

# Reference Guide for the Model RT328 and Model RH348 ISDN Routers

## **NETGEAR**

**NETGEAR**, Inc.  
4500 Great America Parkway  
Santa Clara, CA 95054  
USA

M-RH348NA-2  
September 2000

© 2000 by NETGEAR, Inc. All rights reserved.

## Trademarks

NETGEAR™ is a trademark of Netgear, Inc. Windows® is a registered trademark of Microsoft Corporation. Other brand and product names are trademarks or registered trademarks of their respective holders. Information is subject to change without notice. All rights reserved.

## Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

## Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

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

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

**Note:** 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 residential installation. 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. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

## EN 55 022 Declaration of Conformance

This is to certify that the Model RT328 ISDN Router and the Model RH348 ISDN Router are shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

## Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das Model RT328 ISDN Router und Model RH348 ISDN Router gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

## Certificate of the Manufacturer/Importer

It is hereby certified that the Model RT328 ISDN Router and the Model RH348 ISDN Router have been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

## VCCI-2 Statement

This equipment is in the 2nd Class category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference.

Read instructions for correct handling.

## Customer Support

For assistance with installing and configuring your NETGEAR system or with post-installation questions or problems, contact your point of purchase representative.

To contact customer support or to purchase additional copies of this document and publications for other NETGEAR products, you can contact NETGEAR at the following numbers:

- Phone:

Australia:	1800-787-638	Korea:	00308-11-0319
Austria:	00800-06384327 (00800-0-NETGEAR)	Netherlands:	0800-023-0981
Denmark:	808-82179	New Zealand:	00800-1233-4566
Canada:	1-888-NETGEAR	Norway:	800-12041
Finland:	0800-111-036	Singapore:	001-800-1233-4566
France:	0800-77-17-53	Sweden:	0200-298-298
Germany:	00800-06384327 (00800-0-NETGEAR)	Switzerland:	00800-0638-4327 (00800-0-NETGEAR)
Hong Kong:	001-800-1233-4566	United Kingdom:	020-7216-0014
Japan:	0120-66-5402	United States:	1-888-NETGEAR
		All Other Countries:	+1 801-236-8499

## World Wide Web

NETGEAR maintains a World Wide Web Home Page that you can access at the universal resource locator (URL) <http://www.NETGEAR.com>. A direct connection to the Internet and a Web browser such as Internet Explorer or Netscape are required.



# Contents

## Preface

Purpose .....	xv
Audience .....	xv
Conventions .....	xvi
Special Message Formats .....	xvi
Use of Enter, Type, and Press .....	xvi
Other Conventions .....	xvii
Related Publications .....	xvii

## Chapter 1

### Introduction

About the Router .....	1-1
Features .....	1-1
Key Features .....	1-2
ISDN Support .....	1-3
Multilink PPP Support .....	1-3
TCP/IP Support .....	1-4
IP Address Masquerading by Dynamic NAT+ .....	1-4
Automatic Configuration of Attached PCs by DHCP .....	1-4
Security .....	1-4
Calling Line Identification .....	1-4
PAP and CHAP Authentication .....	1-5
Callback .....	1-5
Management Support .....	1-5
Basic Router Concepts .....	1-6
What is a Router? .....	1-6
Routing Information Protocol .....	1-6
IP Addresses and the Internet .....	1-7
Netmask .....	1-9

Subnet Addressing .....	1-10
Private IP Addresses .....	1-12
Single IP Address Operation Using NAT .....	1-13
Address Resolution Protocol .....	1-14
Domain Name Server .....	1-14
IP Configuration by DHCP .....	1-15

## **Chapter 2**

### **Router Installation and Connection**

Package Contents .....	2-1
ISDN Services Checklist .....	2-2
Network Checklist .....	2-3
Connecting the Router .....	2-4
Connecting the Serial Cable (Optional) .....	2-7
Connecting to the ISDN Port .....	2-7
Connecting the Ethernet Cable .....	2-7
Using Twisted Pair LAN Cabling .....	2-8
Using Coaxial or Fiber LAN Cabling .....	2-8
Connecting to the Hub Ports in the Model RH348 Router .....	2-8
Connecting a Telephone, Fax, or Modem .....	2-8
Connecting the Power Adapter .....	2-8
Connecting for Configuration .....	2-9
Connecting Through a Serial Port .....	2-9
Connecting Through a Telnet Connection .....	2-9

## **Chapter 3**

### **Router Configuration**

Configuration Methods .....	3-1
Powering on the Router .....	3-2
Navigating the Manager .....	3-3
Manager Menu Summary .....	3-5
General Setup Menu .....	3-6
ISDN Menus .....	3-7
North American ISDN Menu .....	3-7
DSS1 ISDN Menu .....	3-8

Ethernet Setup .....	3-11
General Setup Menu .....	3-11
DHCP and TCP/IP Setup .....	3-12
Manager Password Setup .....	3-14
<b>Chapter 4</b>	
<b>Configuration for Internet Access</b>	
Information Checklist .....	4-1
Internet Access Configuration .....	4-2
Configuration for Single User Account .....	4-4
<b>Chapter 5</b>	
<b>Remote Node Configuration</b>	
Editing PPP Options .....	5-4
Bandwidth on Demand .....	5-6
<b>Chapter 6</b>	
<b>Dial-In Configuration</b>	
Default Dial-In Setup .....	6-1
Dial-In Users Setup .....	6-4
<b>Chapter 7</b>	
<b>TCP/IP Configuration</b>	
LAN-to-LAN Application .....	7-1
Remote Node Setup .....	7-2
Static Route Setup .....	7-4
<b>Chapter 8</b>	
<b>Filter Configuration</b>	
Router Filter Structure .....	8-2
Configuring a Filter Set .....	8-2
Configuring a Filter Rule .....	8-4
TCP/IP Filter Rule .....	8-4
Generic Filter Rule .....	8-7
Applying a Filter Set .....	8-8

Reducing Unnecessary Calls by Windows 95 .....	8-9
Diagnosing the Situation .....	8-9
Implementing the Filter .....	8-11
Applying the Filter .....	8-14

**Chapter 9**  
**System Maintenance**

System Status .....	9-1
Terminal Baud Rate .....	9-3
Log and Trace .....	9-4
View Error Log .....	9-4
Syslog and Accounting .....	9-4
Diagnostic Menu .....	9-6
ISDN Tools .....	9-6
TCP/IP Tools .....	9-7
System Tools .....	9-8
Back Up Configuration .....	9-8
Restore Configuration .....	9-8
Software Update .....	9-9
Command Interpreter Mode .....	9-9
Call Control .....	9-10
Blacklist .....	9-10
Budget Management .....	9-10
Call History .....	9-11
Call Control Parameters .....	9-11

**Chapter 10**  
**Troubleshooting**

Basic Functioning .....	10-1
LEDS .....	10-1
Test LED .....	10-2
LAN Link LED .....	10-2
Troubleshooting the ISDN Line .....	10-2
ISDN Initialization or Reset .....	10-3
ISDN Loopback Test .....	10-3



Troubleshooting a TCP/IP Network Using a Ping Utility .....	10-4
Testing the LAN Path to Your Router .....	10-4
Testing the Path from Your PC to a Remote Device .....	10-5
Troubleshooting a Remote Node or ISP Connection .....	10-5
Troubleshooting a Remote User Connection .....	10-6
Troubleshooting the Manager Interface .....	10-7
Testing the Phone Ports .....	10-7
Restoring the Default Configuration and Password .....	10-7

**Appendix A**  
**Technical Specifications**

General Specification .....	A-1
-----------------------------	-----

**Appendix B**  
**Ordering ISDN Lines**

Ordering the Line .....	B-1
Provisioning for Switches in North America .....	B-2
Provisioning for AT&T 5ESS Switch .....	B-2
Provisioning for Northern Telecom Switch .....	B-4

**Appendix C**  
**ISDN Clearing Codes**

Clearing Codes .....	C-1
----------------------	-----

**Appendix D**  
**Using the Protocol Analyzer and Trace Tools**

The Diagnostic Process .....	D-1
ISDN Protocol Analyzer .....	D-2
Packet Tracing .....	D-5
Packet Trace Display Format .....	D-8

**Glossary**

**Index**



# Figures

Figure 1-1.	Three Main Address Classes .....	1-8
Figure 1-2.	Example of Subnetting a Class B Address .....	1-10
Figure 1-3.	Single IP Address Operation Using NAT .....	1-13
Figure 2-1.	Front Panel of Model RT328 Router .....	2-4
Figure 2-2.	Front Panel of Model RH348 Router .....	2-4
Figure 2-3.	Rear Panel of the Model RT328 Router .....	2-6
Figure 2-4.	Rear Panel of the Model RH348 Router .....	2-6
Figure 3-1.	Start-up Display .....	3-2
Figure 3-2.	Manager Main Menu .....	3-4
Figure 3-3.	Menu 1 - General Setup .....	3-6
Figure 3-4.	Menu 2 - ISDN Setup for North America .....	3-8
Figure 3-5.	Menu 2 - ISDN Setup for DSS1 .....	3-10
Figure 7-1.	LAN-to-LAN Application .....	7-1
Figure 8-1.	Outgoing Packet Filtering Process .....	8-1
Figure 8-2.	LAN Packet Which Triggered Last Call .....	8-9
Figure 8-3.	Menu 21 Filter Set Configuration .....	8-11
Figure 8-4.	TCP/IP Filter Rule Menu .....	8-12
Figure 8-5.	Filter Rules Summary Menu .....	8-13
Figure 8-6.	Remote Node Profile Menu .....	8-14

Figure 9-1.	Packet Examples .....	9-3
Figure 9-2.	Trace Display for a Successful TCP/IP Protocol Connection .....	9-7
Figure 9-3.	Trace Display for a Failed TCP/IP Protocol Connection .....	9-7
Figure D-1.	ISDN Protocol Analyzer Display .....	D-4
Figure D-2.	Trace Screen .....	D-7
Figure D-3.	Packet Trace Display Definitions .....	D-8
Figure D-4.	PPP Message Definitions .....	D-8

# Tables

Table 1-1.	Netmask Notation Translation Table for One Octet .....	1-11
Table 1-2.	Netmask Formats .....	1-12
Table 2-1.	LED Descriptions .....	2-5
Table 3-1.	Manager Menu Commands .....	3-3
Table 3-2.	Manager Menu Summary .....	3-5
Table 3-3.	ISDN Setup Menu Parameters for North America .....	3-7
Table 3-4.	ISDN Setup Field Descriptions .....	3-9
Table 3-5.	Ethernet General Setup Menu Fields .....	3-11
Table 3-6.	Menu 3 - Ethernet Setup Menu Fields .....	3-12
Table 5-1.	Menu 11.1 Remote Node Profile Fields .....	5-2
Table 5-2.	Fields in Menu 11.2 - Remote Node PPP Options .....	5-5
Table 5-3.	Relationship Between BTR and MTR .....	5-6
Table 6-1.	Fields in Menu 13 - Default Dial-in Setup .....	6-2
Table 6-2.	Fields in Menu 14.1 - Edit Dial-in User .....	6-5
Table 7-1.	Fields in Menu 11.1 - Remote Node Profile Fields .....	7-2
Table 7-2.	Menu 11.3 Remote Node Network Layer Options Fields .....	7-3
Table 7-3.	Edit IP Static Route Menu Fields .....	7-5
Table 8-1.	Abbreviations Used in Menu 21.1 - Filter Rules Summary .....	8-3
Table 8-2.	Abbreviations Used if Filter Type Is IP .....	8-3
Table 8-3.	Abbreviations Used if Filter Type Is GEN .....	8-4
Table 8-4.	TCP/IP Filter Rule Menu Fields .....	8-5
Table 8-5.	Generic Filter Rule Menu Fields .....	8-7

Table 9-1.	System Maintenance Status Menu Fields .....	9-1
Table 9-2.	System Maintenance Status Menu Fields .....	9-2
Table 9-3.	System Maintenance - Log and Trace Menu Fields .....	9-4
Table 9-4.	System Maintenance - Syslog and Accounting Menu Fields .....	9-5
Table 9-5.	System Maintenance - Diagnostic Menu Fields .....	9-6
Table 10-1.	Code Numbers for Failed ISDN Initialization .....	10-3
Table B-1.	Switch Types Supported .....	B-2
Table B-2.	Provisioning Features and Settings for National ISDN-1 Services .....	B-3
Table B-3.	Provisioning Features and Settings for Multipoint Service .....	B-3
Table B-4.	Provisioning Features and Settings for Point-to-Point Service .....	B-4
Table B-5.	Provisioning Features and Settings for National ISDN-1 Service .....	B-5
Table B-6.	Provisioning Features and Settings for Custom ISDN Service .....	B-5
Table C-1.	ISDN Call Clearing Codes .....	C-1

# Preface

Congratulations on your purchase of the NETGEAR™ Model RT328 ISDN Router or Model RH348 ISDN Router.

These ISDN router models provide connection for one or more computer workstations to the Internet or to the office over Integrated Services Digital Network (ISDN) lines. They operate at a speed of up to 512 kilobits per second (Kbps) or 128 Kbps without compression. At these speeds, you can download video clips, music, or high-resolution color graphics from the World Wide Web or other online services many times faster than you can with an analog modem. The routers support concurrent data and voice communications, reducing cost and administration of multiple phone lines.

## Purpose

---

This guide describes the features of the Model RT328 router and the Model RH348 router and provides installation and configuration instructions. When discussing features, functions, or specifications that apply to both router models, the guide refers to the Model RT328/RH348 router.

## Audience

---

To configure and install the Model RT328/RH348 router, you should have the following background and experience:

- Working knowledge of basic network management concepts and terminology
- Working knowledge of tools and procedures for installing and operating sensitive electronic equipment





## Conventions

---

This section describes the conventions used in this guide.

### Special Message Formats

This guide uses the following formats to highlight special messages:

	<b>Note:</b> This format is used to highlight information of importance or special interest.
	<b>Caution:</b> This format is used to highlight information that will help you prevent equipment failure or loss of data.
	<b>Warning:</b> This format is used to highlight information about the possibility of injury or equipment damage.
	<b>Danger:</b> This format is used to alert you that you may incur an electrical shock by mishandling equipment.

### Use of Enter, Type, and Press

This guide uses “enter,” “type,” and “press” to describe the following actions:

- When you read “enter,” type the text and press the Enter key.
- When you read “type,” type the text, but do not press the Enter key.
- When you read “press,” press only the alphanumeric or named key.



## Other Conventions

This guide uses the following typographical conventions:

<i>italics</i>	Book titles and UNIX file, command, and directory names.
<code>courier font</code>	Screen text, user-typed command-line entries.
Initial Caps	Menu titles and window and button names.
[Enter]	Named keys in text are shown enclosed in square brackets. The notation [Enter] is used for the Enter key and the Return key.
[Ctrl]+C	Two or more keys that must be pressed simultaneously are shown in text linked with a plus (+) sign.
ALL CAPS	DOS file and directory names.

## Related Publications

---

For more information about configuring the Model RT328/RH348 router using FirstGear™ configuration software, refer to *Getting Started Using FirstGear for the Model RT328 and Model RH348 ISDN Routers* (part number M1-RH348NA-0).

For more information about address assignment, refer to RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*.

For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.



# Chapter 1

## Introduction

This chapter describes the features of the NETGEAR Model RT328 ISDN Router and Model RH348 ISDN Router and discusses planning considerations for installation.

### About the Router

---

The Model RT328/RH348 router transports data from one local area network (LAN) to another through a wide area network (WAN) connection.

The router compares the network addresses of data packets sent through the LAN to the entries in its address tables. If a match is found for a destination network, the router passes the packet to the path indicated by the entry in the routing table.

The entry in the path list contains the ISDN phone number(s) of the target router. The router sends the number to the ISDN port for the call to be connected. The WAN path is established, and the data is sent to the remote unit. At the receiving end, the process operates in the reverse order, from the ISDN port to the LAN port.

### Features

---

The Model RT328/RH348 router is a flexible, high-performance, easy-to-use router that provides a cost-effective solution for intelligent networking access across an ISDN line. With minimum setup, you can install and use the router within minutes to meet a wide variety of networking requirements.

## Key Features

The Model RT328/RH348 router provides the following features:

- Standard basic rate ISDN (BRI) connection
  - ISDN, 2B+D, providing two 64 Kbps data channels and a 16 Kbps control channel
  - Four-wire S/T interface on Model RT328-S/RH348-S router
  - Two-wire U interface on Model RT328-U/RH348-U router
  - Two-wire NTT interface on Model RH348-D router
- Protocol Support
  - IP routing
  - Multilink Point-to-Point Protocol (PPP) for 128 Kbps operation
  - Dynamic bandwidth-on-demand with BACP
  - Dynamic NAT+ for operation with a single static or dynamic IP address
  - DHCP for dynamically assigning network configuration information to LAN workstations
- Industry-standard compression
  - Hi/fn (Stac LZS) compression with CCP
- Easy installation and management
  - FirstGear graphical user interface (GUI) management software for Windows® users
  - Built-in Manager interface for Macintosh, UNIX, and PC users, accessible by terminal or Telnet Protocol
  - Configurable through the LAN—no serial connection required
- Security
  - Access control on management functions
  - Dial-in access control by Calling Line Identification (CLID) and Callback
  - PAP and CHAP authentication support

- Twisted pair and AUI Ethernet ports (Model RT328 router only)
  - RJ-45 interface allowing connection to a 10BASE-T network
  - AUI interface allowing connection to a coaxial or fiber network using a transceiver
- Four-port twisted pair Ethernet hub (Model RH348 router only)
  - Four RJ-45 interfaces for connection to 10BASE-T workstations
- Analog voice ports
  - Provides two RJ-11 interfaces
  - Allows a standard analog PSTN device (for example, telephone, fax, or modem) to make and receive calls from other ISDN or PSTN connected devices
  - Eliminates the need for a separate PSTN line in a SOHO (small office/home office) environment
- Eleven LEDs for easy monitoring of status and activity
- Flash EPROM for firmware upgrade
- Five-year warranty
- Free technical support seven days a week, twenty-four hours a day

## **ISDN Support**

The Model RT328/RH348 router is designed to take advantage of Integrated Services Digital Network (ISDN) for transmission of data over digital telephone networks. A basic rate interface (BRI), which is the usual ISDN implementation, consists of two 64 kilobit per second (Kbps) B channels for data and one 16 Kbps D channel for control information.

One advantage of using ISDN to connect routers is that the connection is set up only if there is data to be sent to the remote network. The router sets up a call, transfers the data, and then hangs up automatically when the connection is no longer needed.

## **Multilink PPP Support**

When the single-channel ISDN line utilization exceeds a configurable threshold, the router can automatically establish an additional ISDN call to provide additional bandwidth. During heavy traffic, the two 64 Kbps B channels are combined using Multilink PPP to provide a fast 128 Kbps pipe. When traffic slows down, one of the B channels is idled to save toll charges. The router also reverts back to one B channel for data when an analog port is used.

## **TCP/IP Support**

The Model RT328/RH348 router supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP), which ensures that ISDN connections are established only when passing data.

For further information about TCP/IP, refer to “Basic Router Concepts” on page 1-6.

### **IP Address Masquerading by Dynamic NAT+**

Both NETGEAR routers allow an entire department of networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, an extension of network address translation (NAT), is known as IP address masquerading and typically allows the use of a very inexpensive ISP account.

### **Automatic Configuration of Attached PCs by DHCP**

The routers can dynamically assign network configuration information, including IP, gateway, and domain name server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of LAN-attached workstations.

## **Security**

The Model RT328/RH348 router is equipped with several features designed to maintain security. These security features are described in this section.

### **Calling Line Identification**

The use of Calling Line Identification (CLID or Caller ID) ensures that incoming ISDN calling numbers are checked against known numbers before a call is answered and access is granted, thus providing a first level of security. In many areas, you must specifically request that CLID be enabled by the telephone company for your ISDN line. In some regions, CLID may not be available.

## **PAP and CHAP Authentication**

For connecting to other routers, the Model RT328/RH348 router supports two authentication protocols: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). PAP sends the user name and password in plain text. CHAP scrambles the password before it is sent over the wire. Although CHAP provides better security, PAP is readily available on more platforms.

## **Callback**

For security and simplified cost accounting, the router implements Callback. When a remote user dials in, the router can disconnect the call and call the user back, so that any further call charges are incurred by the location of the router. The caller can provide the callback numbers; or, for security, the router can be programmed to call back a predetermined number.

## **Management Support**

The router is designed to be installed and made operational within minutes after connection to the network.

If you are a PC user, the FirstGear software lets you easily configure the unit from the Windows environment.

If you are a Macintosh, UNIX, or PC user, you can connect to the built-in Manager interface, which can be accessed through a terminal connected to the MGR (manager) port or through a Telnet session across the network. The built-in Manager interface manages and configures the unit through an easily understood screen process.

## Basic Router Concepts

---

In general, the cost of providing network bandwidth is proportional to the data speed and the distance over which the network extends. Large amounts of bandwidth are provided easily and relatively inexpensively in a local area network (office, department, and similar situations). However, providing the same high data speeds between two local networks that are physically distant may be prohibitively expensive. Because of this expense, high-speed local area networks (LANs) are usually interconnected by slower-speed links to form a wide area network (WAN).

In order to make the best use of the slower WAN links, a mechanism must be in place at each location for selecting data meant only for another location and sending it by the best available link. The function of selecting and forwarding this data is performed by a router.

### What is a Router?

A router is a device that forwards traffic between networks based on network layer information in the data and on routing tables maintained by the router. In these routing tables, a router builds up a logical picture of the overall network by gathering and exchanging information with other routers in the network. Using this information, it chooses the best path for forwarding network traffic.

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connections supported. The Model RT328/RH348 router is a small office router that routes the IP protocol over a dial-up ISDN connection.

### Routing Information Protocol

One of the protocols used by a router to build and maintain a picture of the network is the Routing Information Protocol (RIP). RIP is a distance vector protocol, meaning that all the decisions about which path to use are based upon a logical distance between source and destination networks. This distance is measured in “hops,” meaning the number of relaying routers in the path between the source LAN router and the router of the destination LAN. For example, the LAN of router A is considered to be 1 hop away. If router A can reach the network of router B by a direct WAN link to the network of router B, the network of router B is two hops away. If another network must be reached by calling router B and having router B forward the data, that network is n hops away, where n is the number of routers traversed by the data to get to the network farthest away. When there are multiple paths to a network, the path with the fewest number of hops is chosen and is regarded as the best path, and all other information about how to get to that network is discarded.



Using RIP, routers update one another periodically and check to see if there are any changes to be added to the routing table. An important consideration is the convergence time, or how long it takes for a change to the routing topology (such as a new node or a node failure), to be propagated throughout the entire RIP environment. To prevent this convergence process from being excessively long, RIP is limited to 15 hops maximum.

The Model RT328/RH348 router supports both the older RIP-1 and the newer RIP-2 protocols. Among other improvements, RIP-2 supports subnetting and multicasting.

## **IP Addresses and the Internet**

Because TCP/IP networks are interconnected widely across the world, every machine on the Internet must have a unique address to make sure that transmitted data reaches the correct destination. Blocks of addresses are assigned to organizations by the Internet Assigned Numbers Authority (IANA). Individual users and small organizations may obtain their addresses either from the IANA or from an Internet service provider (ISP).

The Internet Protocol (IP) uses a 32-bit address structure. The address is usually written in dot notation (also called dotted-decimal notation), in which each group of eight bits is written in decimal form, separated by decimal points. For example, the binary address:

```
11000011 00100010 00001100 00000111
```

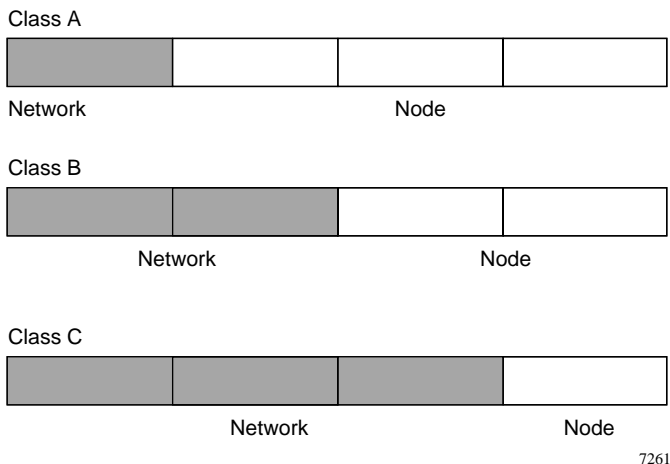
is normally written as:

```
195.34.12.7
```

which is easier to remember and easier to enter into your computer.

In addition, the 32 bits of the address are subdivided into two parts. The first part of the address identifies the network, and the second part identifies the host node or station on the network. The dividing point may vary depending on the address range and the application.

There are five standard classes of IP addresses. These address classes have different ways of determining the network and host sections of the address, allowing for different numbers of hosts on a network. Each address type begins with a unique bit pattern, which is used by the TCP/IP software to identify the address class. After the address class has been determined, the software can correctly identify the host section of the address. The three main address classes are illustrated in Figure 1-1, which shows the network and host sections of the address for each address type.



**Figure 1-1. Three Main Address Classes**

Class A addresses can have up to 16,777,214 hosts on a single network. They use an 8-bit network number and a 24-bit node number. Class A addresses are in this range:

1.x.x.x to 126.x.x.x.

Class B addresses can have up to 65,354 hosts on a network. A Class B address uses a 16-bit network number and a 16-bit node number. Class B addresses are in this range:

128.1.x.x to 191.254.x.x.

Class C addresses can have 254 hosts on a network. Class C addresses use 24 bits for the network address and 8 bits for the node. They are in this range:

192.0.1.x to 223.255.254.x.

Class D addresses are used for multicasts (messages sent to many hosts). Class D addresses are in this range:

224.0.0.0 to 239.255.255.255.

Class E addresses are for experimental use.

This addressing structure allows IP to uniquely identify each physical network and each node on each physical network.

For each unique value of the network portion of the address, the base address of the range (host address of all zeros) is known as the network address and is not usually assigned to a host. Also, the top address of the range (host address of all ones) is not assigned but is used as the broadcast address for sending a packet simultaneously to all hosts with the same network address.

## Netmask

In each of the above address classes, the size of the two parts (network address and host address) is implied by the class. This partitioning scheme can also be expressed by a netmask associated with the IP address. A netmask is a 32-bit quantity that, when logically ANDed with an IP address, yields the network address. For instance, the netmasks for Class A, B, and C addresses are 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.

For example, the address 192.168.170.237 is a Class C IP address whose network portion is the upper 24 bits. When ANDed with the Class C netmask, as shown here, only the network portion of the address remains:

```
11000000 10101000 10101010 11101101 (192.168.170.237)
```

ANDed with:

```
11111111 11111111 11111111 00000000 (255.255.255.0)
```

Equals:

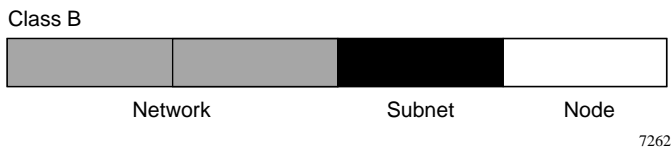
```
11000000 10101000 10101010 00000000 (192.168.170.0)
```

As a shorter alternative to dotted-decimal notation, the netmask may also be expressed in terms of the number of ones from the left. This number is appended to the IP address, following a backward slash (/), as “/n.” In the example, the address could be written as 192.168.170.237/24, indicating that the netmask is 24 ones followed by 8 zeros.

## Subnet Addressing

By looking at the addressing structures, you can see that even with a Class C address, there are a large number of hosts per network. Such a structure is an inefficient use of addresses if each end of a routed link requires a different network number. It is unlikely that the smaller office LANs would have that many devices. You can resolve this problem by using a technique known as subnet addressing.

Subnet addressing allows us to split one IP network address into smaller multiple physical networks known as subnetworks. Some of the node numbers are used as a subnet number instead. A Class B address gives us 16 bits of node numbers translating to 64,000 nodes. Most organizations do not use 64,000 nodes, so there are free bits that can be reassigned. Subnet addressing makes use of those bits that are free, as illustrated in Figure 1-2.



**Figure 1-2. Example of Subnetting a Class B Address**

A Class B address can be effectively translated into multiple Class C addresses. For example, the IP address of 172.16.0.0 is assigned, but node addresses are limited to 255 maximum, allowing 8 extra bits to use as a subnet address. The IP address of 172.16.97.235 would be interpreted as IP network address 172.16, subnet number 97, and node number 235. In addition to extending the number of addresses available, subnet addressing provides other benefits. Subnet addressing allows a network manager to construct an address scheme for the network by using different subnets for other geographical locations in the network or for other departments in the organization.

Although the preceding example uses the entire third octet for a subnet address, note that you are not restricted to octet boundaries in subnetting. To create more network numbers, you need only shift some bits from the host address to the network address. For instance, to partition a Class C network number (192.68.135.0) into two, you shift 1 bit from the host address to the network address. The new netmask (or subnet mask) is 255.255.255.128. The first subnet has network number 192.68.135.0 with hosts 192.68.135.1 to 129.68.135.126, and the second subnet has network number 192.68.135.128 with hosts 192.68.135.129 to 192.68.135.254.



**Note:** The number 192.68.135.127 is not assigned because it is the broadcast address of the first subnet. And 192.68.135.128 is not assigned because it is the network address of the second subnet.

Table 1-1 lists the additional subnet mask bits in dotted-decimal notation. To use the table, write down the original class netmask and replace the 0 value octets with the dotted-decimal value 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 1-1. Netmask Notation Translation Table for One Octet**

Number of Bits	Dotted-Decimal Value
1	128
2	192
3	224
4	240
5	248
6	252
7	254
8	255

Table 1-2 displays several common netmask values in both the dotted-decimal and the masklength formats.

**Table 1-2. Netmask Formats**

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31
255.255.255.254	/32

NETGEAR strongly advises that all hosts on a LAN segment use the same netmask for the following reasons:

- So that hosts recognize local IP broadcast packets  
When a device broadcasts to its segment neighbors, it uses a destination address of the local network address with all ones for the host address. In order for this scheme to work, all devices on the segment must agree on which bits comprise the host address.
- So that a local router or bridge will know which addresses are local and which are remote

## Private IP Addresses

If your networks are isolated from the Internet (for example, only between your two branch offices), you can assign any IP addresses to the hosts without problems. However, the IANA has reserved the following three blocks of IP addresses specifically for private networks:

10.0.0.0 - 10.255.255.255  
172.16.0.0 - 172.31.255.255  
192.168.0.0 - 192.168.255.255

NETGEAR recommends that you choose your private network number from this list.

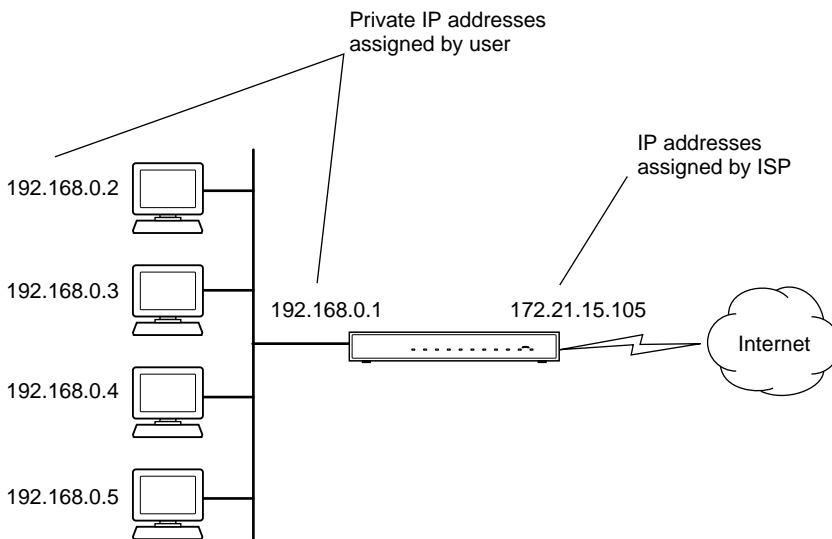
Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines explained here. For more information about address assignment, refer to RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*.

## Single IP Address Operation Using NAT

If multiple stations on a LAN need to access the Internet simultaneously, they usually have to obtain a range of IP addresses from the ISP. This type of Internet account is much more costly than a single-address account typically used by a single user with a terminal adapter rather than a router. The Model RT328/RH348 router employs a method called extended NAT. This method allows an entire department of networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP).

The router accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. The internal LAN IP addresses can be either private addresses or registered addresses. For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

Figure 1-3 illustrates a single IP address operation.



7786EA

**Figure 1-3. Single IP Address Operation Using NAT**

This scheme offers the additional benefit of firewall protection because the internal LAN addresses are not available to the Internet through the translated connection. All incoming inquiries are filtered out by the router. This filtering can prevent intruders from probing your system. You can specify one server (for example, a Web server) on your local network and make it accessible by outside users.

## **Address Resolution Protocol**

An IP address alone cannot be used to deliver data from one device to another on a LAN. In order for data to be sent from one device on the LAN to another, you must convert the IP address of the destination device to its media access control (MAC) address. Each device on an Ethernet network has a unique Ethernet MAC address, which is a 48-bit number assigned to each device by the manufacturer. The technique that associates the IP address with a MAC address is known as address resolution, and IP uses the Address Resolution Protocol (ARP) to do this.

If a device needs to send data to another station on the network and it does not already have the destination MAC address recorded, ARP is used. An ARP request is broadcast onto the network, and all stations receive and read the request. The destination IP address for the chosen station is included as part of the message so that only the station with this IP address responds to the ARP request and all other nodes discard it.

The node with the right IP address responds with its own MAC address directly to the sender, providing the transmitting station with the destination MAC address needed for it to send the data. The IP address data and MAC address data for each node are held in an ARP table, so that the next time data needs to be sent, the address can be obtained from the address information in the table.

## **Domain Name Server**

Many of the resources on the Internet can be addressed by simple descriptive names such as [www.NETGEAR.com](http://www.NETGEAR.com). This addressing is very helpful at the application level, but the descriptive name must be translated to an IP address in order for a user to actually contact the resource. Just as each workstation maintains an ARP table to map IP addresses to MAC addresses, a domain name server (DNS) maps descriptive names of network resources to IP addresses.

When a workstation needs to access a resource by its descriptive name, it first contacts a DNS to obtain the IP address of the resource. It can then send the desired message using the IP address. Many large organizations such as ISPs maintain their own DNSs and allow their customers to use them for address lookup.



## **IP Configuration by DHCP**

When an IP-based local area network is installed, each workstation must be configured with an IP address. If the workstations need to access the Internet, they should also be configured with a gateway address and one or more DNS server addresses. As an alternative to manual configuration, there is a method by which each device on the network can obtain this configuration information automatically. A device on the network may act as a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server stores a list or pool of IP addresses, along with other information (such as gateway and DNS addresses) that it may assign to the other devices on the network. The Model RT328/RH348 router has the capacity to act as a DHCP server.



# Chapter 2

## Router Installation and Connection

This chapter provides instructions for installing the Model RT328/RH348 router and connecting to the built-in interface through a serial or Telnet connection.

### Package Contents

---

The product package should contain the following items:

- Model RT328 router or Model RH348 router
- AC power adapter, 16 V AC output
- 10-foot 10BASE-T Ethernet cable, straight-through wiring (white)
- 10-foot 10BASE-T Ethernet cable, crossover wiring (red) for the Model RT328 router only
- ISDN cable (black)
- 9-pin RS-232 serial cable
- 9-pin D-connector to 25-pin D-connector adapter
- This guide
- *Getting Started Using FirstGear for the Model RT328 and Model RH348 ISDN Routers*
- FirstGear Installation Diskette
- Warranty card

Call your dealer if there are any wrong, missing, or damaged parts. Keep the carton, including the original packing materials, to repack the router if there is a need to return it for repair.

## ISDN Services Checklist

---

The following requirements must be met in order to successfully connect to the ISDN network:

- European Services
  - Your ISDN circuit should conform to DSS1, EURO-ISDN, NET3, or I-CTR3 standards.
  - You should know the ISDN number(s) of your local and remote sites.
  - If you require CLID (Calling Line Identification) for security, order the CLID option from your local carrier.
- North American Services

The Model RT328/RH348 router has been approved by Bellcore and has the IOC (ISDN Ordering Code) “S” Capability, EZ-ISDN1. Ordering your ISDN line in this configuration will provide basic data and voice service. If you wish to use any advanced calling features such as call waiting, you will need to order a higher level of service such as IOC “U.” In particular, you will need to have ACO (Additional Call Offering) provisioned in order to use call waiting or incoming call bumping.

In North America, you must configure your ISDN router according to the type of switch your telephone company has in its local central office. For further information, refer to Appendix B, “Ordering ISDN Lines.”

You need the following information from your telephone company:

- The type of switch at your telephone company

This switch type may be AT&T 5ESS, Northern Telecom DMS-100/DMS-250, or Siemens EWSD.
- The configuration mode of your ISDN line

Your line may be configured in the standard National ISDN mode (NI-1) or in a manufacturer-specific custom mode.
- The local directory number(s) assigned to your line
- The Service Profile Identifiers (SPIDs) associated with the directory numbers

## **Network Checklist**

---

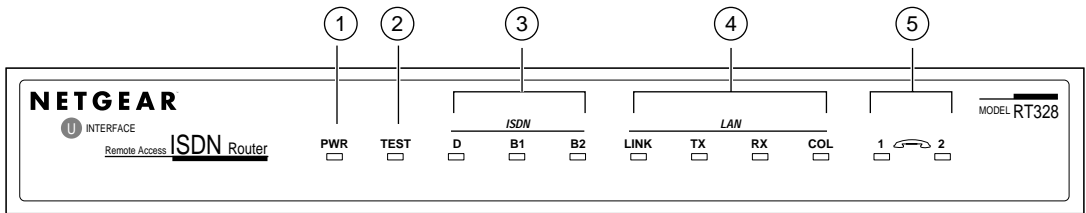
The Model RT328/RH348 router uses the Internet Protocol (IP). The IP configuration has the following requirements:

- Host devices must have established IP addresses (usually defined by your network manager or Internet service provider).
- An IP address must be assigned to the router itself (usually defined by your network manager or Internet service provider).
- Host devices must have the router defined either as the default gateway or as an entry in the static routes table.
- The network or subnetwork numbers must be different on the Local and Remote networks you are routing between.

If you do not have any assigned IP addresses, you must use NAT. In this case, assign IP addresses from a group of designated private IP addresses. Refer to “Single IP Address Operation Using NAT” on page 1-13 for more information about IP address masquerading. Refer to “IP Addresses and the Internet” on page 1-7 for more information about TCP/IP network configuration.

## Connecting the Router

The front panels of the Model RT328 router, as illustrated in Figure 2-1, and the Model RH348 router, as illustrated in Figure 2-2, contain status LEDs. Refer to the illustrations to locate the LEDs and to Table 2-1 for descriptions. You can use some of the LEDs to verify connections.

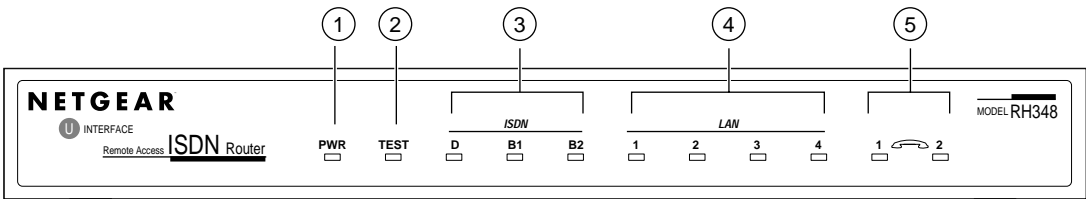


7631EA

Key:

- 1 = PWR (Power) LED
- 2 = TEST LED
- 3 = Channel D, B1, and B2 ISDN LEDs
- 4 = LINK, TX, RX, and COL LAN LEDs
- 5 = PHONE 1 and PHONE 2 LEDs

**Figure 2-1. Front Panel of Model RT328 Router**



8349EA

Key:

- 1 = PWR (Power) LED
- 2 = TEST LED
- 3 = Channel D, B1, and B2 ISDN LEDs
- 4 = LAN 1-4 LEDs
- 5 = PHONE 1 and PHONE 2 LEDs

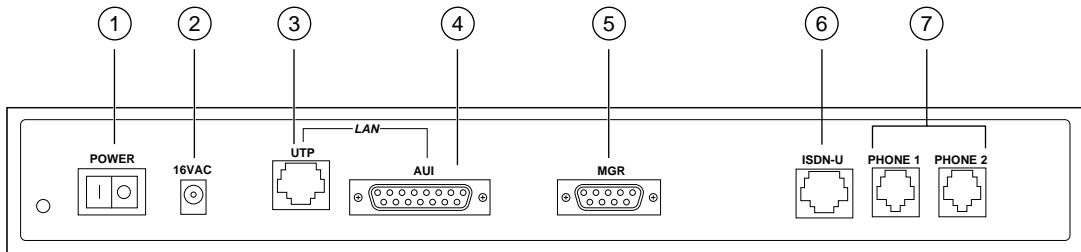
**Figure 2-2. Front Panel of Model RH348 Router**

Table 2-1 lists and describes each LED on the front panel of the router. These LEDs are green when lit.

**Table 2-1. LED Descriptions**

Label	Activity	Description
PWR (Power)	On	Power is supplied to the router.
TEST	Blinking	The router is functioning properly.
ISDN:		
D	On	The router is successfully synchronized with the attached ISDN line.
B1	On	There is an active WAN session on the channel, or the channel is making or receiving a call.
B2	On	There is an active WAN session on the channel, or the channel is making or receiving a call.
LAN (RT328):		
Link	On	This LAN port is synchronized with an attached device.
TX (Transmit)	Blinking	Data is being transmitted on the LAN.
RX (Receive)	Blinking	Data is being received on the LAN.
COL (Collision)	Blinking	Data collision is occurring on the LAN.
LAN (RH348):		
1-4	On	The numbered LAN port is synchronized with an attached device.
	Blinking	Data is being received on the port.
Phone 1	On	The device (telephone, fax, or modem) connected to the PHONE 1 port is in use.
Phone 2	On	The device (telephone, fax, or modem) connected to the PHONE 2 port is in use.

The rear panel of the Model RT328 router is shown in Figure 2-3, and the rear panel of the Model RH348 router is shown in Figure 2-4. Refer to this diagram to identify all of the ports on the router when you attempt to make any connections.

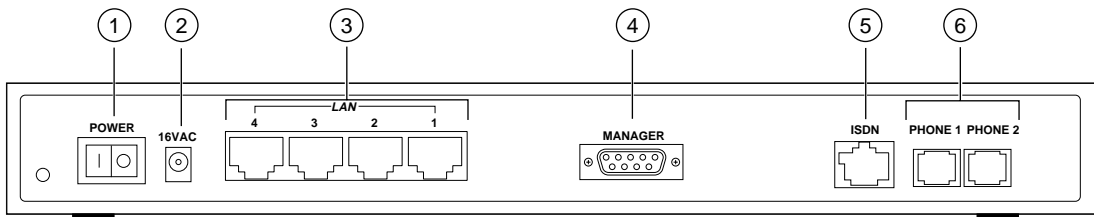


7632EA

Key:

- 1 = Power switch
- 2 = AC adapter outlet for connecting the AC adapter to the router
- 3 = UTP port for connecting the router to the LAN with UTP cable
- 4 = AUI port for connecting the router to the LAN with coaxial or fiber cable using a transceiver
- 5 = RS-232 port for connecting the router to the serial port of a PC
- 6 = ISDN port for connecting the router to ISDN cable
- 7 = Phone ports for connecting the router to a telephone, fax, or modem

**Figure 2-3. Rear Panel of the Model RT328 Router**



8343EA

Key:

- 1 = Power switch
- 2 = AC adapter outlet for connecting the AC adapter to the router
- 3 = UTP hub ports for connecting PCs and workstations
- 4 = RS-232 port for connecting the router to the serial port of a PC
- 5 = ISDN port for connecting the router to ISDN cable
- 6 = Phone ports for connecting the router to a telephone, fax, or modem

**Figure 2-4. Rear Panel of the Model RH348 Router**





**Warning:** Several of the connectors and connection cables are very similar. It is important that you use the correct cable for each connection and that you do not connect the ports incorrectly, because serious damage to your router could result.

## Connecting the Serial Cable (Optional)

Plug one end of the 9-pin RS-232 cable into the MGR (manager) port on the router. Plug the other end into a serial port (such as COM1 or COM2) of your PC. You must use the included 9-pin to 25-pin adapter if your PC has only a 25-pin port available.

## Connecting to the ISDN Port

In regions where the S interface version of the router is used, the ISDN cable will have two 8-pin RJ-45 connectors. Plug one end of the cable into the ISDN port of the router and connect the other end to an NT1 (Network Termination) device, a DSU device, or an S-interface wall jack.

In regions where the U interface version of the router is used, your ISDN cable will have an 8-pin RJ-45 connector on one end and either an 8-pin RJ-45 (earlier versions) or a 6-pin RJ-11 (later versions) connector on the other end. Plug one 8-pin connector into the ISDN port of the router. Connect the other end of the cable directly to your ISDN wall jack. Your wall jack may have either an 8-pin RJ-45 or a 6-pin RJ-11 connector. A 6-pin cable connector will plug into the center of an 8-pin wall jack, but if you have a 6-pin jack and an 8-pin cable connector, you must either change the jack or get a cable with two 6-pin connectors.

## Connecting the Ethernet Cable

The Model RT328 router supports two types of Ethernet connections. Follow the procedure that is appropriate for your installation.

## Using Twisted Pair LAN Cabling

Use the UTP port for connecting your router to a 10BASE-T network, using unshielded twisted pair (UTP) cabling and RJ-45 connectors. The following two types of UTP cable are included with your router:

- Straight-through Ethernet cable  
Use the white straight-through cable to connect your router to an Ethernet hub.
- Crossover Ethernet cable  
Use the red crossover Ethernet cable to connect your router to a PC or workstation.

## Using Coaxial or Fiber LAN Cabling

Use the AUI port for connecting to a transceiver, which provides an interface to coaxial or fiber Ethernet networks.

## Connecting to the Hub Ports in the Model RH348 Router

The Model RH348 router provides four Ethernet twisted pair hub ports for connecting to PCs and workstations. Connections are made using standard straight-through UTP cables like the one included with your router. The hub of the Model RH348 router may be connected to another hub using the uplink port on the hub to which you are connecting or by using a crossover cable to a normal port.

## Connecting a Telephone, Fax, or Modem

Use either one of the phone ports (PHONE 1 or PHONE 2) for connecting your router to an analog telephone, fax, or modem. Be sure that your ISDN line is provisioned by your telephone company for both data and voice calls.

## Connecting the Power Adapter

Plug the connector of the 16 V AC power adapter into the AC adapter outlet on the router. Then plug the adapter into a wall outlet.

## Connecting for Configuration

---

If you are a PC user, you can configure the router through either the FirstGear ISDN Router Configuration Utility, which is an easy-to-use software program, or the menu-based built-in Manager interface. For complete instructions on using FirstGear, refer to *Getting Started Using FirstGear for the Model RT328 and Model RH348 ISDN Routers*.

If you are using a Macintosh or UNIX-based workstation, you can configure the router only by using the built-in Manager interface.

You can access the built-in Manager interface through either a serial port or Telnet on the LAN. In order to use Telnet, you must know the current IP address of the router. For more information about using the built-in Manager interface, refer to Chapter 3, "Router Configuration."

## Connecting Through a Serial Port

You can access the built-in interface through a serial port by using a VT100 terminal or by using a terminal-emulation program on your PC or workstation. If you are using Windows, for example, Microsoft® provides HyperTerminal with Windows 95. Be sure to set the program for VT100 emulation, including arrow keys.

Serial port parameters are as follows:

- 9600 bps
- 8 data bits
- 1 stop bit
- No parity
- No flow control

After the serial session is opened, refer to Chapter 3, "Router Configuration," for further information about the different methods of configuring your router and for configuration instructions.

## Connecting Through a Telnet Connection

You can access the built-in interface by a Telnet call from any TCP/IP workstation on the LAN or the remote network. In order to use the Telnet Protocol, you must know the current IP address of the router. If the router has no IP address, you must first use a serial connection or the FirstGear utility to assign an IP address. The router ships with an address of 192.168.0.1.

To make a Telnet connection from the LAN, you must know which of the two LAN interfaces (UTP or AUI) is enabled and make sure that the interface is connected to the LAN. The factory default is the UTP interface. You must also set up your workstation to be able to reach the IP address of the router by doing one of the following:

- Set your workstation to an IP address on the currently programmed subnet of the router.
- Add a route to the static routing table of the workstation to indicate that the router can be reached through the local LAN port.



**Note:** If you change the LAN IP address of the router while connected through Telnet, you lose the Telnet session. You must then open a new Telnet connection to the new IP address and log in again. If you change the selected LAN interface, you also lose the session and must change the hardware connection to the other Ethernet port.

When using Telnet, consider the following:

- Single administrator

To prevent confusion and discrepancy on the configuration, the router allows only one terminal connection at any time. The router also gives priority to the RS-232 connection over Telnet. If you have already connected to the router through Telnet, you will be logged out if another user then connects through the RS-232 cable. You can use a Telnet connection only after the other administrator has disconnected.

- System timeout

When you are connected to the router through 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 the router automatically disconnects you.

# Chapter 3

## Router Configuration

This chapter contains information about configuring your Model RT328/RH348 router through the built-in Manager interface.

### Configuration Methods

---

If you are using a PC, you have the following two options to configure your router:

- Through FirstGear

FirstGear is an easy-to-use Windows-based utility that leads you through a Quick Setup or an Advanced menu for configuring your router. For FirstGear instructions, refer to *Getting Started Using FirstGear for the Model RT328 and Model RH348 ISDN Routers*.

- Through the built-in Manager interface

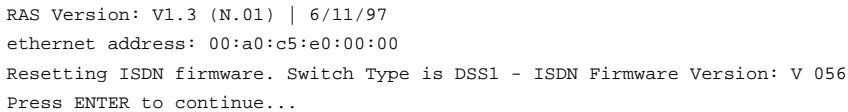
If you are using a Macintosh or UNIX-based workstation, the built-in Manager interface is the only way that you can configure your router through your computer. However, you can use a PC to configure the router and then connect the router to the Macintosh or workstation after the configuration process is complete.

The built-in Manager interface is accessible through either a serial or a Telnet connection (refer to “Connecting Through a Serial Port” or “Connecting Through a Telnet Connection” on page 2-9, respectively, of Chapter 2, “Router Installation and Connection”). If the router has not previously been assigned an IP address, you cannot connect through a Telnet session. You must use a serial connection.

## Powering on the Router

---

When you turn power on to the router, several internal tests are performed by the router and your ISDN line is initialized. After the initialization, the start-up display appears, as illustrated in Figure 3-1.

The start-up display is shown within a rounded rectangular border. It contains the following text:

```
RAS Version: V1.3 (N.01) | 6/11/97
ethernet address: 00:a0:c5:e0:00:00
Resetting ISDN firmware. Switch Type is DSS1 - ISDN Firmware Version: V 056
Press ENTER to continue...
```

**Figure 3-1. Start-up Display**

To continue:

**1. Press [Enter] when prompted.**

A login screen is displayed and prompts you to enter a password.

**2. Enter the default password 1234 to reach the main menu of the Manager.**

Once you are in the Manager and if there is no activity for longer than 5 minutes, the router automatically logs you out and displays a blank screen. If you see a blank screen, press [Enter] to display the password screen again.

---

## Navigating the Manager

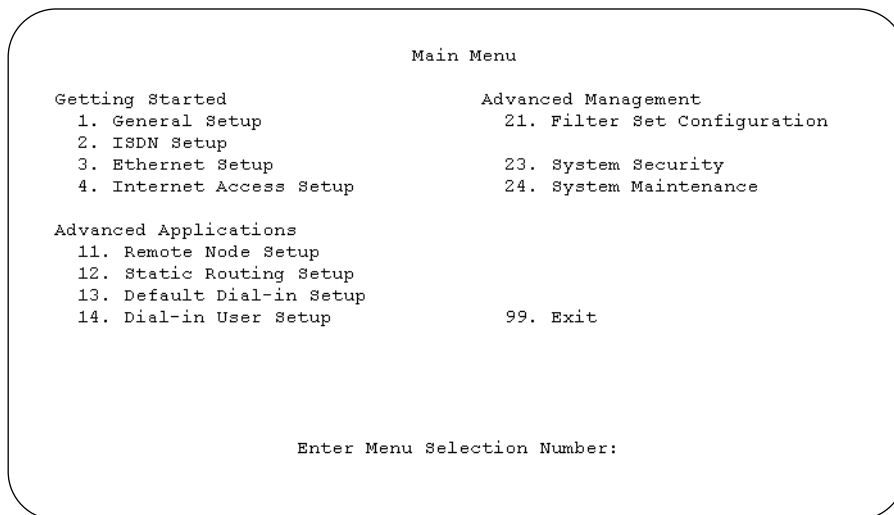
---

The Manager is the interface that you use to configure your router. Table 3-1 lists and describes the commands that enable you to navigate through the menus in the Manager.

**Table 3-1. Manager Menu Commands**

Action	Description
Move forward to another menu	Enter the number of the submenu and press [Enter].
Move back to a previous menu	Press [Esc]. The only exception is the Main Menu, where typing 99 is the only method to exit from the Manager.
Move the cursor	Press [Enter]. You can also use the Up and Down keys to move to the previous and the next field, respectively.
Enter information	There are two types of fields for entering selected parameters. The first requires you to enter the appropriate information. The second gives you options to choose from. When choosing options, press the space bar to toggle through the available options.
Required fields	Some of the fields in the Manager are essential in order to configure the router. The required fields initially show a question mark (?), indicating that the information must be filled in before that menu can be saved.
N/A fields	Some of the fields in the Manager show N/A, meaning the option is not available.
Save your configuration	Press [Enter] when prompted to press ENTER to confirm or ESC to cancel. In most cases, saving the data on the screen takes you to the previous menu.

The Manager Main Menu is illustrated in Figure 3-2.



**Figure 3-2. Manager Main Menu**



## Manager Menu Summary

Table 3-2 describes the top-level Manager menus.

**Table 3-2. Manager Menu Summary**

Number	Menu Title	Description
1	General Setup	This menu is accessed to set up general information and enable specific protocol routing or bridging.
2	ISDN Setup	This menu is accessed to set up ISDN configurations.
3	Ethernet Setup	This menu is accessed to set up Ethernet configurations.
4	Internet Access Setup	This menu provides a quick and easy way to set up an Internet connection.
11	Remote Node Setup	This menu is accessed to set up a remote node for a LAN-to-LAN connection including Internet connection. The router has four remote nodes.
12	Static Routing Setup	This menu is accessed to set up static routes. The router supports four static routes for each protocol.
13	Default Dial-in Setup	This menu is accessed to set up default dial-in parameters so that your router can be a dial-in server for the remote node and remote dial-in user.
14	Dial-in User Setup	This menu is accessed to set up remote dial-in users. The router has eight remote dial-in users.
21	Filter Set Configuration	This menu is accessed to set up filters to be used in Menu 3 and Menu 11 to provide such features as security and call control.
23	System Security	This menu is accessed to set up security-related parameters.
24	System Maintenance	This menu is accessed to provide system status, diagnostics, and firmware upload.
99	Exit	This menu is accessed to exit from the Manager.

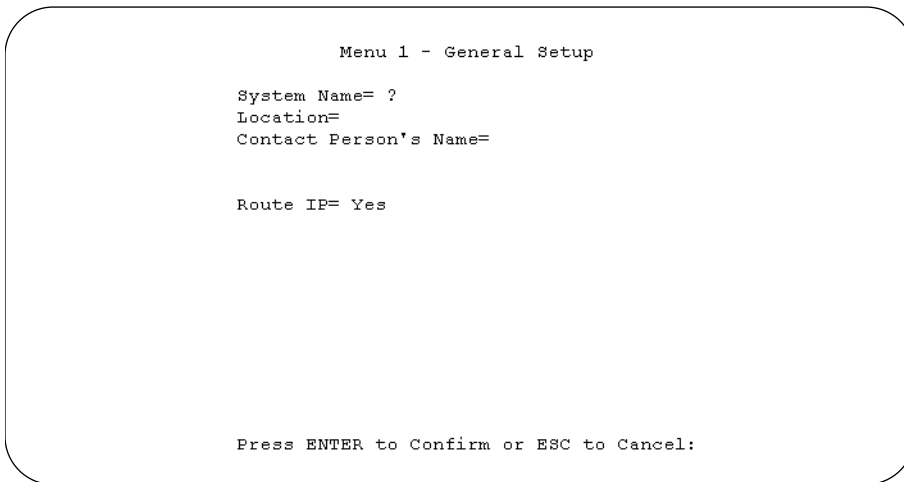
## General Setup Menu

---

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

To enter administrative and system-related information:

1. Enter 1 from the Main Menu to display Menu 1 - General Setup, as illustrated in Figure 3-3.



**Figure 3-3. Menu 1 - General Setup**

2. Enter the system name in the System Name field of the menu.

For identification purposes, choose a descriptive name for the router, such as RT328 or RH348. The name should be no more than 8 alphanumeric characters. Spaces are not allowed, but dashes ( - ) and underscores ( \_ ) are accepted. The name can be used for CHAP authentication and is displayed as the prompt in the Command Mode.

## ISDN Menus

Menu 2 is for configuring your ISDN line. Depending on what switch the telephone company has for your particular installation, you may have more than one telephone number. If you are in North America, you may also have SPIDs (Service Profile Identifiers). Make sure that you have correct and complete telephone numbers and SPIDs. You must complete the ISDN setup before your system can make an outgoing call or answer an incoming call.

### North American ISDN Menu

Use the commands described in Table 3-1 and Table 3-2 to display the ISDN Setup menu for North America. Table 3-3 lists and describes each field in the menu and how to enter the information in each field.

**Table 3-3. ISDN Setup Menu Parameters for North America**

Field	Description
Switch Type	Verify the switch type information with your telephone company. For North America, select the type of switch used by your telephone company. Press the space bar to cycle through the choices, and then press [Enter]. If your line is configured for National ISDN (NI-1) Protocol, choose the NI-1 setting. Otherwise, choose Custom.
B Channel Usage	Switch/Switch should be selected unless one or both B channels are a leased circuit. Toggling this parameter using the Space bar will cycle through all combinations of Switch, Leased, and Unused.
Telephone Number(s)	Enter the telephone number(s) assigned to your ISDN line by your telephone company. For North America, these phone numbers should be in a standard seven-digit local format without area code (for example, 5551212). The router accepts only digits. Do not include dashes ( - ) and spaces in this field. This field should be no longer than 19 digits.
SPID Number(s)	SPID (Service Profile Identifier) is a number used by a switch for identification purposes. Depending on your switch type, you may have zero, one, or two SPIDs assigned to your line.
Analog Call	This field tells the router how to route an incoming analog call. Set to Phone 1 if you want to route the incoming analog call for this telephone number to the PHONE 1 port (POTS port in North America and A/B Adapter in Europe). Set to Phone 2 if you want to route the incoming analog call for this telephone number to the PHONE 2 port. Set to DOVBS if you want to receive an incoming data over voice bearer service call.

Figure 3-4 shows Menu 2 - ISDN Setup for North America.

```
Menu 2 - ISDN Setup

Switch Type= AT&T 5ESS NI-1

B Channel Usage= Switch/Switch
1st Phone #= ?
  SPID #= ?
  Analog Call= Phone 1
2nd Phone #=
  SPID #=
  Analog Call= Phone 2

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

**Figure 3-4. Menu 2 - ISDN Setup for North America**

## DSS1 ISDN Menu

Use the commands described in Table 3-1 and Table 3-2 to display Menu 2 - ISDN Setup for DSS1. When you finish entering the information for all the fields, do the following on both menus:

- Press [Enter] at the Press ENTER to Confirm prompt to save your selections.
- or
- Press [Esc] to cancel.

When you press [Enter], the router uses the information that you enter to initialize the ISDN link to the telephone company switch.

The router asks if you want to test whether or not your ISDN line has been successfully connected to your router. When you select Yes, the router performs a loopback test to check the ISDN line. If the loopback test fails, note the error message that you receive and take the appropriate troubleshooting action. Refer to Chapter 10 for troubleshooting information.

Table 3-4 lists and describes the fields and field descriptions for Menu 2 - ISDN Setup.

**Table 3-4. ISDN Setup Field Descriptions**

Field	Description
Switch Type	This field is fixed as DSS1.
B Channel Usage	Switch/switch should be selected unless one or both B channels are a leased circuit. Toggling this parameter using the Space bar will cycle through all combinations of Switch, Leased, and Unused.
ISDN Data and Subaddress	Enter the telephone number and subaddress assigned to the ISDN data call for the router. It is used as the outgoing CGPN (Calling Party Number) setting for the ISDN data call. The router accepts only digits. Do not include dashes ( - ) and spaces in this field. This field should be no longer than 19 digits for the number and 5 digits for the subaddress.
A/B Adapter 1 and Subaddress	Enter the telephone number and subaddress assigned to the A/B Adapter 1 (POTS port 1) call for the router. It is used as the outgoing CGPN (Calling Party Number) setting for the A/B Adapter 1 call.
A/B Adapter 2 and Subaddress	Enter the telephone number and subaddress assigned to the A/B Adapter 2 (POTS port 2) call for the router. It is used as the outgoing CGPN (Calling Party Number) setting for the A/B Adapter 2 call.
Dial Prefix to Access Outside Line	Enter the prefix number if the router is connected to an ISDN PABX. This number is added to all outgoing calls and should be no longer than 4 digits. If the router is not connected to an ISDN PABX, leave this field blank.
PABX Number (with S/T Bus Number)	Enter the S/T bus number if the router is connected to an ISDN PABX. If this field is left blank, the loopback test is skipped.
Incoming Phone Number Matching	There are three options in this field: <ul style="list-style-type: none"> <li>• Multiple Subscriber Number (MSN): The digital call is answered only when there is a match for the ISDN data number. The analog call is answered as the A/B Adapter 1 call when there is a match for the A/B Adapter 1 number. It is answered as the A/B Adapter 2 call when there is a match for the A/B Adapter 2 number. If an A/B Adapter 1 or 2 number is not specified, the analog call is not answered.</li> <li>• Called Party Sub-Address (CDSA): The digital call is answered when there is a match for the ISDN Data subaddress. The analog call is answered as the A/B Adapter 1 call when there is a match for the A/B Adapter 1 subaddress. The analog call is answered as the A/B Adapter 2 call when there is a match for the A/B Adapter 2 subaddress. If an A/B Adapter 1 or 2 subaddress is not specified, the analog call is not answered.</li> <li>• Don't care - all numbers accepted: All digital calls, including global calls (without CDPN and CDSA in the call setup) to any CDPN (Called Party Number) are answered. All analog calls are routed to either the A/B Adapter 1 or A/B Adapter 2, or they are not answered. Answering analog calls depends on the setting of Analog Call Routing. All global analog calls either accept the numbers or do not answer them depending on the setting of Global Analog Call.</li> </ul>

**Table 3-4. ISDN Setup Field Descriptions (continued)**

Field	Description
Analog Call Routing	All analog calls are routed to the A/B Adapter 1 if the setting is A/B Adapter 1. The calls are routed to the A/B Adapter 2 if the setting is A/B Adapter 2. They are not answered if the setting is Ignore.
Global Analog Call	All global analog calls are answered and routed to the A/B Adapter 1 or A/B Adapter 2 (the setting in the field of Analog Call Routing) if the setting is Accept. They are not answered if the setting is Ignore.

Figure 3-5 shows Menu 2 - ISDN Setup for DSS1.

```

Menu 2 - ISDN Setup

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

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

Dial Prefix to Access Outside Line=
FAX Number (Include S/T Bus Number)=
Incoming Phone Number Matching= Multiple Subscriber Number (MSN)
  Analog Call Routing= N/A
  Global Analog Call= N/A

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

**Figure 3-5. Menu 2 - ISDN Setup for DSS1**

## Ethernet Setup

Menu 3 is for configuring the Ethernet LAN parameters, including interface type, filters, DHCP, and IP address information. From the Main Menu, enter 3 to display Menu 3 – Ethernet Setup. There are two submenus: Menu 3.1 – General Setup and Menu 3.2 – TCP/IP and DHCP Setup. Refer to the following sections for descriptions of these submenus. Refer to Table 3-1 on page 3-3 for information about navigating through the menus.

### General Setup Menu

The General Setup Menu determines the type of Ethernet interface you are using and the filter sets you want to implement to monitor your Ethernet traffic. Refer to Table 3-6 for a description of each field in this menu.

Table 3-5 lists and describes the interface and filter choices in the Ethernet General Setup menu.

**Table 3-5. Ethernet General Setup Menu Fields**

Field	Description
Ethernet Interface (Model RT328 router only)	The router supports two types of Ethernet connections, AUI (15-pin) or UTP 10BASE-T (telephone type connector). Determine which type you are using and select the appropriate option in this field.
Input and Output Filters Sets	Input and Output Filter Sets: Filter sets are used to block certain packets, to reduce traffic, and to prevent a security breach. Leave these fields blank until you have configured the filters. Refer to Chapter 8, "Filter Configuration," for more information about configuring filters.

## DHCP and TCP/IP Setup

The router has the capability to act as a DHCP server, allowing it to assign IP, DNS, and Default Gateway addresses to attached PCs or workstations. The assigned Default Gateway address is the LAN address of the router, as set in the TCP/IP section. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

If you are setting up your network for the first time, read about IP addresses starting with “IP Addresses and the Internet” on page 1-7 and “IP Configuration by DHCP” on page 1-15 for an explanation of DHCP and information about how to assign IP addresses for your network.

Table 3-6 lists and describes the fields to use for setting up TCP/IP parameters. When you finish entering information in all of the fields, press [Enter] at the prompt Press ENTER to Confirm. Your selections are saved. Press [Esc] at any time to cancel the entries you have made.

**Table 3-6. Menu 3 - Ethernet Setup Menu Fields**

Field	Description
DHCP Setup:	
DHCP	If set to Server, the router acts as a DHCP server.
Client IP Pool Starting Address	This field is the beginning of the range of addresses to assign.
Size of Client IP Pool	This field is the number of sequential addresses available for assignment to attached hosts. The maximum is 32.
Primary DNS Server	If you want the router to assign the Primary DNS Server address to attached hosts, enter the address in this field.
Secondary DNS Server	If you want the router to assign the Secondary DNS Server address to attached hosts, enter the address in this field.
TCP/IP Setup:	
IP Address	Enter the IP address of the LAN interface of the router in dotted-decimal notation (four 8-bit numbers, between 0 and 255, separated by periods, for example, 192.168.135.5). Every device on the TCP/IP network must have a unique IP address.
IP Subnet Mask	An IP address consists of two parts, the network ID and the host ID. The IP Subnet Mask specifies the network ID portion of the address, written in dotted-decimal notation. The router automatically calculates this mask for the class of the IP address that you assign. Unless you have a special need for subnetting, use the default subnet mask calculated by the router. All hosts on the LAN segment should use the same mask.



**Table 3-6. Menu 3 - Ethernet Setup Menu Fields (continued)**

Field	Description
TCP/IP Setup (continued) RIP Direction       RIP Version	<p>This parameter determines how the router handles RIP (Routing Information Protocol). If set to Both (default), the router broadcasts the routing table of the router on the LAN and incorporates RIP broadcasts by other routers into its routing table. If set to In Only, the router broadcasts its routing table on the LAN. If set to Out Only, the router broadcasts its routing table, but it ignores any RIP broadcast packets that it receives. If set to None, the router does not participate in any RIP exchange with other routers. Usually, you should leave this parameter at the default (Both) and let RIP propagate the routing information automatically.</p> <p>This field determines how the router handles RIP (Routing Information Protocol).                      The following RIP options are supported by the Model RT328/RH348 router:</p> <ul style="list-style-type: none"> <li>• RIP-1—The router will accept and send RIP-1 messages only.</li> <li>• RIP-2B—The router will accept RIP-1 and RIP-2 messages (both broadcast and multicast) and send RIP-2 messages in broadcast format.</li> <li>• RIP-2M—The router will accept RIP-1 and RIP-2 messages (both broadcast and multicast) and send RIP-2 messages in multicast format.</li> </ul> <p>For most applications, the recommended version is RIP-2B. Select RIP-1 if other connected routers or workstations have problems with RIP-2. Select RIP-2M only in a pure RIP-2 environment.</p>

## Manager Password Setup

---

To change the Manager password:

1. **Select option 23 (System Security) from the main menu.**
2. **Enter 1 to display Menu 23.1 - System Security - Change Password.**
3. **Enter your previous system password and press [Enter].**
4. **Enter your new system password and press [Enter].**
5. **Enter your new system password again for confirmation and press [Enter].**

You must enter this new password when you want to access the Manager through the serial port or by a Telnet connection.

If you lose or forget the Manager password, you must clear the configuration of the router as described in Chapter 10, "Troubleshooting." Clearing the configuration will cause the Manager password to revert to the factory default, 1234.

# Chapter 4

## Configuration for Internet Access

This chapter provides information to help you configure your Model RT328/RH348 router for Internet access.

### Information Checklist

---

Use Menu 4 of the Manager to configure Internet access. Before you configure the router for Internet access, make sure your ISP (Internet service provider) provides you with the following information:

- For your router
  - IP address of the gateway of your ISP (optional)
  - Telephone number(s) of your ISP
  - Login name
  - Password for authentication
- For your workstation
  - IP address of the Domain Name Server (DNS) of your ISP

NETGEAR recommends that you review the information about IP addressing starting with “IP Addresses and the Internet” on page 1-7.

## Internet Access Configuration

---

You can configure the router for access to an Internet service provider (ISP) using Menu 4, Internet Access Setup. When you complete this menu, the router will automatically add a Remote Node for your ISP in Menu 11, using typical ISP configuration parameters in addition to those you have specified in Menu 4. The router will also create a default static route for the ISP in Menu 12. After completing Menu 4, you may go to Menus 11 and 12 and make modifications to any of the parameters. However, if you return to Menu 4, make changes, and then save them, the ISP-related entries in Menu 11 and 12 will once again be programmed to typical ISP configuration parameters, possibly reversing any changes you have made to those menus.

To configure your router for Internet access:

1. **Enter 4 from the Main Menu to display Menu 4 - Internet Access Setup.**
2. **Enter the name of your ISP in the ISPs Name field (for example, mysip).**

This information is for identification purposes only.

3. **Enter the IP Address of the remote gateway at the point of presence (POP) of the ISP in the ISP IP Addr field (optional).**

If you do not have this data, you can leave it blank.

4. **Enter a primary phone number and a secondary phone number in the Pri(mary) Phone # and Sec(ondary) Phone Number fields.**

Both the primary and the secondary phone number refer to the number that the router dials to connect to the ISP. The router calls your ISP using the primary phone number first. If the primary phone number is busy or does not answer, the router calls the secondary phone number if available. The secondary number is not necessarily the number your router will dial to add additional bandwidth for a Multilink call. If the called router supports BACP, that router will provide the dial number for a second call.



**Note:** In North America, you should enter the full long distance number (1 + area code), even if it is a local call. Otherwise, in some areas, the call is placed as a 56K call.

5. **Enter your login name in the My Login Name field.**

Enter the login name given to you by your ISP.

**6. Enter your password in the My Password field.**

Enter the password associated with the login name from your ISP.

**7. Enter single-user account information in the Single User Account field.**

Refer to “Single IP Address Operation Using NAT” on page 1-13 and “Configuration for Single User Account” on the next page for more information about the Single User Account field. The default is No.

**8. Enter the transfer rate in the Telco Options: Transfer Type field.**

When establishing a call in North America, your router specifies a data rate and the type of call based on this field. The following three options are available for this field:

- 64K—The router places a 64 Kbps digital data call (default).
- 56K—The router places a 56 Kbps digital data call.
- DOVBS—The router places a 56 Kbps data over voice bearer service (DOVBS) call.



**Note:** Some phone companies in North America charge less if calls are made using DOVBS.

**9. Use the space bar to make a selection in the Multilink field.**

This field determines under which circumstances the router will place an additional call to the ISP in order to increase the bandwidth of the connection. The following three options are available for this field:

- Off—The router will place only a single channel call to the ISP.
- BOD—The router will add bandwidth on demand (BOD), placing a second call when the data rate increases beyond a specified level for a specified period. These parameters may be changed using the Edit PPP submenu of Menu 11 – Remote Node Setup Menu.
- Always—The router will always call the ISP using both channels for a 128K connection.

**10. Press [Enter] at the Press ENTER to Confirm... prompt to confirm your selections.**

You can also press [Esc] at any time to cancel your selections.

The Manager asks if you want to test the Internet connection. If you select Yes, the router calls the ISP to test the Internet connection. If the test fails, note the error message that you receive and take the appropriate troubleshooting steps.

## Configuration for Single User Account

---

The Model RT328/RH348 router implements NAT (IP masquerading), allowing the use of a single-user account for Internet access. The steps for configuring your router for single-user Internet access are similar to those for conventional Internet access, with the exception that you need to fill in three extra fields. To configure your router for single-user Internet access, follow steps 1 through 6 from the previous section, "Internet Access Configuration." You must provide the following additional information in step 7 before proceeding to step 8 and step 9:

- **Single User Account**

Enter Yes to enable the Single User Account feature. Use the space bar to toggle between Yes and No.

- **Single User Account: 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.

- **Single User Account: Server IP Addr**

If you want to make your local server (for example, a Web server) accessible to outside users, enter the IP address of that server here. Incoming packets with destination port numbers not handled by the router will be forwarded to this server address.

# Chapter 5

## Remote Node Configuration

This chapter discusses the protocol-independent parameters used to configure a remote node. The protocol-dependent (TCP/IP) configuration is covered in a later chapter.

A remote node represents both a remote gateway and the network behind it, across an ISDN connection. A remote node is required for placing calls to a remote network or answering calls from a remote network. When you use Menu 4 to configure your router for Internet access, the router automatically adds a remote node for you because the ISP falls outside the normal criteria that define a remote node.



**Note:** If you access only one remote node (not an ISP), create that remote node using Menu 4 and then edit it with Menu 11. Creating the remote node using Menu 4 and editing it with Menu 11 makes the remote node the default static route.

When a remote node is configured properly, traffic to the remote LAN triggers the router to make a call automatically (Dial On Demand). Similarly, calls from the remote LAN are answered automatically and security is checked.

To create a remote node:

1. **Enter 11 from the Main Menu to display Menu 11 - Remote Node Setup.**
2. **Enter a remote node number (1 to 4) to edit the remote node and to display Submenu 11.1 - Remote Node Profile.**
3. **Press [Enter] at the Press ENTER to Confirm... prompt to confirm your selections.**

Press [Esc] at any time to cancel your selections.

Table 5-1 lists and describes the fields in the Remote Node Profile menu and explains how to enter the information in each field.

**Table 5-1. Menu 11.1 Remote Node Profile Fields**

Field	Description
Rem Node Name	This field is required. Enter a descriptive name for the remote node (for example, MyOffice). This field supports 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 the router, even though it is still kept in the database and can be activated in the future. Deactivated nodes are displayed with a minus sign (-) preceding the name in Menu 11.
Call Direction	If this parameter is set to Both, the router can place and receive calls to and from this remote node. If set to Incoming, the router does not place a call to this remote node. If set to Outgoing, the router will drop any call from this 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.
Incoming:	
Rem Login Name	Enter the login name that this remote node will use when it calls into the router.
Rem Password	Enter the password used when this remote node calls into the router.
Rem CLID	This field is active only if Call Direction is either Both or Incoming. Otherwise, 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, the router checks this number against the CLID in the incoming call. If they do not match and the CLID Authen is Required, the router rejects the call.
Call Back	This field is valid only if Call Direction is Both. Otherwise, N/A appears in the field. This field determines whether or not you want the router to call back after receiving a call from this remote node. If this option is enabled, the router disconnects the initial call from this node and calls the node back at the Outgoing Primary Phone Number.
Outgoing:	
My Login Name	This is a required field if Call Direction is either Both or Out. Enter the login name your router uses when it calls this remote node.
My Password	This is a required field if Call Direction is either Both or Out. Enter the password your router uses when it calls this remote node.
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: <ul style="list-style-type: none"> <li>• CHAP/PAP—Router will try CHAP when CHAP is requested by the remote node or PAP when PAP is requested by the remote node (Default).</li> <li>• PAP—Use PAP only.</li> <li>• CHAP—Use CHAP only.</li> </ul>



**Table 5-1. Menu 11.1 Remote Node Profile Fields (continued)**

Field	Description
Pri(mary) Phone Number and Sec(ondary) Phone Number	Both the Primary and Secondary Phone numbers refer to the number that the router dials to connect to the remote node. The router calls the remote node using the Primary Phone number first. If the Primary Phone number is busy or does not answer, the router calls the Secondary Phone number if available. Note that the secondary number is not necessarily the number your router will dial to add additional bandwidth for a Multilink call. If the called router supports BACP, that router will provide the dial number for a second call. In North America, NETGEAR recommends that you enter 1 and the area code with the number, even if it is a local call. Otherwise, in some areas, the call is placed as a 56K call.
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] to display Menu 11.2 - Remote Node PPP Options. For more information about configuring PPP options, see "Editing PPP Options" on page 5-4.
Rem IP Addr	This field is required on all remote nodes except the ISP node. Enter the IP address of the router at the remote site. A static route will be created to the network address of that router. Note that if the remote network uses a netmask other than the standard class netmask, you must enter the netmask in the Edit IP Options submenu.
Edit IP Options	This field edits the parameters of the TCP/IP protocol. Select Yes and press [Enter] to display Menu 11.3 - Remote Node Network Layer Options. For more information about this screen, refer to Chapter 7, "TCP/IP Configuration."
Telco Options:	
Transfer Rate	When establishing a call in North America, your router specifies a data rate and the type of call based on this field. Three options are available for this field: <ul style="list-style-type: none"> <li>• 64K—The router places a 64 Kbps (kilobits per second) digital data call (default).</li> <li>• 56K—The router places a 56 Kbps digital data call.</li> <li>• DOVBS—The router places a 56 Kbps data over voice bearer service (DOVBS) call. Some phone companies in North America charge less if calls are made using DOVBS.</li> </ul>
Allocated Budget (min)	This field sets a budget on outgoing call time for the remote node. The default for this field is 0 for no budget control.
Period (hr)	This field sets the time interval to reset the above outgoing call budget control.

**Table 5-1. Menu 11.1 Remote Node Profile Fields (continued)**

Field	Description
Session Options: Output Filter Sets 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 the router. 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). Spaces and commas are accepted in this field. The default is blank (no filters are defined). Refer to Chapter 8, "Filter Configuration," for more information about configuring filters.
Idle Timeout (sec)	This value specifies the number of idle seconds elapsed 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 router. Administrative packets such as RIP are not counted as data. The default is 300 seconds (5 minutes).

---

## Editing PPP Options

---

To edit PPP options:

1. **Select Yes in the Edit PPP Options field of Submenu 11.1 - Remote Node Profile.**
2. **Press [Enter] to display Menu 11.2 Remote Node PPP Options.**
3. **Edit the options described in Table 5-2.**
4. **Press [Enter] at the Press ENTER to Confirm... prompt to confirm your selections, and return to the previous menu.**

Press [Esc] at any time to cancel your selections.

5. **Continue to the end of Menu 11.1 and press [Enter] to save the selections you made in Menu 11.2.**

Table 5-2 lists and describes each field in Menu 11.2 - Remote Node PPP Options. Refer to “Bandwidth on Demand” on page 5-6 for further information about related fields in this menu.

**Table 5-2. Fields in Menu 11.2 - Remote Node PPP Options**

Field	Description
Encapsulation	Select CCP (Compression Control Protocol) for the PPP or MP link. Two options are available in this field: <ul style="list-style-type: none"> <li>• Standard PPP—Standard PPP options are used (default).</li> <li>• CISCO PPP—Cisco Systems PPP options are used.</li> </ul>
Compression	Allows the negotiation of data compression with the remote node router.
Multiple Link Options:	
BOD Calculation	Select the direction of the traffic you want to calculate in order to determine when to add or subtract a link. The default for this field is Transmit or Receive.
Base Trans Rate	Select the base data transfer rate for this remote node. This parameter is in kilobits per second (Kbps). Two options are available for this field: <ul style="list-style-type: none"> <li>• 64—Only one channel will be used (default).</li> <li>• 128—Two channels will be used when a packet triggers a call.</li> </ul>
Max Trans Rate	Enter the maximum data transfer rate allowed for this remote node. This parameter is in kilobits per second. There are two options for this field: <ul style="list-style-type: none"> <li>• 64—At most, one channel can be used (default).</li> <li>• 128—A maximum of two channels can be used.</li> </ul>
Target Utility	Enter the two thresholds separated by a hyphen ( - ) for subtracting and adding the second channel. The default is 32-48.
Add Persist	This parameter specifies the number of seconds that traffic must be above the adding threshold before the router brings up the second channel. The default is 5 seconds.
Subtract Persist	This parameter specifies the number of seconds that traffic must be below the subtraction threshold before the router drops the second channel. The default is 5 seconds.

## Bandwidth on Demand

---

The Bandwidth on Demand (BOD) feature allows you to bundle both B channels in one logical connection. The second channel is added and subtracted dynamically according to traffic demand. The router uses the Bandwidth Allocation Control Protocol (BACP) and the Multilink Protocol (MP) in implementing bandwidth on demand.

The configuration of bandwidth on demand focuses on the Base Transmission Rate (BTR) and the Maximum Transmission Rate (MTR). The relationship between BTR and MTR is shown in Table 5-3.

**Table 5-3. Relationship Between BTR and MTR**

<b>BTR &amp; MTR Setting</b>	<b>Number of Channels Used to Initiate Call</b>	<b>Max Number of Channels Used</b>	<b>Bandwidth on Demand</b>
BTR = 64, MTR = 64	1	1	Off
BTR = 64, MTR = 128	1	2	On
BTR = 128, MTR = 128	2	2	Off

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

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

# Chapter 6

## Dial-In Configuration

You can configure the router to receive calls from remote dial-in users (for example, telecommuters) and remote nodes. Several differences exist between remote dial-in users and remote nodes:

- The router can make calls to or answer calls from the remote node, but the remote dial-in user calls are incoming or callback only.
- Each remote node can have its own set of parameters such as bandwidth on demand, protocol, and security; however, all remote dial-in users share one common set, as defined in the Default Dial In Setup (Menu 13).
- Typically, remote dial-in users are individual users who dial in to the router directly from their workstations; and remote nodes represent networks and are used for LAN-to-LAN connections.

This chapter discusses how to set up default dial-in parameters for both a remote node and a remote dial-in user.

### 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. After authentication is completed, if it matches a remote node, the router uses parameters from that particular remote node.

From the Main Menu, enter 13 to display Menu 13 - Default Dial-in Setup.

When you finish filling in Menu 13 - Default Dial-in Setup, press [Enter] at the ENTER to Confirm... prompt to save your selections. You can press [Esc] at any time to cancel your selections.

Table 6-1 lists and describes the fields in the Default Dial-in Setup menu and explains how to configure the protocol-independent fields in this menu.

**Table 6-1. Fields in Menu 13 - Default Dial-in Setup**

Field	Description
Telco Options: CLID Authen	This field sets the CLID authentication parameter for all incoming calls. The three options for this field are: <ul style="list-style-type: none"> <li>• None—No CLID is required (default).</li> <li>• Required—You must provide the CLID, or the call is disconnected.</li> <li>• Preferred—If the CLID is available, it is used to do authentication. If the CLID is not available, the call continues.</li> </ul>
PPP Options: Recv Authen  Compression  Mutual Authen	This field sets the authentication protocol used for incoming calls. The four options for this field are: <ul style="list-style-type: none"> <li>• CHAP/PAP—The router tries CHAP first, but PAP is used if CHAP is not available (default).</li> <li>• CHAP—Use CHAP only.</li> <li>• PAP—Use PAP only.</li> <li>• None—No authentication is required.</li> </ul> This field allows the negotiation of data compression with the equipment of the dial-in user. <p>Some vendors (for example, Cisco Systems) implement a type of mutual authentication. That is, the node that initiates the call requests a user name and password from the far end that it is dialing to. If the remote node that is dialing in implements this type of authentication, set this field to Yes. Choose one of the following for setting PAP:</p> <ul style="list-style-type: none"> <li>• PAP Login—This field is enabled only if the Mutual Authen field is set to Yes. Enter the login name to be used to respond to the PAP authentication request of the far end. This field does not apply to CHAP authentication.</li> <li>• PAP Password—This field is enabled only if the Mutual Authen field is set to Yes. Enter the PAP password to be used to respond to the authentication request of the far end. This field does not apply to CHAP authentication.</li> </ul>

**Table 6-1. Fields in Menu 13 - Default Dial-in Setup (continued)**

Field	Description
Multiple Link Options: Max Trans Rate	Enter the maximum data transfer rate between your router and the remote dial-in user in this field. The unit is in Kbps. The two options for this field are: <ul style="list-style-type: none"> <li>• 64—At most, one B channel is used.</li> <li>• 128—A maximum of two channels can be used (default).</li> </ul> When the router calls back to the remote dial-in user, the maximum data transfer rate is always 64.
Callback Budget Management: Allocated Budget (min) Period (hr)	This field sets a budget callback time for all the remote dial-in users. The default for this field is 0 for no budget control.  This field sets the time interval to reset the above callback budget control.
IP Address Supplied By: Dial-in User IP Pool	If this field is set to Yes, the router allows a remote host to specify its own IP address. If this field is set to No, the remote host uses the IP address assigned by the router from the IP pool. The default is Yes.  If this field is set to Yes, the router provides 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 the router accepts the IP address if the remote peer specifies one; otherwise, an IP address is assigned from the pool. The default is No. Choose from the following options to set the IP address and the IP count: <ul style="list-style-type: none"> <li>• 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.</li> <li>• IP Count (1,2)—In this field, enter the number (1 or 2) 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 has 192.168.135.5 and 192.168.135.6.</li> </ul>

**Table 6-1. Fields in Menu 13 - Default Dial-in Setup (continued)**

Field	Description
Session Options:  Input Filter Sets and Output Filter Sets          Idle Timeout	In these fields, you can select the filter set(s) to filter the incoming and outgoing traffic between your router and the remote dial-in user. These filter set(s) 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). Spaces and commas ( , ) are accepted in this field. For more information about customizing your filter sets, see Chapter 8, "Filter Configuration." The default is blank (no filters).  This value is the number of idle seconds that elapse 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 the router. This field is used only if the Recv. Authen is set to None and the call is not mapped to any remote node or remote dial-in user or the router calls back to the remote dial-in user.

## Dial-In Users Setup

---

To add a remote dial-in user, enter 14 from the main menu to display Dial-in User Setup.

To edit user parameters, select one of the eight users to go to the Edit Dial-in User menu.

When you have completed filling in Menu 14.1 - Edit Dial-in User, press [Enter] at the Press ENTER to Confirm... prompt to save your selections. You can press [Esc] at any time to cancel your selections.



Table 6-2 lists and describes the fields in the Edit Dial-in User menu.

**Table 6-2. Fields in Menu 14.1 - Edit Dial-in User**

Field	Description
User Name	This field is required and 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.
Password	Enter the password in this field for the remote dial-in user.
Callback	This field determines whether the router allows callbacks to the user upon dial-in. Three modes are provided: <ul style="list-style-type: none"> <li>• No (default)—The router does not call back to the dial-in user.</li> <li>• Optional—The router will call back if the dial-in user requests it.</li> <li>• Mandatory—The router will always disconnect and call back to the dial-in user.</li> </ul> If callback is enabled, the router disconnects the initial call and dials back to the specified callback number or to a number specified by the user, depending on which option is set below.
Phone # Phone # Supplied by Caller  Callback Phone #	If this field is Yes, the Remote Dial-in User must specify the callback telephone number on a call-by-call basis, which is useful when the router returns a call back to a mobile user at different numbers. The default is No (the router always calls back to a fixed callback number). If Callback is No, N/A appears in the field.  If the previous field (Phone # Supplied by Caller) is No, this field is required. Otherwise, N/A appears in the field. Enter the telephone number that the router should call back.
Rem CLID	If you have enabled the CLID Authen field in Menu 13, you must specify the telephone number from which this remote dial-in user calls. The router checks this number against the CLID in the incoming call. If they do not match and the CLID Authen is Required, the router rejects the call.
Idle Time-out	Enter the idle time (in seconds). This timeout determines how long the dial-in user can be idle before the router disconnects the call. Idle time is defined as the period of time when there is no data traffic between the dial-in user and the router. The default is 300 seconds (5 minutes).



# Chapter 7

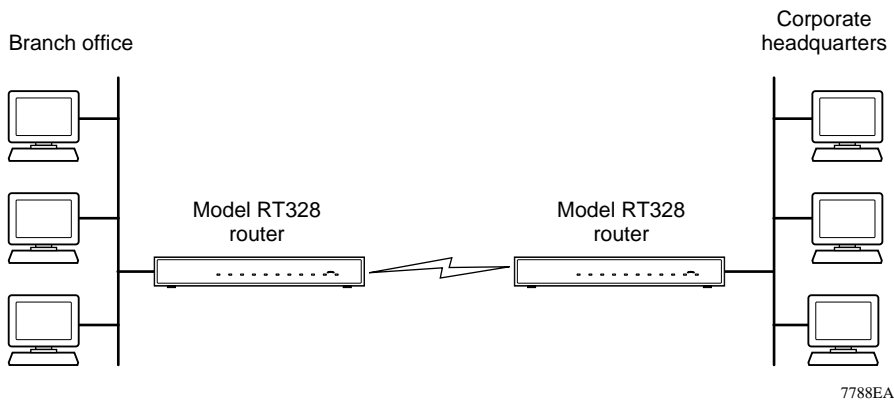
## TCP/IP Configuration

This chapter describes how to configure your Model RT328/RH348 router for TCP/IP. Depending on your particular applications, you must configure different menus. For instance, Internet access is the most common application of TCP/IP. For this application, you should configure Menu 4. Configurations for other applications are provided in the following sections.

### LAN-to-LAN Application

---

An example of a typical LAN-to-LAN application is to use the router to call from a branch office to the headquarters, as shown in Figure 7-1.




**Figure 7-1. LAN-to-LAN Application**

For the branch office, you must 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.

## Remote Node Setup

See Chapter 5, “Remote Node Configuration,” for information about using the protocol-independent parameters on Menu 11.1 - Remote Node Profile. Use the fields described in Table 7-1 to set the protocol-dependent parameters.

	<p><b>Note:</b> If you are configuring the router to receive an incoming call, you must also set the default dial-in parameters in Menu 13 (see Chapter 6).</p>
---	---

**Table 7-1. Fields in Menu 11.1 - Remote Node Profile Fields**

Field	Description
Rem IP Address	Enter the IP address of the router at the remote site. If the remote router uses a different IP address than the one entered here, the call will be terminated. A static route will be created to the network address of the remote router. Note that if the remote network uses a netmask other than the standard class netmask, you must enter the netmask in the Edit IP Options submenu.
Edit IP	Press the space bar to change this field to Yes and press [Enter] to display the Menu 11.3 - Remote Node Network Layer Options menu.

To set the protocol-dependent parameters:

1. **Select Yes in the Edit IP field of Submenu 11.1 - Remote Node Profile.**
2. **Press [Enter] to display Menu 11.3 - Remote Node Network Layer Options.**
3. **Edit the options described in Table 7-2.**
4. **Press [Enter] at the Press ENTER to Confirm... prompt to confirm your selections and return to the previous menu.**  
 Press [Esc] at any time to cancel your selections.
5. **Continue to the end of Menu 11.1 and press [Enter] to save the selections you made in Menu 11.3.**

Table 7-2 lists and describes the fields for Menu 11.3 - Remote Node Network Layer Options.

**Table 7-2. Menu 11.3 Remote Node Network Layer Options Fields**

Field	Description
Rem IP Address	This read-only field shows the IP address you entered for this remote node in the previous menu.
Rem Subnet Mask	This field will display the standard class netmask for the network address of the remote router. If the remote network uses a netmask other than the standard class netmask, you must enter the netmask here.
My WAN Addr	Some network implementations require hosts on both ends of the ISDN link to have separate addresses from the LAN, and these addresses must have the same network number. If this situation, known as numbered links, applies to your network, enter the IP address in this field that is assigned to the WAN port of your router. This is the address assigned to the local router, not the remote router.
Single User Account	If this field is set to Yes, the router performs NAT (IP Address Masquerading) to this node. See "Single IP Address Operation Using NAT" on page 1-13 for information about the Single User Account feature. The default is No.
Single User Account: Server IP Addr	If you have selected Single User Account and want to make your local server accessible to outside users, enter the IP address of that server here. Incoming packets with destination port numbers not handled by the router will be forwarded to this server address.
Metric	The Metric field 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 in this field 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.
Private	This field determines if the router includes the route to this remote node in its RIP broadcasts. If set to Yes, this route is kept private and not included in any RIP broadcast. If set to No, the route to this remote node is propagated to other hosts through RIP broadcasts.

**Table 7-2. Menu 11.3 Remote Node Network Layer Options Fields (continued)**

Field	Description
RIP: RIP Direction	This parameter determines how the router handles RIP (Routing Information Protocol). If set to Both (default), the router broadcasts the routing table of the router on the LAN and incorporates RIP broadcasts by other routers into its routing table. If set to In Only, the router broadcasts its routing table on the LAN. If set to Out Only, the router broadcasts its routing table, but it ignores any RIP broadcast packets that it receives. If set to None, the router does not participate in any RIP exchange with other routers. Usually, you should leave this parameter at the default (Both) and let RIP propagate the routing information automatically.
RIP Version	<p>This field determines how the router handles RIP (Routing Information Protocol). The following RIP options are supported by the Model RT328/RH348 router:</p> <ul style="list-style-type: none"> <li>• RIP-1—The router will accept and send RIP-1 messages only.</li> <li>• RIP-2B—The router will accept RIP-1 and RIP-2 messages (both broadcast and multicast), and send RIP-2 messages in broadcast format.</li> <li>• RIP-2M—The router will accept RIP-1 and RIP-2 messages (both broadcast and multicast), and send RIP-2 messages in multicast format.</li> </ul> <p>For most applications, the recommended version is RIP-2B. Select RIP-1 if other connected routers or workstations have problems with RIP-2. Select RIP-2M only in a pure RIP-2 environment.</p>

## Static Route Setup

---

On a directly connected internetwork, RIP usually handles the routing automatically. However, RIP cannot propagate across isolated networks, as in the case before a connection is made between 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 the router with some static routing information. When you configure for Internet access or a remote node, a static route is implicitly created by the router.

Under normal circumstances, the router has adequate routing information after you configure the Internet access and remote nodes, and you do not need to configure additional static routes. You must configure static routes only for unusual cases (for example, subnetting). To view the routes in the routing table, go to the Command Interpreter Mode (Menu 24.8) and type “ip route stat.” After viewing the table, type “exit” to return to the menus. To create additional static routes for IP, use Menu 12 - Static Route Setup. Select an unused number from the menu, and a new menu appears. This menu is Menu 12.1, the Edit IP Static Route menu.

When you complete the menu, press [Enter] at the Press ENTER to Confirm... prompt to save your selections, or press [Esc] at any time to cancel your selections.

Table 7-3 lists and describes the fields for Menu 12.1 - Edit IP Static Route.

**Table 7-3. Edit IP Static Route Menu Fields**

Field	Description
Route Name	Enter a descriptive name for this route for identification purposes only.
Active	This field allows you to activate or deactivate this static route.
Destination IP Address	This field 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. For more information about setting IP subnet masks, see "Subnet Addressing" on page 1-10.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of the router that forwards the packet to the destination. On the LAN, the gateway must be a router on the same segment as the router. Over ISDN, the gateway must be the IP address of one of the remote nodes.
Metric	The Metric field represents the cost of transmission for routing purposes. IP routing uses hop counts 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 does not have to be precise, but it must be between 1 and 16. In practice, 2 or 3 is usually a good number.
Private	This field determines if the router includes the route to this remote node in its RIP broadcasts. If set to Yes, this route is kept private and not included in any RIP broadcast. If set to No, the route to this remote node is propagated to other hosts through RIP broadcasts.





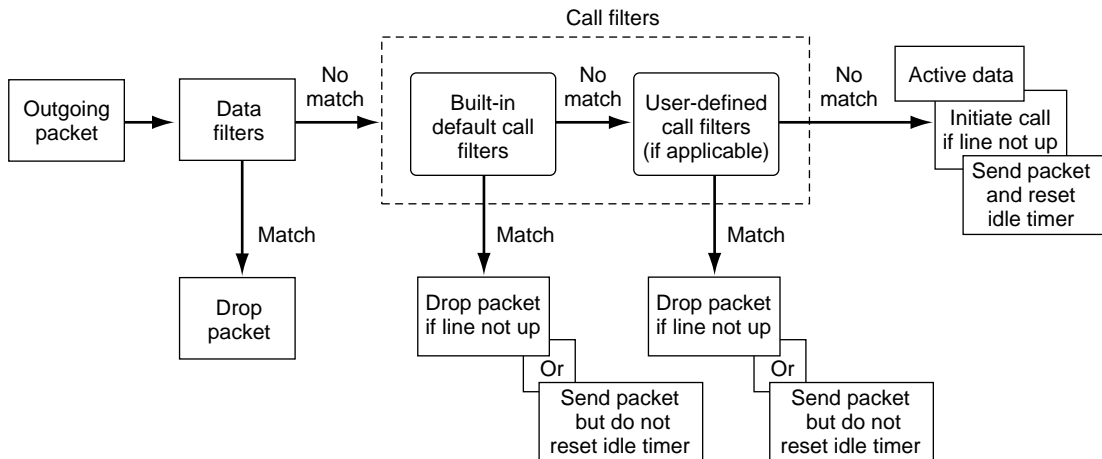
# Chapter 8

## Filter Configuration

This chapter provides information about using filters and configuring filters for your Model RT328/RH348 router.

The router uses filters to decide whether to allow passage of a data packet and/or to make a call over the ISDN line. Three types of filters are involved: incoming data filters, outgoing data filters, and 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 call filters. The call filters are divided into two groups: default call filters and user-defined call filters. The Model RT328/RH348 router has default call filters that filter out administrative packets (for example, RIP packets). The router applies the default filters first and then, if applicable, applies the user-defined call filters as shown in Figure 8-1.



7787EA

**Figure 8-1. Outgoing Packet Filtering Process**

For incoming packets, the router applies data filters only. Packets are processed depending on whether a match is made. The router allows you to customize the filter sets that you want to use. The following sections describe how to configure the filter sets for the router.

## **Router Filter Structure**

---

You can configure up to 12 filter sets, each with up to six rules. For IP packets, these rules involve comparing the protocol type of a data packet (for example, TCP, UDP), source or destination addresses, or port numbers. Also, a generic filter may be defined to merely test for a byte or pattern of bytes in a particular location in the packet. When a rule is met (or not met), a user-specified action is taken. This action may be to forward the packet, drop the packet, or go to the next rule.

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.

## **Configuring a Filter Set**

---

To configure a filter set, select option 21 in the Main Menu. This selection brings up Menu 21 - Filter Set Configuration. From this menu, you can choose from among 12 filter sets. Select the filter that you want to configure or choose an unused set to create a new filter. In order to distinguish between the 12 filter sets, each filter set should have a name or some comments. When you select a set for editing, you will be prompted to provide some descriptive text to be displayed in the comment field of Menu 21 next to the filter number.

When you have finished filling in the Edit Comments field, press [Enter] at the Press ENTER to Confirm... prompt to confirm your selections, 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.

When you press [Enter], Menu 21.1 - Filter Rules Summary is displayed. The information in this menu is read-only; the parameters of each rule that you configured for that set are displayed.

Table 8-1 lists and describes the abbreviations used in Menu 21.1 - Filter Rules Summary.

**Table 8-1. Abbreviations Used in Menu 21.1 - Filter Rules Summary**

Abbreviation	Description
#	Refers to the filter rule number (1–6).
A	Refers to Active. Y means the filter rule is active, and N means the filter rule is inactive.
Type	Refers to the type of filter rule and can display GEN for generic or IP for TCP/IP.
Filter Rules	The filter rule parameters are displayed here.
M	Refers to More. Y means there are more rules to check. N means there are no rules to check.
m	Refers to Action Matched. F means to forward the packet, D means to drop the packet, and N means to check the next rule.
n	Refers to Action Not Matched. F means to forward the packet, D means to drop the packet, and N means to check the next rule.

For more information about filter rules, refer to “Configuring a Filter Rule,” on page 8-4.

If the filter type is IP (TCP/IP), the abbreviations listed in Table 8-2 are used.

**Table 8-2. Abbreviations Used if Filter Type Is IP**

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

If the filter type is GEN (generic), the abbreviations listed in Table 8-3 are used.

**Table 8-3. Abbreviations Used if Filter Type Is GEN**

Abbreviation	Description
Off	Offset
Len	Length

To configure a specific filter rule, select the number of the filter rule (1–6) that you want to configure and press [Enter] to display Menu 21.1.1 - TCP/IP Filter Rule.

## Configuring a Filter Rule

---

You can configure two types of filter rules. Some of the parameters differ depending on the type of rule. When you first enter the filter rule menu, Menu 21.1.1 - TCP/IP Filter Rule is displayed. If you want to configure another type of filter rule, select the appropriate type by pressing the space bar under the Filter Type field and then pressing [Enter] to display the menu for the filter rule you want to enter.

### TCP/IP Filter Rule

This section provides information about how to configure a TCP/IP filter rule for your router. The fields in the menu are given in Table 8-4. When you have completed Menu 21.1.1 - TCP/IP Filter Rule, press [Enter] at the Press ENTER to Confirm...prompt to confirm your selections. You can press [Esc] at any time to cancel your selections. The data you entered on Menu 21.1.1 - TCP/IP Filter Rule is displayed on Menu 21.1 - Filter Rules Summary.

Table 8-4 lists and describes the TCP/IP Filter Rule menu fields and a description of each field.

**Table 8-4. TCP/IP Filter Rule Menu Fields**

<b>Field</b>	<b>Descriptions</b>
Active	In this field, you can make the filter rule active (Yes) or make the filter rule inactive (No).
IP Protocol	Protocol refers to the IP-specific number of the protocol. The range for the value entered in this field should be between 0 and 255 (for example, 6 refers to the TCP protocol).
IP Source Route	Yes or No in this field determines whether to check the source route.
Destination: IP Addr  IP Mask  Port #  Port # Comp	<p>In this field, enter the destination IP address of the packet you want 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.</p> <p>In this field, enter the IP subnet mask that will be used to mask the bits of the IP address given in Destination: IP Addr. Refer to Chapter 1, "Introduction," for more information.</p> <p>In this field, enter the destination port of the packets that you want to filter. The range of this field is 0 to 65535.</p> <p>In this field, select the comparison quantifier you want to enable to compare to the value given in Destination: Port #. There are five options for this field:</p> <ul style="list-style-type: none"> <li>• None (default)</li> <li>• Less</li> <li>• Greater</li> <li>• Equal</li> <li>• Not Equal</li> </ul>
Source: IP Addr  IP Mask  Port #	<p>In this field, enter the source IP address of the packet you want to filter. The IP 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.</p> <p>In this field, enter the IP subnet mask that is used to mask the bits of the IP Address given in Source: IP Addr. See "Netmask" on page 1-9 for information about IP subnet masks.</p> <p>In this field, enter the source port of the packets that you want to filter. The range of this field is 0 to 65535.</p>

**Table 8-4. TCP/IP Filter Rule Menu Fields (continued)**

Field	Descriptions
Source (continued):  Port # Comp	In this field, select the comparison quantifier you want to use to compare to the value given in Source: Port #. There are five options for this field: <ul style="list-style-type: none"> <li>• None (Default)</li> <li>• Less</li> <li>• Greater</li> <li>• Equal</li> <li>• Not Equal</li> </ul>
TCP Estab	This field is dependent upon the IP Protocol field. This field is 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: <ul style="list-style-type: none"> <li>• Yes—Filter match only established TCP connections</li> <li>• No—Filter match both initial and established TCP connections (Default)</li> </ul>
More	In this field, you can determine if you want to pass the packet through the next filter rule before an action is taken. Two options are available for this field: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No (default)</li> </ul> If More is Yes, then Action Matched and Action Not Matched is N/A.
Log	In this field, you can determine if you want to log the results of packets attempting to pass the filter rule. These results are displayed on the System Log (see “View Error Log” on page 9-4). Seven options are available for this field: <ul style="list-style-type: none"> <li>• None—No packets are logged (default).</li> <li>• Action Matched—Only packets that match the rule parameters are logged.</li> <li>• Action Not Matched—Only packets that do not match the rule parameters are logged.</li> <li>• Both—All packets are logged.</li> <li>• Check Next Rule (default)</li> <li>• Forward</li> <li>• Drop</li> </ul>
Action Matched Action Not Matched	If the conditions for the filter rule are not met, you can specify what to do with the packet. There are three options for this field: <ul style="list-style-type: none"> <li>• Check Next Rule (default)</li> <li>• Forward</li> <li>• Drop</li> </ul>

## Generic Filter Rule

This section provides information about configuring the protocol-independent parameters for a generic filter rule for your router. Table 8-5 lists the fields in the menu. When you complete Menu 21.1.1 - Generic Filter Rule, press [Enter] at the Press ENTER to Confirm... prompt to confirm your selections. Press [Esc] at any time to cancel your selections. The data entered is displayed on Menu 21.1 - Filter Rules Summary.

**Table 8-5. Generic Filter Rule Menu Fields**

Field	Description
Active	In this field, you can make the filter rule active (Yes) or inactive (No).
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 the router 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.
Mask	In this field, specify (in hexadecimal) the value that the router should logically qualify and the data in the packet. Because length is given in bytes, enter a hexadecimal number that is twice the specified length for numbers in this field. For example, if length is 4, a valid Mask must have 8 hexadecimal numbers (1155ABF8).
Value	In this field, specify (in hexadecimal) the value that the router should use to compare with the masked packet. The value should align with Offset. Because length is given in bytes, you need to enter twice the length in hexadecimal numbers for this field. For example, if length is 4, a valid Value must have 8 hexadecimal numbers (1155ABF8). If the result from the masked packet matches Value, then the packet is considered matched.
More	In this field, you can determine whether to pass the packet through the next filter rule before an action is taken. There are two options for this field: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No (Default)</li> </ul> If Yes is selected for this field, Action Matched and Action Not Matched will be N/A.

**Table 8-5. Generic Filter Rule Menu Fields (continued)**

Field	Description
Log	In this field, you can determine if you want to log the results of packets attempting to pass the filter rule. These results are displayed on the System Log (see “View Error Log” on page 9-4). Seven options are available for this field: <ul style="list-style-type: none"> <li>• None—No packets are logged (default).</li> <li>• Action Matched—Only packets that match the rule parameters are logged.</li> <li>• Action Not Matched—Only packets that do not match the rule parameters are logged.</li> <li>• Both—All packets are logged.</li> <li>• Check Next Rule (default)</li> <li>• Forward</li> <li>• Drop</li> </ul>
Action Matched, Action Not Matched	If the conditions for the filter rule are not met, you can specify what to do with the packet. Three options are available for this field: <ul style="list-style-type: none"> <li>• Check Next Rule (default)</li> <li>• Forward</li> <li>• Drop</li> </ul>

## Applying a Filter Set

After configuring a filter set in Menu 21, you must specify where and how the filter will be used. Data filters can be applied either at the LAN interface (in Menu 3.1) or at the Remote Node interface (Menu 11.1) and can be specified for incoming or outgoing packets. Call filters, which determine whether or not to place a call to forward the packet, are applied at the Remote Node interface (Menu 11.1). Up to four filter sets can be applied to the same port by entering the numbers of the desired filter sets, separated by commas, with no spaces. In the following example, the Remote Node Profile line of Menu 11.1 specifies that filter sets 1, 3, and 10 are used to determine whether a packet causes a call to be placed to the Remote Node.

```
Call Filter Sets = 1,3,10
```



## Reducing Unnecessary Calls by Windows 95

---

One example of when to apply a filter set is reducing unnecessary calls by Windows® 95. When using Windows 95 with a dial-up ISDN router, you may need to make some configuration changes to avoid having ISDN calls placed unnecessarily. Most of these unnecessary calls are caused by PCs on the LAN trying to perform local NetBIOS name resolution, either in response to a user action (browsing the Network Neighborhood or turning a PC on or off, for example) or as periodic background activity. In some cases, this NetBIOS activity can be kept local by other means, such as configuring a WINS or DNS server on the local network, using an LMHOSTS file to store addresses of local hosts, or turning off NetBIOS name resolution by DNS. A simpler method is to filter NetBIOS traffic using the filtering capabilities of your Model RT328/RH348 router.

### Diagnosing the Situation

If you already know the source or types of packets that are causing the problem, you can proceed directly to the design of the filter. Otherwise, you can use a sniffer or the router's built-in tools to determine the source. A particularly useful tool is the display in Menu 24.1 of the "LAN Packet Which Triggered Last Call." Figure 8-2 illustrates the header of the packet that caused an unwanted call to be placed.

```
LAN Packet Which Triggered Last Call: (Type: IP)
45 00 00 3E 9E 05 00 00 1F 11 CC 9D 8D FB 17 12 CF 45 BC B9 00 89 00 35
00 2A 63 C8 01 85 01 00 00 01 00 00 00 00 00 0A 53 41 4E 54 41 43 4C
```

**Figure 8-2. LAN Packet Which Triggered Last Call**

You can wait until an erroneous call is placed, then examine this packet header to determine the source and cause. The IP packet header contains information such as the next-level protocol type (for example, ICMP, TCP, UDP), source and destination addresses, and source and destination port numbers. Analyzing this data reveals the cause of the call, which provides the user with an approach to eliminating the calls. For example, the first line of the packet shows the following (hex values converted to decimal):

- 45 00 00 3E 9E 05 00 00 1F **11** CC 9D 8D FB 17 12 CF 45 BC B9 00 89 00 35  
Bold characters denote protocol (17, or 11h =UDP).
- 45 00 00 3E 9E 05 00 00 1F 11 CC 9D **8D FB 17 12** CF 45 BC B9 00 89 00 35  
Bold characters denote source IP (141.251.23.18=local PC).
- 45 00 00 3E 9E 05 00 00 1F 11 CC 9D 8D FB 17 12 **CF 45 BC B9** 00 89 00 35  
Bold characters denote destination IP (207.69.188.185=DNS server).
- 45 00 00 3E 9E 05 00 00 1F 11 CC 9D 8D FB 17 12 CF 45 BC B9 **00 89** 00 35  
Bold characters denote source port number (137 or 89h=NetBIOS name service).
- 45 00 00 3E 9E 05 00 00 1F 11 CC 9D 8D FB 17 12 CF 45 BC B9 00 89 **00 35**  
Bold characters denote destination port number (53, or 35h=DNS).

This packet represents a NetBIOS name service request from a local PC to the DNS server of the ISP. An initial strategy for blocking this type of call would be to set up a call filter to prevent calls from being originated by UDP packets with a source port of 137 (NetBIOS name service). Further investigation would reveal that other ports are associated with NetBIOS services, and these ports should be blocked, too.

A comprehensive list of protocol and port numbers for common IP traffic can be found in IETF RFC1700, "Assigned Numbers." Many common port numbers are also listed on any Windows PC in a file called \windows\services. In the case of filtering NetBIOS traffic, the relevant ports are:

- 137 (TCP and UDP) NetBIOS Name Service
- 138 (TCP and UDP) NetBIOS Datagram Service
- 139 (TCP and UDP) NetBIOS Session Service

## Implementing the Filter

Now you can proceed to define a call filter to block the three NetBIOS service ports.

The Filter Set Configuration Menu is shown in Figure 8-3.

To define a call filter:

1. **Go to Menu 21 - Filter Set Configuration, and choose a name and filter set.**

```

Menu 21 - Filter Set Configuration

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

      Enter Filter Set Number to Configure= 1

      Edit Comments= netbios

      Press ENTER to Confirm or ESC to Cancel:

```

**Figure 8-3. Menu 21 Filter Set Configuration**

2. **Next, define the filter rules.**

You want your filter to ignore (drop) UDP and TCP packets originating from ports 137, 138, and 139. Because each protocol/port combination must be specified as a separate rule, there will be six rules. Each filter set contains six rules, so you will fill one entire set. Begin with rule 1, as illustrated in Figure 8-3.

3. Set “Active” to Yes, and specify the IP Protocol as 17, which is the UDP protocol number (in decimal) from the Assigned Numbers RFC as described on page 8-10.
4. Specify Source Port #137, NetBIOS Naming Service, and set the Port # Comparison field to look for port numbers “equal” to 137.

For packets that match this comparison, you want to drop the packet, so set Action Matched to “Drop.” For packets not matching, you want to continue to the next rule, so set Action Not Matched to “Check Next Rule.”

Figure 8-4 shows 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= Yes
IP Protocol= 17      IP Source Route= No
Destination: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port # = 0
                Port # Comp= None
Source: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port # = 137
                Port # Comp= Equal

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

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

**Figure 8-4. TCP/IP Filter Rule Menu**

**5. Define the next five rules the same way—one for each combination of the three port numbers and the two protocol types.**

The last rule, however, will be slightly different. For Action Not Matched, select “Forward.” Any packet that has not matched any of the six rules will be forwarded for routing.

When all six rules are defined, Menu 21.1 should appear as it does in Figure 8-5. As a visual check, make sure that all six rules contain “Y” in the A (Active) field, “D” (Drop) in the m (matched) field, and “N” (next rule) in the n (not matched) field, except for the last rule, which should have “F” (Forward) in the n field.

Figure 8-5 shows the Filter Rules Summary menu with all six rules defined.

Menu 21.1 - Filter Rules Summary						
#	A	Type	Filter Rules	M	m	n
1	Y	IP	Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0	N	D	N
2	Y	IP	Pr=17, SA=0.0.0.0, SP=138, DA=0.0.0.0	N	D	N
3	Y	IP	Pr=17, SA=0.0.0.0, SP=139, DA=0.0.0.0	N	D	N
4	Y	IP	Pr= 6, SA=0.0.0.0, SP=137, DA=0.0.0.0	N	D	N
5	Y	IP	Pr= 6, SA=0.0.0.0, SP=138, DA=0.0.0.0	N	D	N
6	Y	IP	Pr= 6, SA=0.0.0.0, SP=139, DA=0.0.0.0	N	D	F

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

**Figure 8-5. Filter Rules Summary Menu**

## Applying the Filter

When the filter design is finished, you must tell the router where to apply the filter. Apply it as a Call Filter in the remote node that reaches your DNS server(s) (usually your ISP node). Go to Menu 11.1, Remote Node Profile, and enter the number of the filter under “Call Filter Sets” as shown in Figure 8-6. If you have multiple filters, you can cascade up to four by entering their numbers separated by commas.

Figure 8-6 shows the Remote Node Profile Menu.

```
Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP           Edit PPP Options= No
Active= Yes                    Rem IP Addr= 0.0.0.0
Call Direction= Outgoing       Edit IP= No

Incoming:                      Telco Option:
  Rem Login=                   Transfer Type= 64K
  Rem Password= *****       Allocated Budget(min)= 0
  Rem CLID= N/A                Period(hr)= 0
  Call Back= N/A

Outgoing:                      Session Options:
  My Login= netgear            Input Filter Sets=
  My Password= *****        Output Filter Sets=
  Authen= CHAP/PAP             Call Filter Sets= 1 <<- APPLY
  Pri Phone #= 18005551212     Idle Timeout(sec)= 300
  Sec Phone #=

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

**Figure 8-6. Remote Node Profile Menu**

When you finish, restart the router.

# Chapter 9

## System Maintenance

The Model RT328/RH348 router provides diagnostic tools for maintenance. These diagnostic tools include displays of system status, ISDN B channel status, log and trace capabilities, and upgrades to the system software. This chapter describes the use of these tools.

### System Status

---

The System Maintenance Status Menu (Menu 24.1) allows the user to monitor the operation of the router. This screen displays the current status of the ISDN telephone line and the Ethernet port, and it counts the number of packets sent and received. It also displays the system software version.

Enter 24 from the Main Menu to display the System Maintenance Menu. Then enter 1 to display Menu 24.1 - System Maintenance Status Menu. Table 9-1 lists the commands used in the System Maintenance Status Menu.

**Table 9-1. System Maintenance Status Menu Fields**

Command	Field Name	Description
Enter 1	Discon B1	This field disconnects the current B1 channel call.
Enter 2	Discon B2	This field disconnects the current B2 channel call.
Enter 3	Reset counters	This field resets the counters.
[Esc]		Pressing [Esc] exits the screen.

Table 9-2 lists the fields for Menu 24.1 - System Maintenance Status. These fields are read-only fields.

**Table 9-2. System Maintenance Status Menu Fields**

Field	Description
ISDN:	This field displays the statistics for B1 and B2 channels. For each channel the screen displays:
Link	The remote node the channel is currently connected to, or the status of the channel (Idle, Calling, or Answering).
Type	The current connecting speed (56 K or 64 K).
TXPkt	The number of packets transmitted on this channel since reset or manual clear.
RXPkt	The number of packets received on this channel since reset or manual clear.
Error	The number of error packets on this channel since reset or manual clear.
CLU	The current line utilization—percentage of current bandwidth used on this channel.
ALU	The average line utilization —average CLU for this channel.
Up Time	The time that this channel has been connected to the current remote node.
Total Outcall Time	The total outgoing call time for both B1 and B2 channels since the system has been powered on. Note that the time is shown in B-channel hours. When both B channels are active simultaneously, the values in this field will increase at twice real time.
Ethernet:	This field displays the current status of the LAN connection on your router.
Status	This field displays the current status of the LAN port.
TX Pkt	This field displays the number of transmitted packets to LAN.
RX Pkt	This field displays the number of received packets from LAN.
Collision	This field displays the number of collisions.
Name	This field displays the name of your router, which you configured in Menu 1 - General Setup.
RAS S/W Version	This field displays the version of the current router software.
ISDN F/W Version	This field displays the version of the current ISDN firmware.
Ethernet Address	This field displays the Ethernet MAC address assigned to your router.



**Table 9-2. System Maintenance Status Menu Fields (continued)**

Field	Description
Country Code	This field displays the one-byte country code value (in decimal notation). For example, 255 indicates North America.
LAN Packet Which Triggered Last Call	This field displays the first 48 octets of the LAN packet that triggered the last outgoing call. Two types of packets are displayed: IP and RAW. By viewing the packet information, you can determine which station has sent a packet to cause the router to make an outgoing call.

Figure 9-1 illustrates two packet examples shown on Menu 24.1. The first is an ICMP Ping packet (Type: IP) triggering the call, and the second is a SAP broadcast packet (Type: RAW). With this information, you can determine the source IP address (C0 44 87 22) of the packet or the source MAC address (00 40 95 90 04 B9) of the packet.

```

LAN Packet Which Triggered Last call: (Type: IP)
45 00 00 3C 02 12 00 00 38 01 36 49 00 00 00 00 C0 44 87 22 08 00 62 2B
20 04 00 00 00 08 A9 D0 C0 44 87 22 00 01 02 03 04 05 06 07 08 09 0A 0B

LAN Packet Which Triggered Last Call: (Type: Raw)
FF FF 00 22 00 11 00 00 00 00 FF FF FF FF FF FF 04 52 00 00 00 00 00 40
95 90 04 B9 40 08 00 03 02 78 01 A5 A5 A5 A5 A5 A5 A5 A5

```

**Figure 9-1. Packet Examples**

## Terminal Baud Rate

You can change the baud rate of the serial Manager connection through Menu 24.2, Terminal Baud Rate. The router supports 9600 (default), 19200, and 38400 bits per second (bps) for the RS-232 connection.

To change the rate, toggle the selection using the space bar. When the desired rate is shown, press [Enter]. You are given the opportunity to change the baud rate of your terminal before continuing.

## Log and Trace

---

Log and trace tools allow the user to view the error logs and trace records in order to troubleshoot any errors that may occur. The router can also generate system logs (syslogs) to send to other machines.

Enter 24 to display Menu 24 - System Maintenance. Enter 3 to select the Log and Trace option and display Menu 24.3 - System Maintenance - Log and Trace.

Table 9-3 lists the fields and commands for Menu 24.3 - System Maintenance - Log and Trace.

**Table 9-3. System Maintenance - Log and Trace Menu Fields**

Command	Field
Enter 1	View Error Log
Enter 2	Syslog and Accounting

### View Error Log

Select the first option from Menu 24.3 - System Maintenance - Log and Trace to display the Error Log in the system. Use the space bar to scroll this screen if necessary. After each display, you are prompted with an option to clear the Error Log. Enter the appropriate choice and press [Enter].

### Syslog and Accounting

Syslog and Accounting can be configured in Menu 24.3.2 - System Maintenance - Syslog and Accounting. Menu 24.3.2 configures the router to send UNIX system logs to another machine.

You must configure the parameters to activate syslog (Table 9-4).

**Table 9-4. System Maintenance - Syslog and Accounting Menu Fields**

Field	Command	Description
Active	Press the space bar to toggle between yes and no.	The syslog option is turned on or off.
Syslog IP Address	Enter the address in dotted-decimal notation such as a.b.c.d where a, b, c, and d are numbers between 0 and 255.	This field is the IP address location to send your syslog.
Log Facility	Press the space bar to toggle between on and off.	Seven different local options can be selected. This feature is used for UNIX applications.

The router sends three different types of syslog messages:

- Call information messages (CDR)
- Error information messages
- Session information messages

Examples of these messages are as follows:

- 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
```

## Diagnostic Menu

---

The diagnostic menu allows you to test several functions of your router. From the Main Menu, enter 24 to display Menu 24 - System Maintenance. Enter 4 to display Menu 24.4 - System Maintenance - Diagnostic.

The diagnostic tools described in this section allow the user to perform the following functions:

- Test the ISDN connection
- Test the TCP/IP configuration
- Reboot the system
- Change the interface mode to command-line mode

## ISDN Tools

Use the commands and fields listed in Table 9-5 to test the ISDN connection from Menu 24.4 - System Maintenance - Diagnostic.

**Table 9-5. System Maintenance - Diagnostic Menu Fields**

Field	Command	Description
Hang Up B1 Call	[Enter 1]	This command hangs up B channel 1. It is useful only if the B1 line is currently connected to a remote node or a dial-in user.
Hang Up B2 Call	[Enter 2]	This command hangs up B channel 2. It is useful only if the B2 line is currently connected to a remote node or a dial-in user.
Reset ISDN	[Enter3]	This command reinitializes the ISDN link to the telephone company.
ISDN Connection Test	[Enter 4]	This command instructs the router to perform a loopback test of the ISDN line. A call is placed from one B channel to the other, and data is passed. A failure of this test indicates a problem either with the ISDN line itself or with your current ISDN configuration. Note the error message that you receive and see your network administrator.
Manual Call	[Enter 5]	This command allows the user to place a manual call to a remote node and tests the connectivity to that remote node. As the call is placed, traces are displayed on the screen showing the progress of the call setup and protocol negotiation.

Figure 9-2 illustrates an example of a trace display for a successful call when using a TCP/IP protocol connection.

```
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 9-2. Trace Display for a Successful TCP/IP Protocol Connection**

Figure 9-3 shows an example of a trace display for a failed call when using a TCP/IP protocol connection.

```
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 Terminate REQ
LCP down
Line Down chan<2>
```

**Figure 9-3. Trace Display for a Failed TCP/IP Protocol Connection**

## TCP/IP Tools

Enter 11 to select the Internet Setup Test. This test checks to see if your Internet access configuration has been done correctly. The router dials the ISP, performs authentication, and establishes a connection. If everything is working properly, you receive an appropriate response. If you receive an error message, note the error message and consult your network administrator.

Enter 12 to select Ping Host. This diagnostic test pings a local or remote host. You are prompted for the IP address of the host.

## System Tools

Enter 21 to select Reboot System. Your system is rebooted, implementing any changes that may have been recently added to your system.

Enter 22 to select Command Interpreter Mode. This option changes the Manager interface on your router from the screen-based mode to a command line mode. The command line mode allows you to configure, diagnose, and test your router using a specified set of commands. This mode is capable of executing user-defined scripts sent from the terminal. For more information, refer to "Command Interpreter Mode," on page 9-9.

## Back Up Configuration

---

Select option 5 from Menu 24 - Maintenance to back up the current configuration settings of your router onto a disk. NETGEAR highly recommends backing up your router configuration after it is functioning.

The procedure for downloading varies depending on the type of terminal software used to access the router. Your terminal software must have the ability to transfer data using the XMODEM Protocol to perform the backup. A backup is possible only through the serial cable connection.

## Restore Configuration

---

Select option 6 from Menu 24 - Maintenance to reload a previously backed up configuration from a disk to the router. The configuration is stored in the internal flash ROM of your router and is retained even if a power failure occurs.

The procedure for uploading varies depending on the type of terminal software used to access the router. Your terminal software must have the ability to transfer data using the XMODEM Protocol to perform the upload. Restoring a configuration is possible only through the serial cable connection.

## Software Update

---

Software updates are possible only through the serial cable connection. You cannot use the Telnet Protocol to update the software version of your router. Your serial communications software must have the ability to transfer data using the XMODEM Protocol.



**Caution:** This procedure deletes the existing software before installing the new software. Do not attempt to use this menu unless you have the new software version.

To update the software:

**1. Select Menu 24 - System Maintenance.**

**2. Enter 7 to select Software Update.**

A message is displayed asking if you want to continue.

**3. Press y and wait for the Debug Mode command prompt.**

**4. Enter the command atur and wait.**

After about 30 seconds, the router displays the Starting XMODEM upload... message.

**5. Transfer the new software file to the router using the XMODEM Protocol of your serial communications software.**

**6. Enter the command atgo to restart the router when the router displays the OK message.**



**Note:** NETGEAR recommends that you change the Manager port baud rate to 38400 before updating the software. Doing so results in an update time of 5 to 10 minutes.

## Command Interpreter Mode

---

Select option 8 from Menu 24, Maintenance, to enter the command interpreter mode. This mode allows you to diagnose, test, and configure your router using a script or 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 at <http://NETGEAR.baynetworks.com>.

## Call Control

---

The Model RT328/RH348 router provides call control management functions for the remote node and remote dial-in user. These functions are budget management, blacklist, and call history, which are on the Call Control menu. Select option 9 from Menu 24 to display the Call Control menu.

### Blacklist

The blacklist function prevents the router from redialing an unreachable phone number (a number to which it has been unable to connect). The router maintains a list of phone numbers (up to a maximum of 14) to which it will not make an outgoing call. When the router attempts to dial a phone number and fails a certain number of times (configurable in Menu 24.9.1), the phone number is put onto the blacklist. You must restore the number manually before it can be dialed again. You can remove a phone number from the list by entering its index number at the Remove Selection prompt.

### Budget Management

The budget management function provides a way for you to set a limit on ISDN utilization to prevent any accidental overuse. This function limits the total outgoing call time of the router over a period of time to each remote node and remote dial-in user (callback only). When this limit is reached, the call is dropped and further outgoing calls to that remote node or remote dial-in user (callback) fail. If the total outgoing call time exceeds the set limit, future outgoing calls are not made and the current call is dropped. After each total period, the total budget is reset. The default for the total budget is 0 minutes, and the total period is 0 hours. These values disable budget control. You can reset the total outgoing call time through the Call Control menu. The total outgoing call timer can be programmed to reset itself periodically through menus 11 and 13.



## Call History

The call history function displays statistics of data calls to or from up to the first 10 phone numbers seen. The following statistics are shown:

- Phone number
- Direction (incoming or outgoing)
- Data rate
- Number of calls
- Call time (maximum, minimum, and total)

This information is erased when the router is reset.

## Call Control Parameters

General call control parameters are configured in Menu 24.9.1 - Call Control Parameters. The following parameters are general call control parameters:

- **Dialer Timeout: Digital Call (sec)**  
The router gives up if it cannot set up an outgoing digital call within the timeout value. The default is 30 seconds.
- **Retry Counter**  
This parameter counts how many times a busy or no-answer phone number is tried before it is put on the blacklist. The default value of 0 disables the blacklist control.
- **Retry Interval (sec)**  
This parameter specifies the waiting period after a call fails before the call is tried again. This waiting period applies before a phone number is blacklisted.



---

# Chapter 10

## Troubleshooting

This chapter gives information about troubleshooting your Model RT328/RH348 router. After each problem description, instructions are provided to help you diagnose and solve the problem.

### Basic Functioning

---

After you turn on power to the router, the PWR LED lights. If the PWR LED does not light, refer to the next section, “LEDS.” After the PWR LED lights, the router performs a self-test for 10 seconds. This self-test includes turning all of the ISDN LEDs on. After this self-test, the Test LED should begin to blink at a rate of about 0.5 Hz. If these steps do not occur, refer to “Test LED,” on page 10-2.

If the Ethernet connection is made, the LAN Link LED should be on. If the LAN Link LED is off, refer to “LAN Link LED,” on page 10-2.

If your router has been configured, the ISDN D LED should turn on within the first two minutes of operation. If not, refer to “Troubleshooting the ISDN Line,” on page 10-2.

### LEDS

If the LEDs are off when your router is turned on, make sure that the power cord is properly connected to your router and that the power supply adapter is properly connected to a functioning power outlet. Check that the power switch on the router is in the on position. If the error persists, you have a hardware problem and should contact technical support.

## Test LED

When the router has been turned on for about 10 seconds, the Test LED blinks at a rate of about 0.5 Hz. If the Test LED does not blink, or if it stops blinking, there is a fault within the router. Cycle the power and see if it recovers. If the error persists, you might have a hardware problem and should contact technical support.

## LAN Link LED

If the LAN Link LED does not light when the Ethernet connection is made, check the following:

- Physical Ethernet cables

Make sure that the connections are secure at the router and at the hub or workstation.

- Connected hub or workstation

Make sure that the connected hub or workstation is powered on.

- Configuration of the router

Make sure that you configured the router to use the correct Ethernet interface (AUI or UTP) for your LAN connection. The factory default interface for a router that is not configured is the UTP port.

- Correct Ethernet cable

If you are connecting a Model RT328 router directly to a workstation or to the uplink (MDI) port of a hub, use the red crossover cable. If you are connecting a Model RT328 router to a normal (MDI-X) hub port, use the white straight-through cable.

Workstations should be connected to the Model RH348 router hub ports using straight-through cables.

## Troubleshooting the ISDN Line

---

Within the first two minutes after power is turned on to the configured router, the ISDN D LED should light. If the LED does not light, check the physical connection of the ISDN line, referring to the installation information in this guide.

If the physical connection is correct, the problem should be diagnosed using the internal Manager interface. Refer to instructions in this guide regarding the use of the Manager interface.

The following two sections explain how to examine the ISDN initialization results and how to perform an ISDN loopback test to verify operation with the phone company.

## ISDN Initialization or Reset

During the power-on initialization, during manual ISDN reset through the diagnostic menu, or when attempting to save the parameters entered in Menu 2, you might receive this message:

```
Failed to initialize ISDN
```

If this message is displayed, check the error log in Menu 24.3.1. There is a log entry for the ISDN initialization failure in the message:

```
ISDN init failed. code<n>....
```

The code number n will be 1, 2, or 3. Refer to the corresponding instructions in Table 10-1.

**Table 10-1. Code Numbers for Failed ISDN Initialization**

Code Number	Description	Malfunction and Troubleshooting Instructions
1	The ISDN link is not up.	Either the ISDN line is not properly connected to the router or the ISDN line is not activated. Verify that the ISDN cable is connected to the router and also to the wall outlet (to the telephone company). Confirm that the ISDN line has been activated by the telephone company.
2	There is an SPID error (North America only).	The SPIDs that you entered in menu 2 might not be correct. If these are correct, initialize again from menu 24.4.3.
3	There is a general failure.	The provisioning information for your switch might not be correct. Contact your telephone company to verify the provisioning information for your switch and verify the SPIDs in Menu 2 (applies to North America only).

## ISDN Loopback Test

If the ISDN initialization has passed, the loopback test should also pass. This test may be executed from Menu 24.4, where it is shown as test 4, ISDN Connection Test. If test 4 fails, verify the phone numbers that you entered in Menu 2. The loopback test dials the number entered in the second phone # field (except for switch types with only one phone number). If you are required to dial a prefix (for example, 9) to get an outside line, you must enter the prefix with the phone number (for example, 95551212 or 914085551212). If it is an internal line, you might need to enter only the last four or five digits depending on your internal dialing plan (for example, 51212).

## Troubleshooting a TCP/IP Network Using a Ping Utility

---

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. Troubleshooting a TCP/IP network is made very easy by using the ping utility in the built-in Manager interface (Menu 24.4) or in your PC or workstation.

### Testing the LAN Path to Your Router

To verify that the LAN path to your router is set up correctly, from the Windows 95 (or Windows NT®) run menu, type Ping and the IP address of the router. Press the Enter key.

You should see a message like this one:

```
Pinging <IP address> with 32 bytes of data
```

If the path is working, you see this message:

```
Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
```

If the path is not working, you see this message:

```
Request timed out
```

If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections
  - Make sure the LAN Link LED is on. If the LAN Link LED is off, follow the instructions in “LAN Link LED” on page 10-2.
  - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
- Wrong network configuration
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
  - Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

## Testing the Path from Your PC to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device. From the Windows run menu, type PING -n 10 followed by the IP address of the remote device you are calling.

If the path is functioning correctly, the B1 or B2 LED on the router should turn on, indicating that a call is being placed. If the B1 or B2 LEDs do not turn on, follow these instructions:

- Check that your PC has the IP address of your router listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in the control panel network utility. Go to the Run... window and run winipcfg. The IP address of the router should appear as the Default Gateway.
- Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check Menu 12 and verify that at least one static route exists.

As the ISDN call is being set up, your PC should display a few timeouts followed shortly by replies. If the path is not functioning correctly, only timeouts are displayed. This response indicates that the router is unable to establish a PPP connection with the remote LAN. Refer to the next section, "Troubleshooting a Remote Node or ISP Connection."

## Troubleshooting a Remote Node or ISP Connection

---

To troubleshoot a remote node or an ISP connection, follow these instructions:

- Check Menu 24.1 to verify the ISDN status. If the menu indicates the ISDN status as down, then refer to "Troubleshooting the ISDN Line," on page 10-2.
- Place a manual call to the remote node, using Menu 24.4.5. The progress of the call is displayed on the screen. If the call does not connect, verify the following parameters in Menu 11:
  - Pri(mary) Phone #
  - Sec(ondary) Phone #
  - Transfer Rate

- Verify your IP address in Menu 3.2 and verify the following parameters in Menu 11:
  - My Login
  - My Password
  - Rem IP Addr

If the call is connected but quickly terminated, it indicates the possibility of a negotiation problem.

- Check the error log in Menu 24.3.1, which usually provides some indication of why the call was dropped. If there is nothing in the log, the call may have been dropped by the remote device. Verify that the configuration parameters between these two devices are consistent.

If you are still unable to determine the problem, refer to Appendix D, “Using the Protocol Analyzer and Trace Tools.”

## Troubleshooting a Remote User Connection

---

To troubleshoot a remote user connection, follow these instructions:

- Verify that you configured the authentication parameters in Menu 13. These parameters are:
  - CLID Authen
  - Recv Authen
  - Mutual Authen
- Verify that the IP address is supplied correctly in Menu 13 if the remote dial-in user is negotiating IP. Check that the remote dial-in user is supplying a valid IP address and that the router is assigning a valid address from the IP pool.
- Verify the user name and password for the remote dial-in user in Menu 14.

If you are still unable to determine the problem, refer to Appendix D, “Using the Protocol Analyzer and Trace Tools.”



## Troubleshooting the Manager Interface

---

Refer to the following instructions if you cannot access the Manager interface by the serial port or by using the Telnet Protocol.

If you cannot access the Manager interface by the serial port, follow these instructions:

- Verify that the router is connected to the serial port of your terminal or computer using the included cable.
- Check the configuration parameters of your terminal or communications program. The connection should be configured as follows:
  - VT100 terminal emulation
  - 9600 baud rate (unless this setting has been changed previously in the router setup)
  - No parity, 8 data bits, 1 stop bit

If you cannot access the Manager by using the Telnet Protocol, refer to “Testing the LAN Path to Your Router,” on page 10-4.

## Testing the Phone Ports

---

To test the phone ports, lift the telephone handset when there are no calls in progress. You should hear a dial tone, and the LED for that phone port should be on. If there is no dial tone, the line may be configured incorrectly. Check with your telephone company to make sure that your ISDN line is configured for both data and voice.

## Restoring the Default Configuration and Password

---

The user can erase the current configuration and restore factory defaults by uploading the utility file romfile0, which can be found in the directory in which FirstGear was installed. It is also available on the NETGEAR Web site. This procedure will restore the Manager password to 1234 and will set the Manager baud rate to 9600. This recovery method is for cases when the Manager password is not known.

To upload romfile0, you must enter the BootModule debug mode with a serial connection to the Manager port:

**1. While monitoring the serial port, turn on the router. Wait for the following message:**

Press Any key to enter Debug Mode within 3 seconds...

**2. Press any key and wait for the following message:**

Enter Debug Mode

**3. (Optional) Type atba1 to change the baud rate atba1of the router to 38.4k, and then change the baud rate of your terminal.**

Changing the baud rate may be necessary if the file transfer is unreliable at 9600 baud.  
(Note: The character after atba is the number 1.)

**4. Type atur3 and wait for the following messages:**

Now erase flash ROM for uploading ...  
Starting XMODEM upload.....

**5. From your terminal program, send the binary file romfile0 using XMODEM transfer protocol. Wait for the following message:**

Programming successful....

**6. Restart the router.**

# Appendix A

## Technical Specifications

This appendix provides technical specifications for the Model RT328/RH348 router.

### General Specification

---

#### Network Protocol and Standards Compatibility

WAN Protocols:	PPP, Multilink PPP, BACP
Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP
ISDN Standard:	National ISDN-1 (North America) AT&T 5ESS Custom (North America) Nortel DMS-100 (North America) EuroISDN DSS1, NET-3 (Europe) NTT INS-Net64 (Japan)

#### Security

PAP, CHAP, Caller ID

#### Data Compression

Hi/fn (Stac LZS) Compression with CCP

### Power Adapter

North America:	120V, 60 Hz, input
United Kingdom:	240V, 50 Hz, input
Europe:	230V, 50 Hz, input
Japan:	100V, 50/60 Hz, input
All regions (output):	16 V AC @ 1A output, 22W maximum

### Physical Specifications

Dimensions:	253 by 181 by 35 mm 9.95 by 7.1 by 1.4 in.
Weight:	1.1 kg 2.5 lb.

### Environmental Specifications

Operating temperature:	0 to 40° C
Operating humidity:	90% maximum relative humidity, noncondensing

### Electromagnetic Emissions

Meets requirements of:	FCC Part 15 Class B VCCI Class 2 EN 55 022 (CISPR 22), Class B
------------------------	--

### Interface Specifications

LAN:	UTP (10BASE-T), RJ-45 AUI, DB15F
ISDN:	S/T interface, RJ-45 (requires external NT1) or U Interface, RJ-45 (NT1 built-in)
Analog:	Voice/fax/modem, RJ-11, 3 REN (Ring Equivalents)
Manager:	RS-232, DB9F

# Appendix B

## Ordering ISDN Lines

Use the information in this section to order your ISDN line. If you have already installed your ISDN line, you can check the following information to make sure that you can use all the features of your Model RT328/RH348 router.

### Ordering the Line

---

To order your ISDN line:

- 1. Contact the ISDN Ordering Center of your local telephone company to find out what type of ISDN service is available.**
- 2. Provide your telephone company with the proper provisioning information.**

Refer to the next sections to determine the provisioning information for the appropriate switch type and ISDN service.

- 3. Obtain configuration information from the telephone company.**

When the telephone company installs your ISDN line, make sure you obtain the following information:

- ISDN switch type and protocol
- ISDN telephone number(s)
- ISDN Service Profile Identifier (SPID) number(s) (only for North America)

Table B-1 summarizes the different switch types supported by your router and the related information about the switch types (number of phone numbers and SPID numbers). The information in this table refers to a “common” case and is recommended for such a case. However, exceptions still exist to these figures. You can locate the provisioning information for the appropriate North American switch type in the next sections.

**Table B-1. Switch Types Supported**

Switch Type	Region	No. of Phone #s	No. of SPIDs
AT&T 5ESS NI-1	North America	2	2
AT&T 5ESS Point to Point	North America	1	0
AT&T 5ESS Multipoint	North America	2	2
Northern Telecom NI-1	North America	2	2
Northern Telecom Custom	North America	2	2
DSS1	Europe, Asia	2	N/A

---

## Provisioning for Switches in North America

---

For North America, the Model RT328/RH348 router has been approved by Bellcore and has the IOC (ISDN Ordering Code) “S” Capability, EZ-ISDN1. Ordering your ISDN line in this configuration provides basic data and voice service. If you wish to use any advanced calling features such as call waiting, you need to order a higher level of service such as IOC “U.” In particular, you need to have ACO (Additional Call Offering) provisioned in order to use call waiting or incoming call bumping. If your telephone company is not familiar with the IOC ordering codes, ask them what type of switch you will be connected to and whether it is provisioned for National ISDN or a custom protocol. Use the information under each switch to order your ISDN line.

### Provisioning for AT&T 5ESS Switch

The AT&T 5ESS switch supports three types of ISDN service: National ISDN-1 (NI-1), Multipoint, and Point-to-Point.

Table B-2 lists the provisioning features and settings for National ISDN-1 services when using the AT&T 5ESS switch.

**Table B-2. Provisioning Features and Settings for National ISDN-1 Services**

Provisioning Feature	Setting
Term Type	A
Circuit Switched Voice (CSV)	1
CSV Additional Call Offering (ACO)	Unrestricted
CSV limit	2
CSV Notification Busy (NB) limit	1
Circuit Switched Data (CSD)	1
CSD Additional Call Offering (ACO)	Unrestricted
CSD limit	2
CSD Notification Busy (NB) limit	1
MTERM	2

Table B-3 lists the provisioning features and settings for multipoint ISDN services when using the AT&T 5ESS switch.

**Table B-3. Provisioning Features and Settings for Multipoint Service**

Provisioning Feature	Setting
Term Type	D
Call Appearances (CA)	1
CA Quantity	1
Circuit Switched Voice (CSV)	1
CSV Flexible Call Offering (FCO)	Unrestricted
CSV limit	2
CSV Notification Busy (NB) limit	1
Circuit Switched Data (CSD)	1
CSD Flexible Call Offering (FCO)	Unrestricted
CSD limit	2
CSD Notification Busy (NB) limit	1
MTERM	2

Table B-4 lists the provisioning features and settings for Point-to-Point ISDN services when using the AT&T 5ESS switch.

**Table B-4. Provisioning Features and Settings for Point-to-Point Service**

<b>Provisioning Feature</b>	<b>Setting</b>
Term Type	A
Call Appearances (CA)	1
CA Quantity	1
Circuit Switched Voice (CSV)	1
CSV Flexible Call Offering (FCO)	Unrestricted
CSV limit	2
CSV Notification Busy (NB) limit	1
Circuit Switched Data (CSD)	1
CSD Flexible Call Offering (FCO)	Unrestricted
CSD limit	2
CSD Notification Busy (NB) limit	1
MTERM	2

## Provisioning for Northern Telecom Switch

The Northern Telecom switch type supports two types of ISDN service, National ISDN-1 and Custom. Table B-5 lists the provisioning features and settings for National ISDN-1 services when using the Northern Telecom switch.



**Table B-5. Provisioning Features and Settings for National ISDN-1 Service**

Provisioning Feature	Setting
Signaling	Functional
Protocol Version Control (PVC)	2 (National ISDN-1)
TEI assignment	Dynamic
Maximum number of keys (maxkeys)	3 (1 to 64 OK)
Release key	No
Ringing indicator	No
Electronic Key Telephone System (EKTS)	Yes or No (set to opposite of ACO)
Additional Call Offering (ACO)	Yes or No (set to opposite of EKTS)
Number of call appearances	2
Notification Busy Limit	3

Table B-6 lists the provisioning features and settings for custom ISDN services when using the Northern Telecom switch.

**Table B-6. Provisioning Features and Settings for Custom ISDN Service**

Provisioning Feature	Setting
Signaling	Functional
Protocol Version Control (PVC)	1 (Custom)
TEI assignment	Dynamic
Maximum number of keys (maxkeys)	3 (1 to 64 OK)
Release key	No
Ringing indicator	No
Electronic Key Telephone System (EKTS)	Yes or No (set to opposite of ACO)
Additional Call Offering (ACO)	Yes or No (set to opposite of EKTS)



# Appendix C

## ISDN Clearing Codes

This appendix provides information about the ISDN call clearing codes returned by the network when you use your Model RT328/RH348 router. These codes may vary depending on your service provider.

### Clearing Codes

---

Table C-1 lists the ISDN call clearing codes.

**Table C-1. ISDN Call Clearing Codes**

Reason	Description
0	Undefined
1	Unallocated (unassigned number)
2	No route specified transit network
3	No route to destination
4	Channel unacceptable
6	Channel unacceptable
7	Call awarded and being delivered in an established channel
16	Normal call clearing
17	User busy
18	No user responding
19	No answer from user (user alerted)
21	Call rejected
22	Number changed

**Table C-1. ISDN Call Clearing Codes (continued)**

<b>Reason</b>	<b>Description</b>
26	Nonselected user clearing
27	Destination out of order
28	Invalid number format
29	Facility rejected
30	Response to status inquiry
31	Normal, unspecified
34	No circuit/channel not available
38	Network out of order
41	Temporary failure
42	Switching equipment congestion
43	Access information discarded
47	Resources unavailable (unspecified)
50	Requested facility not subscribed to
63	Service or option not available
84	Call identity in use
88	Incompatible destination
90	Destination address incomplete
102	Recovery on timer expired
127	Internetworking unspecified

# Appendix D

## Using the Protocol Analyzer and Trace Tools

This appendix describes the steps for using the advanced internal diagnostic tools of the Model RT328/RH348 router. These tools can be used to troubleshoot ISDN and PPP connection problems. Several basic tests can be found in the menus of the internal Manager interface, while the more advanced protocol and packet trace tools are accessible from the command line interface.

### The Diagnostic Process

---

Many router connection problems can be diagnosed using the ISDN and Remote Node connection tests in the Internal Manager Interface of the Model RT328/RH348 router. These tests can be found in Menu 24.4, System Maintenance (Diagnostic). Detailed information about using this menu can be found in Chapter 9, "System Maintenance."

To begin problem diagnosis:

**1. Execute test 4, the ISDN Connection test, from Menu 24.4.**

This test performs a data loopback call from one B channel to the other. This call serves as a basic test of your ISDN line. If this test fails, verify the ISDN hardware connection, the status of your line, and the information entered in Menu 2, ISDN Setup.

**2. Try test 5, placing a Manual Call to a Remote Node.**

This test will display some basic progress information that may be sufficient to determine the problem.

If these tests are not sufficient to diagnose a problem, you can run the more advanced protocol and packet trace tools. These tools consist of an embedded ISDN protocol analyzer and a PPP packet trace. The output of these trace tools can be captured to a file, which can then be faxed or sent by e-mail to NETGEAR support, your ISP, or your telco for analysis.

## ISDN Protocol Analyzer

---

An ISDN call connection failure can be diagnosed using the ISDN embedded protocol analyzer (EPA) of the Model RT328/RH348 router. The EPA executes from the command line interface within the internal Manager. You must first connect to the router using the serial Manager port. The EPA will not operate by Telnet.

To invoke the EPA:

1. **Access the internal Manager using a serial terminal connection.**
2. **If you will be tracing an outgoing call, go to Menu 11 (Remote Node Setup) and note which remote node number, N, corresponds to the location you will be calling.**
3. **Invoke the Command Interpreter Mode (Menu 24.8).**
4. **Turn on the screen capture/log capability:**

```
rt328> isdn ana on
```

5. **Trace the call.**

To trace an outgoing call, force the router to dial the remote node by entering:

```
rt328> isdn dial N
```

(N is the remote node number shown in Menu 11.)

Or, to trace an incoming call, enable incoming trace by entering:

```
rt328> sys event
```

6. **Wait for all progress messages, and then (if necessary) force the router to drop the ISDN connection by entering:**

```
rt328> isdn drop all
```

7. **Display the analyzer trace by entering:**

```
rt328> isdn ana disp
```

The trace appears on the screen as in Figure D-1. Use PageUp and PageDown to inspect the entire trace.

Figure D-1 shows the ISDN Protocol Analyzer Display.

```

-----Start Isdn Protocol Analyzer Display-----
Start of buffer
00:00:11.52 4 bytes LAPD D NT C SAPI=0 TEI=97 RR P/F=1 NR=6
00:00:11.53 4 bytes LAPD D TE R SAPI=0 TEI=97 RR P/F=1 NR=7
00:00:12.62 38 bytes LAPD D TE C SAPI=0 TEI=97 INFO P=0 NR=7 NS=6
    34 bytes Northern American
    Orig CR=0X03 PD=Q.931 SETUP
    1 00000100 INFORMATION ELEMENT : BEARER CAPability
    2 00000010 IE length : 2 octets
    3 1----- Extension bit : not continued
    -00----- Coding standard : CCITT
    ---01000 Info. trans. cap. : unrestricted digital information
    4 1----- Extension bit : not continued
    -00----- Transfer mode : circuit mode
    ---10000 Info. transfer rate : 64 kbit/s
    1 00011000 INFORMATION ELEMENT : CHANNEL IDentification
    2 00000001 IE length : 1 octets
    3 1----- Extension bit : not continued
    -0----- Interface ident. : implicitly identified
    --0----- Interface type : basic interface
    ---0---- Spare
    ---0--- Preferred/exclusive : preferred
-----0-- D-channel indicator : not D-Channel
    -----11 Info. chan. sel. : any channel
    1 00101100 INFORMATION ELEMENT : KEYPAD
    2 00001011 IE length : 11 octets
    3 ***** Keypad information : [Called Number]
    1 01101100 INFORMATION ELEMENT : CALLING party NUMBER
    2 00001000 IE length : 8 octets
    3 1----- Extension bit : not continued
    -00----- Type of number : unknown
    ---0000 Numbering plan : unknown
    4 ***** Number : [Directory Number 1]

00:00:12.65 4 bytes LAPD D NT R SAPI=0 TEI=97 RR P/F=0 NR=7
00:00:12.75 11 bytes LAPD D NT C SAPI=0 TEI=97 INFO P=0 NR=7 NS=7
    7 bytes Northern American
    Dest CR=0X03 PD=Q.931 CALL PROCeeding
    1 00011000 INFORMATION ELEMENT : CHANNEL IDentification
    2 00000001 IE length : 1 octets
    3 1----- Extension bit : not continued
    -0----- Interface ident. : implicitly identified
    --0----- Interface type : basic interface
    ---0---- Spare
    ---1--- Preferred/exclusive : exclusive
    ----0-- D-channel indicator : not D-Channel
    -----01 Info. chan. sel. : B1 channel

00:00:12.77 4 bytes LAPD D TE R SAPI=0 TEI=97 RR P/F=0 NR=8
00:00:13.40 11 bytes LAPD D NT C SAPI=0 TEI=97 INFO P=0 NR=7 NS=8
    7 bytes Northern American
    Dest CR=0X03 PD=Q.931 ALERTing

```

```

1 00110100 INFORMATION ELEMENT : SIGNAL
  2 00000001 IE length      : 1 octets
  3 00000001 Signal value   : ring back tone on

00:00:13.42  4 bytes LAPD    D TE R SAPI=0 TEI=97 RR   P/F=0 NR=9
00:00:13.44  11 bytes LAPD   D NT C SAPI=0 TEI=97 INFO  P=0   NR=7 NS=9
      7 bytes Northern American
      Dest CR=0X03 PD=Q.931 CONNect
1 00110100 INFORMATION ELEMENT : SIGNAL
  2 00000001 IE length      : 1 octets
  3 00111111 Signal value   : tones off

00:00:13.46  4 bytes LAPD    D TE R SAPI=0 TEI=97 RR   P/F=0 NR=10
00:00:13.47  8 bytes LAPD   D TE C SAPI=0 TEI=97 INFO  P=0   NR=10 NS=7
      4 bytes Northern American
      Orig CR=0X03 PD=Q.931 CONNect ACKnowledge

00:00:13.49  4 bytes LAPD    D NT R SAPI=0 TEI=97 RR   P/F=0 NR=8
00:00:24.65  4 bytes LAPD    D NT C SAPI=0 TEI=88 RR   P/F=1 NR=2
00:00:24.66  4 bytes LAPD    D TE R SAPI=0 TEI=88 RR   P/F=1 NR=3
00:00:36.14  12 bytes LAPD   D TE C SAPI=0 TEI=97 INFO  P=0   NR=10 NS=8
      8 bytes Northern American
      Orig CR=0X03 PD=Q.931 DISConnect
  1 00001000 INFORMATION ELEMENT : CAUSE
  2 00000010 IE length      : 2 octets
  3 1----- Extension bit   : not continued
    -00----- Coding standard : CCITT
    ---0---- Spare
    ---0000 Location         : user
  4 1----- Extension bit   : not continued
    -0010000 Cause value     : Normal call clearing

00:00:36.16  4 bytes LAPD    D NT R SAPI=0 TEI=97 RR   P/F=0 NR=9
00:00:36.36  8 bytes LAPD   D NT C SAPI=0 TEI=97 INFO  P=0   NR=9 NS=10
      4 bytes Northern American
      Dest CR=0X03 PD=Q.931 RELease

00:00:36.38  4 bytes LAPD    D TE R SAPI=0 TEI=97 RR   P/F=0 NR=11
00:00:36.39  8 bytes LAPD   D TE C SAPI=0 TEI=97 INFO  P=0   NR=11 NS=9
      4 bytes Northern American
      Orig CR=0X03 PD=Q.931 RELease COMPLETE

00:00:36.41  4 bytes LAPD    D NT R SAPI=0 TEI=97 RR   P/F=0 NR=10
End of buffer

```

Figure D-1. ISDN Protocol Analyzer Display



## Packet Tracing

---

You can diagnose PPP connection failures using the packet trace feature of the Model RT328/RH348 router.

To invoke the packet trace:

1. **Access the internal Manager of the router using a serial or Telnet terminal connection.**
2. **If you will be tracing an outgoing call, go to Menu 11 (Remote Node Setup) and note which remote node number, N, corresponds to the location you will be calling.**
3. **Invoke the Command Interpreter Mode (Menu 24.8).**
4. **Clear any existing trace information by entering:**

```
rt328> sys trcl cl
```

5. **Turn on the trace log by entering:**

```
rt328> sys trcl sw on
```

6. **Turn on the packet trace by entering:**

```
rt328> sys trcp sw on
```

7. **Trace the call.**

To trace an outgoing call, force the router to dial the remote node by entering:

```
rt328> isdn dial N
```

(N is the remote node number shown in Menu 11.)

Or, to trace an incoming call, enable incoming trace by entering:

```
rt328> sys event
```

8. **Wait for the desired activity, and then display the trace log by entering:**

```
rt328> sys trcl disp
```

The trace appears on the screen as in Figure D-2. Use PageUp and PageDown to inspect the entire trace.

```
rt328> sys trcl c1
Program Trace Switch OFF
rt328> sys trcl sw on
rt328> sys trcp sw on
rt328> isdn dial 1
Start dialing for node<1>
Dialing chan<1> phone(last 9-digit):40201
### Hit any key to continue.###

Call CONNECT speed<64000> chan<1> prot<1>
LCP up
CHAP send response
CHAP login to remote OK!
IPCP negotiation started
BACP negotiation started
BACP up

<<< ----- user strikes a key to get a prompt
rt328> sys trcl disp
102 fe3792 15e PDI1 dialer Dialing chan<1> phone(last 9-digit):40201
103 fe3ea4 169 PDI1 dialer Call CONNECT speed<64000> chan<1> prot<1>
104 fe3eb8 0 POU1 ebp=4aa00,seqNum=17 PPP1-XMIT:24 len:40
0000: ff 03 c0 21 01 12 00 24 01 04 05 f4 02 06 00 00
0010: 00 00 08 02 0d 03 06 11 04 05 f4 13 09 03 00 a0
105 fe3f30 0 PNET ebp=4aa30,seqNum=18 PPP1-RCV:24 len:42
0000: ff 03 c0 21 01 30 00 26 01 04 05 f4 02 06 00 00
0010: 00 00 03 05 c2 23 05 08 02 11 04 05 f4 13 09 03
106 fe3f3a 0 POU1 ebp=4aa60,seqNum=19 PPP1-XMIT:24 len:42
0000: ff 03 c0 21 02 30 00 26 01 04 05 f4 02 06 00 00
0010: 00 00 03 05 c2 23 05 08 02 11 04 05 f4 13 09 03
107 fe3f44 0 PNET ebp=4aa90,seqNum=1a PPP1-RCV:24 len:40
0000: ff 03 c0 21 02 12 00 24 01 04 05 f4 02 06 00 00
0010: 00 00 08 02 0d 03 06 11 04 05 f4 13 09 03 00 a0
108 fe3f44 186 PNET ppp LCP up
109 fe3fc6 0 PNET ebp=4aac0,seqNum=1b PPP1-RCV:24 len:15
0000: c2 23 01 11 00 0d 08 00 00 48 e4 00 04 fc 6c
110 fe3fc6 190 PNET ppp CHAP send response
111 fe3fd0 0 POU1 ebp=4aaF0,seqNum=1c PPP1-XMIT:24 len:28
0000: c2 23 02 11 00 1a 10 ce f1 4c 9f fe 01 a9 85 04
0010: bb 0b 51 e5 17 3e 5e 50 32 38 36 34
112 fe4002 0 PNET ebp=4ab20,seqNum=1d PPP1-RCV:24 len:13
0000: c2 23 03 11 00 0b 57 65 6c 63 6f 6d 65
113 fe4002 195 PNET ppp CHAP login to remote OK!
114 fe400c 0 PNET ebp=4ab50,seqNum=1e PPP1-RCV:24 len:8
0000: c0 29 01 32 00 06 01 02
115 fe400c 0 POU1 ebp=4ab80,seqNum=1f PPP1-XMIT:24 len:8
0000: c0 29 02 32 00 06 01 02
116 fe402a 0 PNET ebp=4abb0,seqNum=20 PPP1-RCV:24 len:8
0000: c0 29 03 32 00 06 01 02
117 fe4034 225 PNET ppp IPCP negotiation started
118 fe403e 0 POU1 ebp=4abe0,seqNum=21 PPP1-XMIT:24 len:18
0000: 80 21 01 12 00 10 02 06 00 2d 0f 01 03 06 cc f7
0010: cb b7
```

```
119 fe403e 2d7 PNET ppp      BACP negotiation started
120 fe4048 0 POU1 ebp=4ac10,seqNum=22 PPP1-XMIT:24 len:12
0000: 80 71 01 13 00 0a 01 06 00 00 00 01
121 fe4048 0 PNET ebp=4ac40,seqNum=23 PPP1-RCV:24 len:12
0000: 80 2b 01 16 00 0a 01 06 00 00 00 00
122 fe4048 0 POU1 ebp=4ac70,seqNum=24 PPP1-XMIT:24 len:20
0000: ff 03 c0 21 08 13 00 10 80 2b 01 16 00 0a 01 06
0010: 00 00 00 00
123 fe4052 0 PNET ebp=4aca0,seqNum=25 PPP1-RCV:24 len:12
0000: 80 71 01 17 00 0a 01 06 ff ff ff ff
124 fe4052 0 POU1 ebp=4acd0,seqNum=26 PPP1-XMIT:24 len:12
0000: 80 71 02 17 00 0a 01 06 ff ff ff ff
125 fe405c 0 PNET ebp=4ad00,seqNum=27 PPP1-RCV:24 len:26
0000: ff 03 c0 21 08 33 00 16 80 21 01 12 00 10 02 06
0010: 00 2d 0f 01 03 06 cc f7 cb b7
126 fe4066 0 PNET ebp=4ad30,seqNum=28 PPP1-RCV:24 len:12
0000: 80 71 02 13 00 0a 01 06 00 00 00 01
127 fe4066 2d8 PNET ppp      BACP up
Program Trace Switch OFF
Packet Trace Switch OFF
rt328>
```

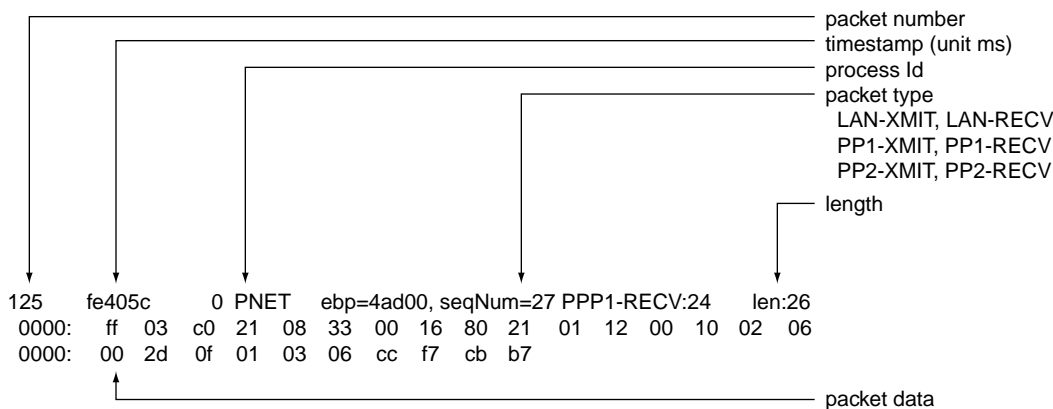
**Figure D-2. Trace Screen**

## Packet Trace Display Format

Data packets are time stamped and displayed up to the first 32 bytes. PPP message packets are summarized, but their contents are not displayed. The format of the packet trace display is shown in the following packet example:

```
125 fe405c 0 PNET ebp=4ad00,seqNum=27 PPP1-RECV:24 len:26
```

Figure D-3 breaks down and defines the packet trace display for the preceding packet example.



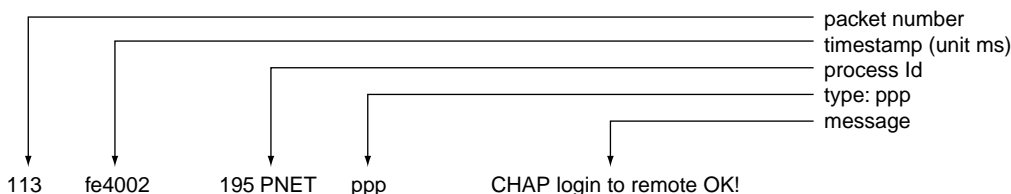
8439EA

**Figure D-3. Packet Trace Display Definitions**

The following is an example of the PPP message format:

```
113 fe4002 195 PNET ppp CHAP login to remote OK!
```

Figure D-4 breaks down and defines the PPP message format for the preceding packet example.



8440EA

**Figure D-4. PPP Message Definitions**

# Glossary

<b>10BASE-T</b>	IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.
<b>AUI</b>	<i>See</i> attachment unit interface.
<b>attachment unit interface</b>	A 15-pin connector for attaching an Ethernet transceiver.
<b>B channel</b>	A 64 Kbps “Bearer” channel used to carry voice or data over the ISDN network.
<b>BACP</b>	<i>See</i> Bandwidth Allocation Control Protocol.
<b>BRI</b>	<i>See</i> Basic Rate Interface.
<b>Bandwidth Allocation Control Protocol</b>	An extension to the Point-to-Point Protocol (PPP) for dynamic control of the combining of B channels.
<b>Basic Rate Interface</b>	The ISDN Basic Rate Interface, composed of two B channels and one D channel.
<b>blacklist</b>	A list of phone numbers that cannot be dialed because of problems connecting in the past.
<b>CLID</b>	<i>See</i> Caller Line Identification.
<b>callback</b>	A feature in which a user dials in to the router, which then disconnects and places a call to the user.
<b>Caller Line Identification</b>	Also known as Caller ID. The directory number of the caller is provided by the telephone company to the party called during call setup.
<b>CHAP</b>	<i>See</i> Challenge Handshake Authentication Protocol.
<b>Challenge Handshake Authentication Protocol</b>	A method of establishing security on PPP links where the peers must exchange a plain text “secret,” or password, in order to establish a link.

<b>D channel</b>	A 16 Kbps channel used for signaling between the ISDN interface and the ISDN network. This channel controls call setup and tear down.
<b>DHCP</b>	<i>See</i> Dynamic Host Configuration Protocol.
<b>DOSBS</b>	<i>See</i> Data Over Speech Bearer Service.
<b>DOVBS</b>	Also known as DOSBS. <i>See</i> Data Over Speech Bearer Service.
<b>Data Over Speech Bearer Service</b>	The process of sending data over a call that was established as a voice call. Sending data in this method may result in a lower tariff in some parts of North America.
<b>Dynamic Host Configuration Protocol</b>	An Ethernet protocol that provides a centralized administration point for assigning network configuration information.
<b>IP</b>	<i>See</i> Internet Protocol.
<b>IP Address</b>	A 4-byte number uniquely defining each host on the Internet. Ranges of addresses are assigned by Internic, an organization formed for this purpose. Usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57).
<b>IPX</b>	<i>See</i> Internet Packet Exchange.
<b>ISDN</b>	<i>See</i> Integrated Services Digital Network.
<b>ISP</b>	Internet service provider.
<b>Integrated Services Digital Network</b>	A digital telephone network for transmission of voice and data.
<b>Internet Packet Exchange</b>	Novell's internetworking protocol.
<b>Internet Protocol</b>	The main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.
<b>LAN</b>	<i>See</i> local area network.
<b>local area network</b>	A communications network serving users within a limited geographical area, such as one floor of a building, controlled by a network operating system and using a transport protocol.
<b>MP</b>	<i>See</i> Multilink Protocol.
<b>MSB</b>	<i>See</i> Most Significant Bit or Most Significant Byte.

<b>MRU</b>	<i>See</i> Maximum Receive Unit.
<b>MSN</b>	<i>See</i> Multiple Subscriber Numbering.
<b>masquerading</b>	A technique by which several hosts share a single IP address for access to the Internet. This process is an extension of Network Address Translator (NAT). <i>See also</i> Network Address Translator.
<b>Maximum Receive Unit</b>	The size in bytes of the largest packet that can be sent or received.
<b>Most Significant Bit or Most significant Byte</b>	The portion of a number, address, or field that is farthest left when written as a single number in conventional hexadecimal ordinary notation. The part of the number having the most value.
<b>Multilink Protocol</b>	An extension to the point-to-point protocol allowing the combination of both B channels to provide a single 128 Kbps channel. <i>See</i> Point-to-Point Protocol.
<b>Multiple Subscriber Numbering</b>	A service of the telephone company in which a range of numbers is assigned to one line. Each device attached to that line (for example, a phone or router) must know which number it should answer.
<b>National ISDN (NI-1)</b>	Bellcore standard for first phase of ISDN interoperability among U.S. telephone companies.
<b>NAT</b>	<i>See</i> Network Address Translator.
<b>netmask</b>	A number that explains which part of an IP address comprises the network address and which part is the host address on that network. It can be expressed in dotted-decimal notation or as a number appended to the IP address. For example, a 28-bit mask starting from the MSB can be shown as 255.255.255.192 or as /28 appended to the IP address.
<b>Network Address Translator (or Translation)</b>	A proposal for IP address reuse, where the local IP address is mapped to a globally unique address. <i>See also</i> masquerading.
<b>NT1 (Network Termination 1)</b>	Termination device that connects the user's equipment to the ISDN network. Converts the local equipment's four-wire S/T interface to the two-wire telephone company interface. The NT1 is provided by the telephone company in most of the world, but it is provided by the user in North America. Referred to in some areas as a DSU.
<b>numbered links</b>	<i>See</i> unnumbered links.
<b>PAP</b>	<i>See</i> Password Authentication Protocol.
<b>POTS</b>	<i>See</i> Plain Old Telephone Service.

<b>PPP</b>	<i>See</i> Point-to-Point Protocol.
<b>PSTN</b>	Public Switched Telephone Network.
<b>Password Authentication Protocol</b>	A method of enabling security on PPP links. When the link is established, a password is sent by the caller. <i>See</i> Challenge Handshake Authentication Protocol.
<b>Plain Old Telephone Service</b>	The standard analog phone system.
<b>Point-to-Point Protocol</b>	A protocol allowing a computer using TCP/IP to connect directly to the Internet.
<b>RFC</b>	Request For Comment. Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet.
<b>RIP</b>	<i>See</i> Routing Information Protocol.
<b>Routing Information Protocol</b>	A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.
<b>S/T Interface</b>	The four-wire ISDN interface or reference point at the user or local side of the NT1. <i>See also</i> U interface.
<b>Service Profile Identifier</b>	A number assigned by the telephone company to an attached device, used to identify the characteristics of that device.
<b>SPID</b>	<i>See</i> Service Profile Identifier.
<b>subnet mask</b>	<i>See</i> netmask.
<b>U Interface</b>	The two-wire ISDN interface or reference point at the telephone company side of the NT1. <i>See also</i> S/T interface.
<b>unnumbered links</b>	A method of connecting two LANs by way of a WAN, where the two WAN end points do not have their own IP addresses.
<b>WAN</b>	<i>See</i> wide area network.
<b>wide area network</b>	A long distance link used to extend or connect remotely located local area networks.



## A

- A/B Adapter 2 field, ISDN Setup menu, 3-9
- A/B Adapter field, ISDN Setup menu, 3-9
- accounting function, 9-4
- Action Matched/Not Matched field
  - Generic Filter Rule menu, 8-8
  - TCP/IP Filter Rule menu, 8-6
- Active field
  - Edit Dial-in User, 6-5
  - Edit IP Static Route menu, 7-5
  - Generic Filter Rule menu, 8-7
  - Remote Node Profile menu, 5-2
  - Syslog and Accounting menu, 9-5
  - TCP/IP Filter Rule menu, 8-5
- Address Resolution Protocol, 1-14
- Analog Call field, ISDN Setup menu, 3-7
- Analog Call Routing field, ISDN Setup menu, 3-10
- analog voice ports, 1-3

## B

- B Channel Usage field, ISDN Setup menu, 3-7, 3-9
- Bandwidth Allocation Control Protocol, 5-6
- Bandwidth on Demand, 5-6
- Base Transmission Rate, 5-6
- blacklist function, 9-10
- budget management, 9-10

## C

- cables, 2-7
- call control, 9-10

- Call Direction field, Remote Node Profile menu, 5-2
- Callback Budget Management field, Default Dial-in Setup, 6-3
- Callback field, Edit Dial-in User, 6-5
- callback function, 1-5
- calling line identification, 1-4
- CHAP authentication, 1-5, 5-2, 6-2
- coaxial cable, 2-8
- command interpreter mode, 9-9
- command-line mode, 9-6
- compression, 1-2
- Compression field, Remote Node PPP Options menu, 5-5
- configuration
  - automatic by DHCP, 1-4
  - backup, 9-8
  - restoring, 9-8
- connecting
  - cables, 2-7
  - devices, 2-8
  - power, 3-2
  - router, 2-4
  - serial port, 2-9
  - through Telnet session, 2-9
- conventions, xvi
- Country Code field, System Maintenance menu, 9-3
- customer support, iii

## D

- data over voice bearer service call, 3-7, 4-3, 5-3
- Default Dial-in Setup menu, 6-2
- Destination field, TCP/IP Filter Rule menu, 8-5
- Destination IP Address field, Edit IP Static Route menu, 7-5
- DHCP, 1-4, 1-15
- DHCP Setup field, Ethernet Setup menu, 3-12
- Diagnostic menu, 9-6
- Dial Prefix field, ISDN Setup menu, 3-9
- Dial-in User Setup menu, 6-4, 6-5
- dial-in users, 6-1
- domain name server, using, 1-14
- DSS1, 3-9
- dynamic NAT. *See* network address translation

## E

- Edit Dial-in User menu, 6-4, 6-5
- Edit IP Static Route menu, 7-5
- Edit PPP Options field, Remote Node Profile menu, 5-3
- Encapsulation field, Remote Node PPP Options menu, 5-5
- EPROM, for firmware upgrade, 1-3
- error log, 9-4
- Ethernet Address field, System Maintenance menu, 9-2
- Ethernet cable, connecting, 2-7
- Ethernet field, System Maintenance menu, 9-2
- Ethernet Interface field, Ethernet Setup menu, 3-11
- Ethernet Setup menu, 3-12

## F

- features, 1-1
- fiber cable, 2-8

- Filter Rules Summary menu, 8-3, 8-7
- filter type, Generic IP, 8-3
- filtering process, example, 8-1
- filters, configuring, 8-1
- FirstGear
  - description, 1-2
  - for configuration, 1-5, 3-1
- front panel, 2-4

## G

- Gateway IP Address field, Edit IP Static Route menu, 7-5
- General Setup menu, 3-6
- Generic Filter Rule menu, 8-7
- Global Analog Call field, ISDN Setup menu, 3-10

## H

- Hang Up B1 Call field, Diagnostic menu, 9-6
- Hang Up B2 Call field, Diagnostic menu, 9-6

## I

- Idle Time-out field, Edit Dial-in User, 6-5
- Incoming Phone Number field, ISDN Setup menu, 3-9
- initialization, 10-3
- Input and Output Filters field, Ethernet Setup menu, 3-11
- installation, 1-2
- Internet, accessing, 4-2
- IP Address Supplied By field, Default Dial-in Setup, 6-3
- IP addresses
  - and NAT, 1-13
  - and the Internet, 1-7
  - assigning, 1-7, 4-1
  - masquerading, 1-4
  - private, 1-12
- IP configuration, by DHCP, 1-15

- IP Protocol field, TCP/IP Filter Rule menu, 8-5
- IP Source Route field, TCP/IP Filter Rule menu, 8-5
- IP Subnet Mask field, Edit IP Static Route menu, 7-5
- ISDN
  - cable, 2-7
  - checklist, 2-2
  - clearing codes, C-1
  - DSS1, 3-9
  - North American, 2-2, 3-7
  - ordering lines, B-1
  - support, 1-3
  - testing connection, 9-6
  - troubleshooting, 10-2
- ISDN Connection Test field, Diagnostic menu, 9-6
- ISDN Data field, ISDN Setup menu, 3-9
- ISDN F/W Version field, System Maintenance menu, 9-2
- ISDN field, System Maintenance menu, 9-2
- ISDN Menus, manager interface, 3-7
- ISDN Setup menu, 3-7, 3-9
- ISP Connection, troubleshooting, 10-5

**L**

- LAN Packet field, System Maintenance menu, 9-3
- LEDs
  - description, 2-5
  - troubleshooting, 10-2
- Length field, Generic Filter Rule menu, 8-7
- log, 9-4
- Log and Trace menu, 9-4
- Log Facility field, Syslog and Accounting menu, 9-5

- Log field
  - Generic Filter Rule menu, 8-8
  - TCP/IP Filter Rule menu, 8-6

## M

- Macintosh, using to configure, 1-5, 2-9, 3-1
- manager interface
  - accessing through serial port, 2-9
  - accessing through Telnet, 2-9
  - menus, 3-5
  - troubleshooting, 10-7
  - using for configuring, 1-2, 1-5, 2-9, 3-1
- manager interface commands, 3-3
- manager interface menus
  - Default Dial-in Setup, 6-2
  - Diagnostic, 9-6
  - Dial-in User Setup, 6-4, 6-5
  - Edit Dial-in User, 6-4, 6-5
  - Edit IP Static Route, 7-5
  - Ethernet Setup Menu, 3-11
  - Filter Rules Summary, 8-3, 8-7
  - General Setup Menu, 3-6
  - Generic Filter Rule, 8-7
  - Internet Access Setup, 4-2
  - ISDN Setup, 3-8
  - Log and Trace, 9-4
  - Main, 3-4
  - Remote Node Network Layer Options, 7-3
  - Remote Node PPP Options, 5-5
  - Remote Node Profile, 5-1, 7-2
  - Remote Node Setup, 5-1
  - Static Route Setup, 7-4
  - Syslog and Accounting, 9-4
  - System Security, 3-14
  - System Security - Change Password, 3-14
  - System Status, 9-1
  - TCP/IP Filter Rule, 8-4
- Manual Call field, Diagnostic menu, 9-6
- Mask field, Generic Filter Rule menu, 8-7
- Max. Transmission Rate, 5-6

Metric field  
  Edit IP Static Route menu, 7-5  
  Remote Node Network Layer Options menu,  
  7-3

MGR port, 2-7

mode, command interpreter, 9-9

More field  
  Generic Filter Rule menu, 8-7  
  TCP/IP Filter Rule menu, 8-6

Multilink Protocol, 5-6

Multiple Link Options field  
  Default Dial-in Setup, 6-3  
  Remote Node PPP Options menu, 5-5

My WAN Add field, Remote Node Network  
  Layer Options menu, 7-3

## N

Name field, System Maintenance menu, 9-2

NAT. *See* network address translation

netmask  
  description, 1-9  
  translation table, 1-11, 1-12

network address translation, 1-4, 1-13

network checklist, 2-3

North American ISDN, 2-2, 3-7

## O

Offset field, Generic Filter Rule menu, 8-7

Outgoing field, Remote Node Profile menu, 5-2

## P

PABX Number field, ISDN Setup menu, 3-9

package contents, 2-1

PAP authentication, 1-5, 5-2, 6-2

password  
  changing, 3-14  
  entering at startup, 3-2  
  restoring, 10-7

Password field, Edit Dial-in User, 6-5

PC, using to configure, 1-5, 2-9, 3-1

Phone # field, Edit Dial-in User, 6-5

### port

  analog voice, 1-3

  Ethernet, 1-3

  locations, 2-6, 2-7

  MGR, 2-7

  Phone, testing, 10-7

  serial, connecting, 2-9

power, connecting, 3-2

### PPP

  options, editing, 5-4

  support, 1-3

PPP Options field, Default Dial-in Setup, 6-2

### Private field

  Edit IP Static Route menu, 7-5

  Remote Node Network Layer Options menu,  
  7-3

### protocols

  Address Resolution, 1-14

  Bandwidth Allocation Control, 5-6

  DHCP, 1-4, 1-15

  Internet, 1-4

  Multilink, 5-6

  Routing Information, 1-4, 1-6

  support, 1-2

  TCP/IP, 9-7

  Transmission Control, 1-4

  XMODEM, 9-8

publications, related, xvii

## R

RAS S/W Version, System Maintenance menu,  
  9-2

rear panel, 2-6, 2-7

Rem CLID field, Edit Dial-in User, 6-5

Rem IP Addr field  
  Remote Node Network Layer Options, 7-3

  Remote Node Profile menu, 5-3, 7-2

- Rem Node Name field, Remote Node Profile menu, 5-2
- Rem Subnet Mask field, Remote Node Network Layer Options, 7-3
- remote dial-in users, 6-1
- remote node
  - configuring, 5-1
  - setup, 5-1, 7-2
  - troubleshooting, 10-5
- Remote Node Network Layer Options menu, 7-3
- Remote Node PPP Options menu, 5-5
- Remote Node Profile menu, 5-2, 7-2
- Remote Note Set Up menu, 5-1
- remote user, troubleshooting, 10-6
- Reset ISDN field, Diagnostic menu, 9-6
- Route Name field, Edit IP Static Route menu, 7-5
- router concepts, 1-6
- Routing Information Protocol, 1-4, 1-6

## S

- security, 1-2, 1-4, 3-14
- serial cable, 2-7
- serial port, connecting to, 2-9
- Session Options field
  - Default Dial-in Setup, 6-4
  - Remote Node Profile menu, 5-4
- Single User Account field, Remote Node Network Layer Options menu, 7-3
- single user account, configuring for, 4-4
- software, updating, 9-9
- Source field, TCP/IP Filter Rule menu, 8-5
- SPIID Number(s) field, ISDN Setup menu, 3-7
- static route setup, 7-4
- Static Route Setup menu, 7-4

- Subaddress field, ISDN Setup menu, 3-9
- subnet addressing, 1-10
- Switch Type field, ISDN Setup menu
  - DSS1, 3-9
  - North America, 3-7
- Syslog and Accounting menu, 9-4
- Syslog IP Address field, Syslog and Accounting menu, 9-5
- System Maintenance Status menu, 9-2
- System Status Menu, 9-1
- system tools, 9-8

## T

- TCP Estab field, TCP/IP Filter Rule menu, 8-6
- TCP/IP
  - configuration, testing, 9-6
  - configuring, 7-1
  - network, troubleshooting, 10-4
  - Protocol, 9-7
  - requirements, 2-3
  - tools, 9-7
  - using with LAN-to-LAN, 7-1
- TCP/IP Filter Rule menu, 8-4
- TCP/IP Setup field, Ethernet Setup menu, 3-12
- Telco Options field
  - Default Dial-in Setup, 6-2
  - Remote Node Profile menu, 5-3
- Telephone Number(s) field, ISDN Setup menu, 3-7
- Telnet session, connecting to manager interface, 2-9
- terminal baud rate, 9-3
- trace display, 9-7
- trace tools, 9-4
- troubleshooting, 10-1

## **U**

UNIX system, using to configure, 1-5, 2-9, 3-1

User Name field, Edit Dial-in User, 6-5

## **V**

Value field, Generic Filter Rule menu, 8-7

## **W**

warranty, 1-3

World Wide Web, iii

## **X**

XMODEM Protocol, 9-8

## Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>