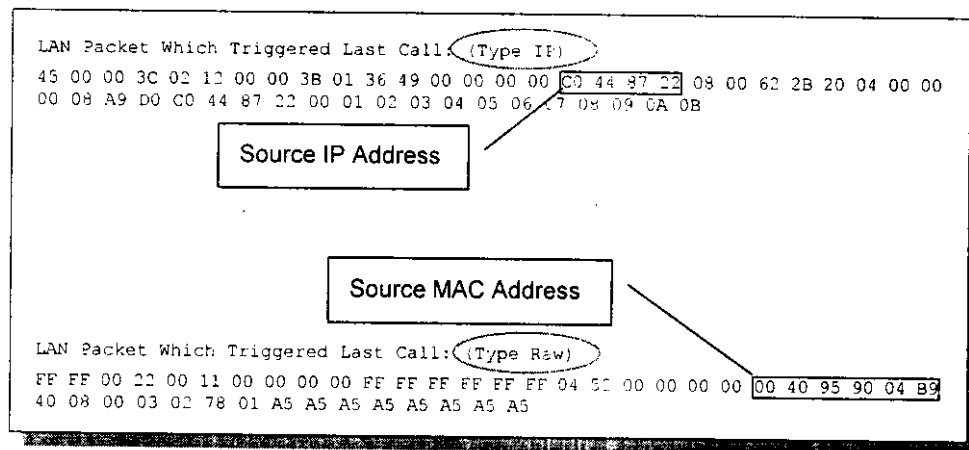


Figure 13-3. LAN Packet Which Triggered Last Call

13.2 Terminal Baud Rate

Users can set up different baud rates for the RS-232 connection through Menu 24.2 - Terminal Baud Rate. Your *Prestige* supports 9600 (default), 19200, 38400, 57600, and 115200bps for the RS-232 connection. The terminal baud rate is displayed in Menu 24.2, as shown in Figure 13-4.

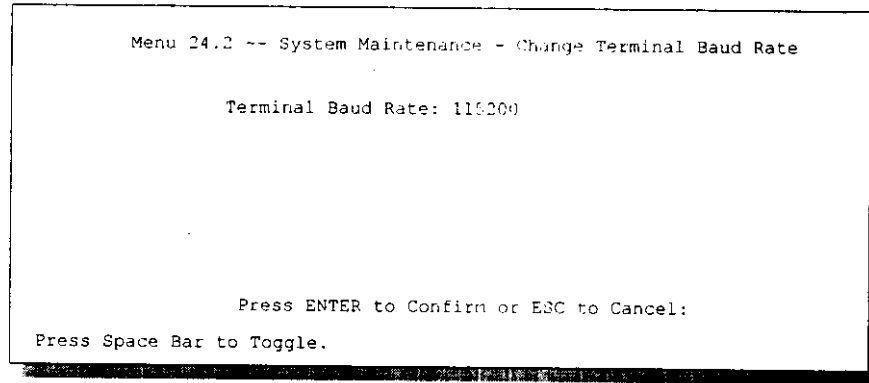


Figure 13-4. Menu 24.2 - System Maintenance - Change Terminal Baud Rate

13.3 Log and Trace

Log and trace tools allow users of the *Prestige* to view the error logs and trace records to troubleshoot any errors that may occur. The *Prestige* is also able to generate syslogs to send to other machines.

Follow the procedure below to get to the Log and Trace:

- Step 1.** Select option 24 from the Main Menu to access Menu 24 - System Maintenance.
- Step 2.** From Menu 24, select option 3 to bring you to Menu 24.3 - System Maintenance - Log and Trace.

Step 3. You will be given two options.

1. View Error Log.
2. Syslog and Accounting.

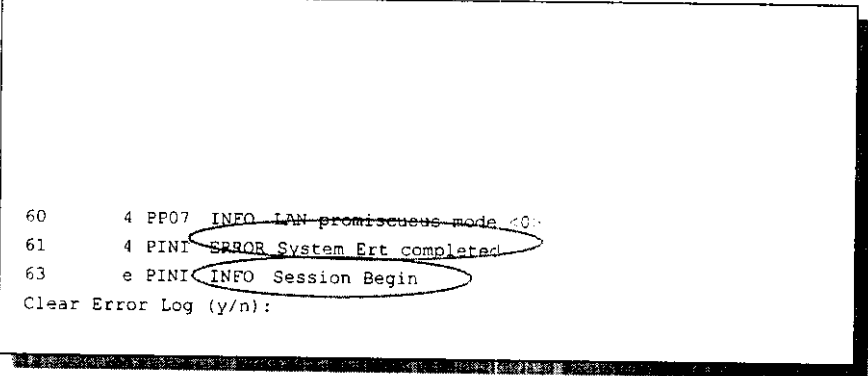
The following list describes the fields involved in the trace and log options.

13.3.1 View Error Log

Selecting the first option from Menu 24.3 - System Maintenance - Log and Trace will display the Error Log in the system. The Error Log does not only provide the error messages but it is also a source of information about your *Prestige*.

You can also clear the Error Log on your *Prestige*. After each display, you are prompted with an option to do so. Enter the appropriate choice and press [Enter].

Examples of typical Error and Information Messages are presented in Figure 13-5.



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

Figure 13-5. Examples of Error and Information Messages

13.3.2 Syslog And Accounting

Syslog and Accounting can be configured in Menu 24.3.2 - System Maintenance - Syslog and Accounting, as shown in Figure 13-6. This menu configures your *Prestige* to send UNIX syslogs to another machine.

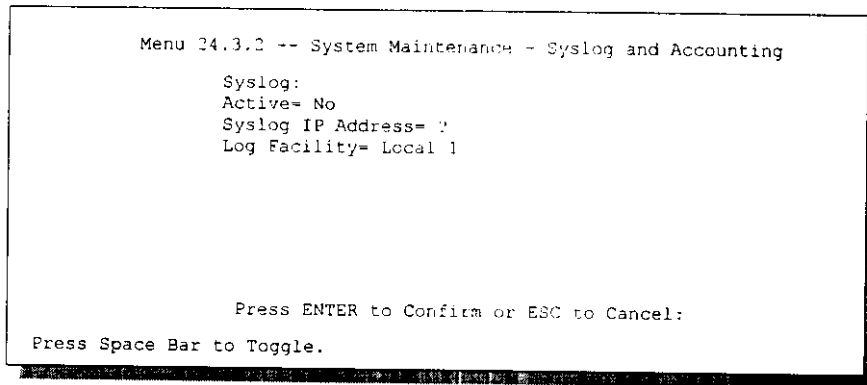


Figure 13-6. Menu 24.3.2 - System Maintenance - Syslog and Accounting

The User needs to configure the following 3 parameters described in Table 13-2 to activate syslog.

Table 13-2. System Maintenance Menu Syslog Parameters

Parameter	Description
Active	Use the space bar to turn on or off the syslog option
Syslog IP Address	Input the IP Address that you wish to send your syslog to. The address is usually written in dotted decimal notation such as a.b.c.d where a, b, c, and d are numbers between 0 and 255.
Log Facility	Use the space bar to toggle between the 7 different Local options. This feature is used for UNIX application.

Your *Prestige* will send three different types of syslog messages: Call information messages (i.e. CDR), Error information messages, and Session information messages. Some examples of these syslog messages are shown below:

Call Information Messages:

line 1 channel 1, call 41, C01, Incoming Call, 40001
line 1 channel 1, call 41, C01, ANSWER Connected, 64K 40001
line 1 channel 1, call 41, C01, Incoming Call, Call Terminated

Error Information Messages:

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

Session Information Messages:

line 1, channel 1, call 41, I01, IPCP up, 306L
line 1, channel 1, call 41, I01, IPCP down, 306L

13.4 Diagnostic

The diagnostic functions on your *Prestige* allow you to test aspects of your device to determine if they are working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown in Figure 13-7. provides a short description to the types of diagnostic tests available to your system.

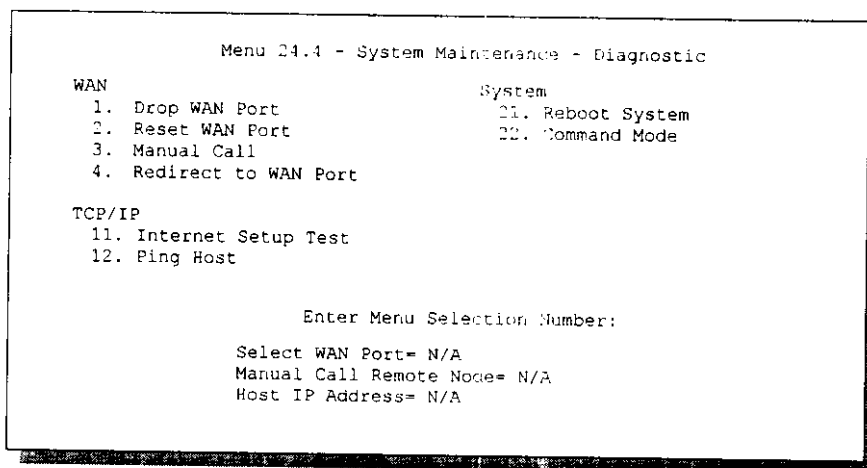


Figure 13-7. Menu 24.4 - System Maintenance - Diagnostic

Follow the procedure below to get to Diagnostic

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

The following Table 13-3 describes the eight diagnostic test options available in Menu 24.4 to test your *Prestige* and its connections.

Table 13-3. System Maintenance Menu Diagnostic Test Options

Fields	Description
Drop WAN Port	This command will drop the call in the specified WAN port.
Reset WAN Port	This command will reset the specified WAN port.
Redirect to WAN Port	This command will redirect SMT (System Manager Terminal) to the specified WAN port. To redirect to a WAN Port, you must set [Port Speed] of the WAN Port (in Menu 2) to match [Terminal Baud Rate] in Menu 24.2.
Internet Setup Test	This test checks to see if your Internet access configuration has been done correctly. When this option is chosen, your <i>Prestige</i> will PING the Internet IP Address. If everything is working properly, you will receive an appropriate response. Otherwise, note the error message and consult your network administrator.
Ping Host	This diagnostic test pings the host which determines the functionality of the TCP/IP protocol on your system.
Reboot System	This option reboots the system. This serves to implement any changes that may have been recently added to your system.
Command Mode	This option allows the user to enter the command mode. This mode allows you to diagnose and test your <i>Prestige</i> using a specified set of commands.
Manual Call	This provides a way for the users of the <i>Prestige</i> to place a manual call to a Remote Node. This tests the connectivity to that Remote Node. When you use this command, you will see traces displayed on the screen showing what is happening during the call setup and protocol negotiation.

Figure 13-8 displays an example of a successful connection after selecting option [3. Manual Call] in Menu 24.4.

```
Start dialing for node <1>
### Hit any key to continue. ###
Dialing chan<2> phone<last 9-digit>:40101
Call CONNECT speed<64000> chan<2> prot<1>
LCP up
CHAP send response
CHAP login to remote OK!
IPCP negotiation started
IPCP up
```

Figure 13-8. Trace Display for a Successful IPCP Connection Via Manual Call

On the opposite, Figure 13-9 shows an example of a Trace Display for a Failed IPCP Connection via Manual Call.

```
Start dialing for node <1>
### Hit any key to continue. ###
Dialing chan<2> phone<last 9-digit>:40101
Call CONNECT speed<64000> chan<2> prot<1>
LCP up
CHAP send response
***Login to remote failed. Check name/passwd.
Receive Terminal REQ
IPCP down
Line Down chan<2>
```

Figure 13-9. Trace Display for a Failed IPCP Connection Via Manual Call

13.5 Backup Configuration

Selecting option 5 from Menu 24 - System Maintenance will allow you to backup your current *Prestige* configuration onto disk. Backup is highly recommended once your *Prestige* configuration is functioning.

You need to download the configuration onto disk. The procedure for downloading varies depending on the type of software used to access the *Prestige*, but you must use the XMODEM protocol to perform the download.

13.6 Restore Configuration

Selecting option 6 from Menu 24 - System Maintenance will restore backup configuration from disk to the *Prestige*. You need to upload a backup file to the *Prestige*. The procedure for uploading varies depending on the type of software used to access the *Prestige*, but you must use the XMODEM protocol to restore the configuration.

Keep in mind that the configuration data are stored on flash ROM in the *Prestige*, so even if power failure were to occur, your configuration is safe.

13.7 Software Update

Software updates are only possible through the RS-232 cable connection. You cannot use telnet to update the software version of your *Prestige*. Note that this function will delete the old software before installing the new software. Do not attempt to utilize this menu unless you have the new software version. There are two different software updates: RAS code and ROM File, as shown in Menu 24.7 (Figure 13-10).

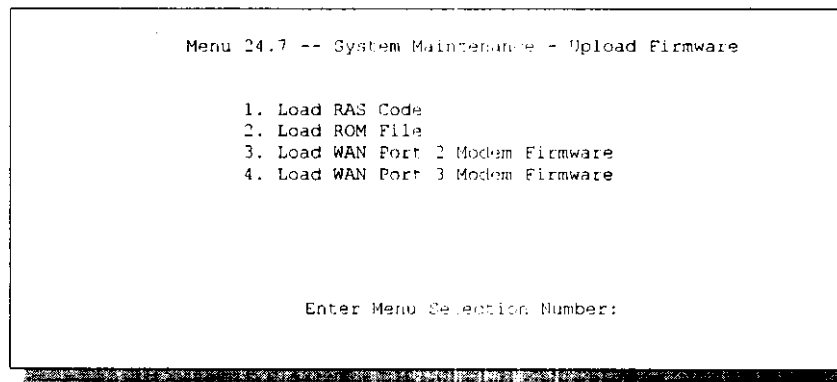


Figure 13-10. Menu 24.7 - System Maintenance - Upload Firmware

13.7.1 Load RAS code

Type [atur] and wait until your *Prestige* responds with an [OK] to begin uploading the new software (upload procedure varies depending on the type of software used to access your *Prestige*). You must use the XMODEM protocol to perform the upload. After uploading is successful, type [atgo] to start your *Prestige*. Below is an example of downloading RAS using PCPLUS.

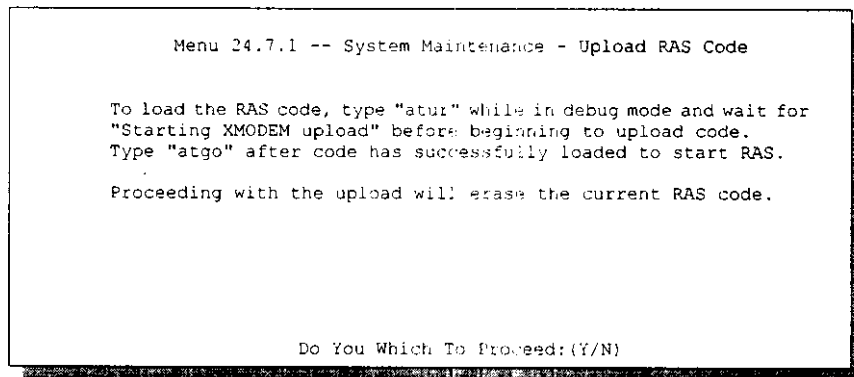


Figure 13-11. Menu 24.7.1 - Example of Uploading RAS Using PCPLUS

13.7.2 Load ROM File

Type [atur3] and wait until your *Prestige* responds with an [OK] to begin uploading the new ROM File, as shown in Figure 13-12. ROM File includes *Prestige* configuration, system-related data, error and trace log. After uploading the new ROM File, you will lose all data. You need to set the SMT baud rate to the default: 9600. You also need to reconfigure your *Prestige*.

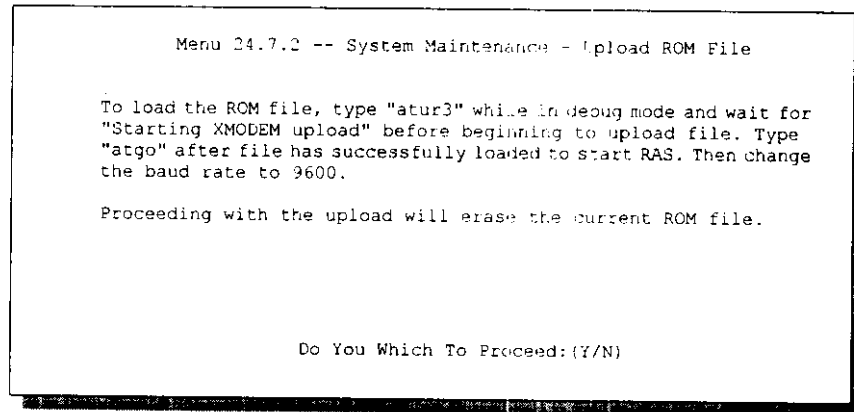


Figure 13-12. Menu 24.7.2 - System Maintenance - Upload ROM File

13.7.3 Load Modem Firmware

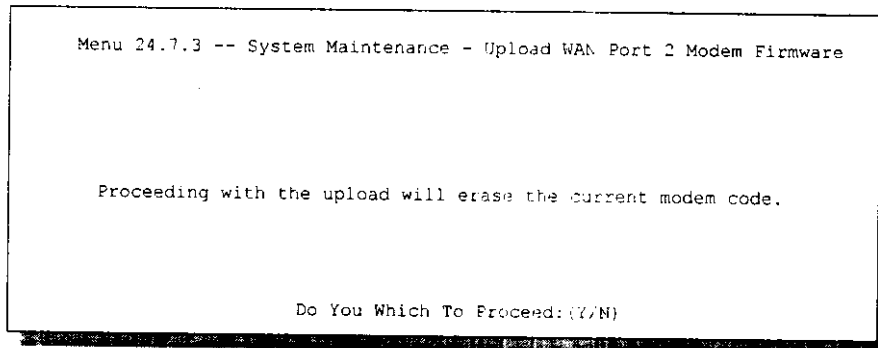


Figure 13-13. Menu 24.7.3 - System Maintenance - Upload WAN Port 2 Modem Firmware

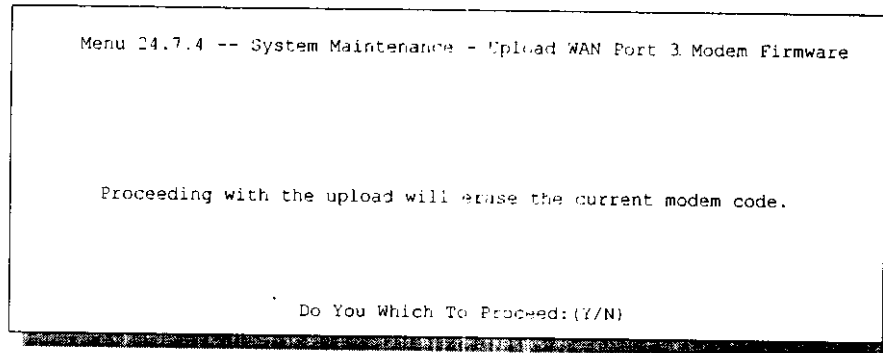


Figure 13-14. Menu 24.7.4 - System Maintenance - Upload WAN Port 2 Modem Firmware

13.8 Command Interpreter Mode

This option allows the user to enter the command interpreter mode. This mode allows you to diagnose, test, and configure your *Prestige* using a specified set of commands. A list of valid commands can be found by typing [help] at the command prompt. For more detailed information, check the NETGEAR Web site or send an e-mail to the NETGEAR Support Group.

13.9 Call Control

The *Prestige* provides two Call Control Management functions for the Remote Node and Remote Dial-in User. They are the Budget Management and Blacklist.

The Budget Management function provides the budget control for the outgoing call and a way for users to set a limit on their PSTN/ISDN line utilization to prevent any accidental usage. It limits the total outgoing call time of the *Prestige* over a period of time for each Remote Node & Remote Dial-in User (callback only). If the total outgoing call time exceeds the set limit, future outgoing calls will not be made and the current call will be dropped.

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

To enter the Call Control Menu, select option [9. Call Control] in Menu 24 to go to Menu 24.9 - System Maintenance - Call Control, as shown in Figure 13-15.

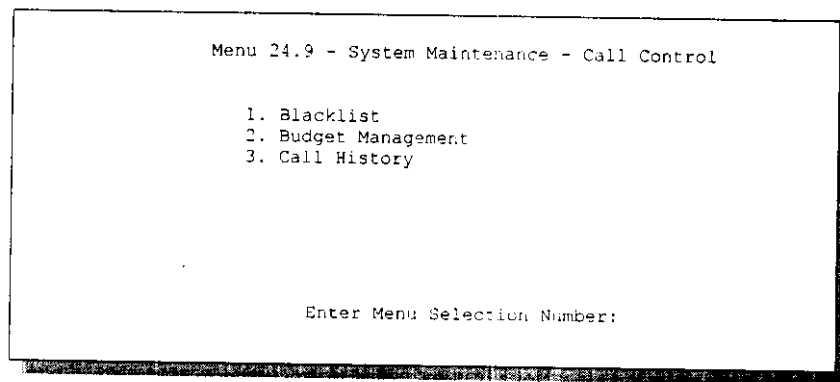
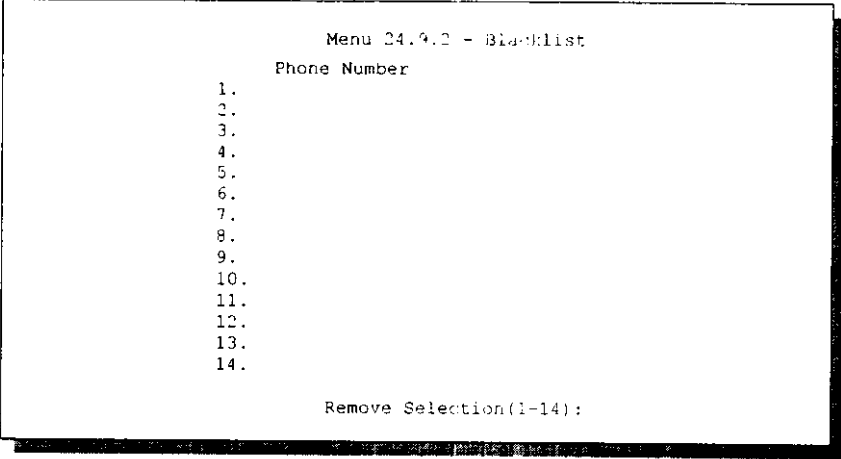


Figure 13-15. Menu 24.9 - System Maintenance - Call Control

13.9.1 Blacklist

Menu 24.9.2 shown in Figure 13-16 displays the list of dial-out telephone numbers blacklisted.



Menu 24.9.2 - Blacklist

Phone Number

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

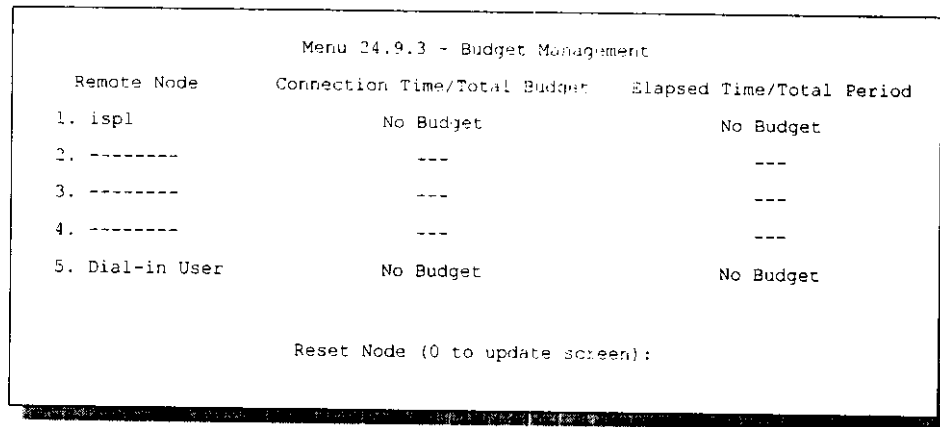
Remove Selection(1-14):

Figure 13-16. Menu 24.9.2 - Blacklist

The phone numbers on this list cannot be entered directly, instead, they are numbers which have had problems connecting in the past. The user can take a number off the list by entering the index number of entry.

13.9.2 Budget Management

The Budget Management parameters for outgoing calls to Remote Nodes and Dial-in User can be viewed in Menu 24.9.3, as shown in Figure 13-17.



Remote Node	Connection Time/Total Budget	Elapsed Time/Total Period
1. ispl	No Budget	No Budget
2. -----	---	---
3. -----	---	---
4. -----	---	---
5. Dial-in User	No Budget	No Budget

Reset Node (0 to update screen):

Figure 13-17. Menu 24.9.3 - Budget Management

The total budget is the time limit for an outgoing call to a Remote Node or Dial-in User. When this limit is reached, the call will be dropped and further outgoing calls to that Remote Node or Remote Dial-in User (callback) will fail. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours. This means no budget control. The user can reset the total outgoing call time through this menu. The total outgoing call timer can be programmed to reset itself periodically through the Menu 11 and 13.

Chapter 14

Troubleshooting

This chapter covers possible ways of dealing with potential problems you may run into when using your *Prestige*. After each problem description, we have provided some instructions to help you diagnose and solve the problem.

14.1 Problems Starting Up the *Prestige*

Table 14-1. Troubleshooting the Start-Up of your *Prestige*

Troubleshooting	Corrective Action	
None of the LEDs are on when you power on the <i>Prestige</i>	Check the power cord and the power supply and make sure it is properly connected to your <i>Prestige</i>. If the error persists you may have a hardware problem. In this case you should contact technical support.	
Connecting the RS-232 cable, cannot access the SMT	1. Check to see if the <i>Prestige</i> 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 Baud rate.
		No parity, 8 Data bits, 1 Stop bit.

14.2 Problems With the WAN Ports

Table 14-2. Troubleshooting a WAN Port Connection

Troubleshooting	Corrective Action
RDY LED of a WAN Port is not ON	Check if WAN Port 1 is connected to an external modem/ISDN TA.
	Check if LINE 1 or LINE 2 is connected to a PSTN telephone line.
	Check if the power of the external modem/ISDN TA is turned on.

14.3 Problems with the LAN Interface

Table 14-3. Troubleshooting the LAN Interface

Troubleshooting	Corrective Action
Can't PING any station on the LAN	Check the LAN LED on the front panel of your <i>Prestige</i> . If it is on, then the link is up. If it is off, then check the cables connecting your <i>Prestige</i> to your LAN.
	Check the type of Ethernet interface that you have configured in Menu 3.1. Verify that you are using the same (AUI or 10BaseT) as configured in this menu.
	Verify with your network administrator that the IP address and the IP subnet mask configured in Menu 3.2 are valid for that LAN.
	Check the physical Ethernet cable, and make sure the connections on the <i>Prestige</i> and also to the hub are secure

14.4 Problems Connecting to a Remote Node or ISP

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

Troubleshooting	Corrective Action
Can't Connect to a Remote Node or ISP	Check Menu 24.1 to verify the PSTN/ISDN status. If it indicates [down], then refer to the section on the PSTN/ISDN line problems.
	In Menu 24.4.5, do a manual call to that Remote Node. You will see some messages printed onto the screen. The messages will show you whether the call has been connected or not. If the call is not connected, verify the following parameters in Menu 11: Pri(mary) Phone #, Sec(ondary) Phone #, and Transfer Rate.
	If the call is connected, but the call still terminates, then there may be some kind of negotiation problem. Verify the following parameters in Menu 11: My Login, My Password, Route, IP LAN Addr. Also verify your IP address in Menu 3.2.
	If you check the error log in Menu 24.3.1, this will usually give you some logs regarding why the call was dropped. If there is nothing in the log, the call may have been dropped by the remote device that you dialed in to. Make sure that the configuration parameters between these two devices are consistent.

14.5 Problems Connecting to a Remote User

Table 14-5. Troubleshooting a Connection to a Remote User

Troubleshooting	Corrective Action
Can't Connect to a Remote User	First verify that you have configured the authentication parameters in Menu 13. These would be CLID Authen, Recv. Authen, and Mutual Authen.
	If the Remote Dial-in User is negotiating IP, verify that the IP address is supplied correctly in Menu 13. Check that either the Remote Dial-in User is supplying a valid IP address, or that the <i>Prestige</i> is assigning a valid address from the IP pool.
	If the Remote Dial-in User is negotiating IPX, verify that the IPX network number is valid from the IPX pool (if it is being used).
	In Menu 14, verify the user name and password for the Remote Dial-in User.

Index

10Base-T, 1-4, 2-2, 2-5

56K Modem

2 built-in 56K modems, 1, 1-1, 1-3, 2-5, 2-16, 2-17,
2-18

A

Active field, 3-16

AUI, 14-2

B

Backup Configuration, 13-12

Backup ISP Account, 3-15

BACP, 1-6, 3-10, 5-6, 5-8

BAP, 1-6

Baud Rate, 13-5, 13-10

BOD, 4-1, 5-8, 5-9, 5-10

Branch Office, 1-9

Bridging, 1, ii, xix, xx, 1-1, 1-5, 2-1, 2-3, 2-13, 2-21,
2-22, 5-1, 5-6, 5-7, 5-17, 6-2, 6-4, 7-7, 7-8, 8-1, 8-2,
8-3, 8-4, 8-5, 8-6, 8-7, 12-2

Bridging Configuration, 8-4

C

Call Control

blacklist, 13-16, 13-17

budget management, 13-16, 13-18

Call Control Parameters, 2-18, 2-20

Callback

budget, 4-6

field, 4-6, 4-7

function, 2-19

CCP, 1-7, 5-10, 5-19

CDR, 13-8

CHAP, 1-6, 1-10, 2-13, 4-5, 5-5, 5-15, 11-1

CLID, 2-19, 4-5, 4-10, 5-4, 11-2, 11-4, 11-5, 13-8, 14-
4

Client, 3-7, 4-2, 7-2, 7-5, 7-8, 7-9, 8-1, 8-2, 8-3, 11-3,
11-4

Connecting

adapter cables, 2-1, 2-4

cables, 2-4

computer and VT100 terminal, 2-4

Ethernet LAN, 2-5

power adapter, 2-5

RM356D, 2-3

Corporate Office, 1-9

D

DHCP, 1-6, 2-22, 3-6, 3-7

Dial On Demand, 5-1

Dial-in

default dial-in setup, 2-9, 4-4, 4-5, 4-6, 4-7, 8-6

users setup, 4-5
Dial-in Server, 4-3
Dial-in User, 1-1, 1-10, 2-9, 3-13, 4-1, 4-2, 4-4, 4-5, 4-6, 4-7, 4-8, 4-9, 4-10, 5-3, 5-13, 13-16, 13-18, 14-4
DNS, 3-7, 3-9

E

Ethernet
interface, 1-3, 14-2
setup, 2-9, 2-21, 2-22, 3-6, 3-7, 3-8, 7-3, 7-4, 7-5, 8-2, 8-3

F

Filtering, 9-1, 9-2
call filter, 5-7, 5-18, 7-3, 8-1, 9-1
filter rules, 9-2, 9-4, 9-5, 9-7, 9-9, 9-11, 9-13
filter type, 9-5, 9-6, 9-7
filters sets, 2-21, 2-22, 4-7, 5-7, 5-18, 9-2, 9-3
Firmware, 13-14, 13-15
FTP, vii, 3-10, 11-2

G

Gateway IP Address, 6-8

I

IANA, 3-4, 3-13
ICMP, 3-13, 13-4
Idle Timeout, 4-7, 5-8, 5-18

Internet

Internet Access, xix, xx, 1-8, 2-9, 2-13, 2-22, 3-1, 3-5, 3-9, 3-10, 3-11, 3-14, 6-3, 6-4, 6-6
ISP, 1-8, 3-1, 3-4, 3-9, 3-10, 3-11, 3-12, 3-13, 3-15, 3-16, 3-17, 14-3
Internet Connection
test, 2-9, 3-11, 3-15
IP Address, 3-1, 3-2, 3-4, 3-8, 3-9, 3-10, 3-16, 4-6, 6-3, 6-4, 6-8, 8-7, 9-8, 12-2, 13-7, 13-10
IP Pool, 3-7, 4-6
IP Subnet Mask, 3-2, 3-3, 3-8, 6-4, 6-8, 14-2
IPCP, 13-8, 13-11
ISDN TA, 1-1, 1-4, 1-5, 1-10, 2-2, 2-4, 2-6, 2-14, 2-15, 2-16, 2-17, 2-18, 2-19, 3-11, 4-2, 5-6, 5-16, 9-1, 14-2

L

LAN-to-LAN

applications, xix, xx, 1-1, 1-8, 1-9, 2-9, 4-1, 6-3
Login
name, 3-9, 3-10, 5-4, 5-14

M

Manual Call, 13-10, 13-11
Metric, 6-5, 6-8
Modem
external modem, 1-1, 1-5, 1-6, 2-6, 2-14, 2-15, 2-16, 2-17, 2-18, 14-2
internal 56K modems (x2), 1, 1-1, 1-3, 2-5, 2-16, 2-17, 2-18
MP, 1-6, 1-10, 3-10, 5-6, 5-8, 5-10, 5-19

Multiple Link. 4-6, 5-10

N

NAT, 3-13

Netware

server, 7-9

Novell IPX, xix, xx, 1-5, 1-9, 2-22, 7-1, 7-4, 7-5, 7-6,
7-7, 7-8, 7-10, 9-4, 9-6, 9-10, 9-12

P

PAP, 1-6, 1-10, 4-5, 5-5, 5-15, 11-1

Password, 1-6, 2-7, 2-10, 2-11, 3-9, 3-10, 4-5, 4-9, 5-4,
5-5, 5-14, 5-15, 5-17, 11-1, 11-4, 11-5, 14-3

Phone Number

pri(mary), 3-10, 14-3

sec(ondary), 3-10, 5-6, 14-3

Power Adapter, 2-1, 2-5

PPP, 1-6, 1-10, 3-10, 4-5, 5-6, 5-7, 5-9, 5-10, 5-11, 5-
12, 5-17, 5-19, 8-6

PPP Options, 4-5, 5-7, 5-9, 5-10, 5-11, 5-17, 5-19, 8-6

Primary ISP, 3-16

Private IP Address, 3-4

PSTN

initialization, 2-6

R

RADIUS, 1-6, 4-1, 11-1, 11-2, 11-3, 11-4

RAS, 13-4, 13-12, 13-13

Remote Node

configuration, xx, 4-3, 5-1, 6-2, 8-2

network layer options, 5-7, 5-17, 6-2, 6-3, 6-4, 6-5,
7-7, 7-8, 8-4

profile, 5-1, 5-2, 5-3, 5-4, 5-5, 5-6, 5-7, 5-8, 5-9, 5-
12, 5-13, 5-14, 5-15, 5-16, 5-17, 5-18, 5-19, 6-2,
6-3, 7-7, 8-4, 8-5

setup, 2-9, 5-1, 5-2, 6-2, 6-8, 7-7, 7-10, 8-4

RIP, 3-8, 3-16, 5-8, 5-18, 6-5, 6-6, 7-3, 7-8, 8-1, 8-2,
9-1, 9-13

direction, 3-8

RJ-11 cable, 1-4, 2-1

RJ-45 cable, 1-4, 2-1, 2-4, 2-5

ROM, vii, 2-14, 13-12, 13-14

Routing, 2-13, 3-5, 5-6, 5-7, 5-17, 6-2, 6-4, 6-6, 6-8, 7-
7, 7-8, 7-9, 8-7, 9-8, 14-3

RS-232 cable, iii, 2-1, 2-4, 12-2, 13-12, 14-1

S

Seed router, 7-3, 7-5

Server, xx, 1-6, 1-10, 2-9, 3-7, 3-9, 3-10, 3-13, 3-15,
4-1, 4-3, 4-10, 6-4, 7-1, 7-2, 7-3, 7-5, 7-6, 7-8, 7-9,
7-10, 8-1, 8-2, 8-3, 9-13, 11-1, 11-2, 11-3, 11-4

SMT, xix, xx, 1-4, 2-1, 2-4, 2-6, 2-7, 2-8, 2-9, 2-10, 2-
11, 3-9, 3-11, 11-1, 11-5, 13-10, 13-14, 14-1

SNA, 2-13, 5-6, 5-17, 7-1, 7-5

SNMP, xx, 1-6, 2-9, 2-13, 10-1, 10-2, 10-3

Software

update, 13-12

Static Route, 6-1, 6-6, 6-7, 7-9, 7-10, 8-6, 8-7

IP static route, 6-7, 6-8, 7-10

setup, 6-6, 6-7, 7-9, 8-6

SUA, 3-12, 3-13, 3-14, 3-15

Subnet Mask, 3-2, 3-3, 3-8, 3-16, 6-4, 6-8

Subnetting, 3-2, 3-3, 3-8, 6-6

Subnetwork, 6-6

Class C, 3-12, 6-6

System Maintenance, xx, 2-9, 13-1, 13-2, 13-3, 13-4,
13-5, 13-6, 13-7, 13-9, 13-10, 13-12, 13-13, 13-14,
13-15, 13-16

diagnostic, 13-9, 13-10

system status, 13-2

System Management Terminal, xix, 2-6, 2-7, 2-8, 2-9

System Security, xx, 2-9, 2-10, 2-11, 4-1, 11-1, 11-2,
11-3, 11-5

T

TCP/IP

configuration, xx, 6-1, 6-4, 6-5

Telco Options, 4-5, 5-7

Telecommuting, xx, 1-8, 1-10, 4-1, 4-2

telecommuter, 4-2

Telnet

configuration, xx, 2-4, 12-1

Transfer Rate, 14-3

Troubleshooting

connecting, 14-3, 14-4

LAN interface, 14-2

starting up, 14-1

WAN port connection, 14-2

U

UDP, 3-13

UNIX, 6-4, 11-1, 11-2, 11-3, 13-7

UTP, 1-3, 2-5

W

WAN Port Setup, 2-9, 2-14, 2-15, 2-16, 2-17, 2-18, 2-
19, 2-20, 3-10, 5-12, 5-14

X

XMODEM, 13-12, 13-13

Z

NETGEAR

Support Group, 13-15

Website, vii