Reference Guide for the Model RM356 Modem Router

NETGEAR

NETGEAR, Inc.
A Bay Networks Company
4401 Great America Parkway
Santa Clara, CA 95054 USA
Phone 800-211-2069

M-RM356NA-0
July 1998

Trademarks

Bay Networks is a registered trademark of Bay Networks, Inc.

NETGEAR and FirstGear are trademarks Bay Networks, Inc.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the product(s) 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 RM356 Modem Router is 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 RM356 Modem Router und Model 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 RM356 Modem Router has 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: 1800-142-046
  France: 0800-90-2078
  Germany: 0130-817305

  Japan: 0120-66-5402

  Korea: 00308-11-0319

  New Zealand: 0800-444-626

  Sweden: 020-790086

  United Kingdom: (44) 171-571-5120

  U.S./Canada: 800-211-2069

- Fax:

  U.S./Canada: 510-498-2609

World Wide Web

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

Contents

Preface

Chapter 1
Introduction

Chapter 2
Router Installation and Connection

Chapter 3
Router Configuration

Chapter 4
Configuration for Internet Access

Chapter 5
Remote Node Configuration

Chapter 6
Dial-In Configuration

Chapter 7
TCP/IP Configuration

Chapter 8
Filter Configuration

Chapter 9
System Maintenance

Chapter 10
Troubleshooting

Figures

Tables

Preface

Congratulations on your purchase of the NETGEAR™ Model RM356 Modem Router.

The Model RM356 Modem Router integrates a 4-port hub and one high-speed 56K internal modem into a single package. In a modem-sized box, your Model RM356 router offers a complete internetworking solution for your home or branch office. The Model RM356 router is ideal for browsing the Internet, receiving calls from remote dial-in users, or making LAN-to-LAN connections to remote nodes.

The Model RM356 router features one 56 kilobits per second (Kbps) modem line that can connect directly to your local PSTN (Public Switch Telephone Network) network, thereby saving you the cost of buying additional external modems.

Purpose

This guide describes the features of the Model RM356 Modem Router and provides installation and configuration instructions.

Audience

To configure and install the Model RM356 Modem 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:

➡	**Note:** This format is used to highlight information of importance or special interest.

⛔	**Caution:** This format is used to highlight information that will help you prevent equipment failure or loss of data.

⚠	**Warning:** This format is used to highlight information about the possibility of injury or equipment damage.

⚡	**Danger:** 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:

italics	Book titles and UNIX file, command, and directory names.
`courier font`	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 RM356 Modem Router using FirstGear™ configuration software, refer to *Getting Started Using FirstGear for the Model RM356 Modem Router* (part number M1-RM356NA-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,* which are published by the Internet Engineering Task Force (IETF).

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 RM356 Modem Router and discusses planning considerations for installation.

About the Router

The Model RM356 Modem 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 using the entry in the routing table. The entry in the path list contains the phone number(s) of the target router. The router sends the number to the modem port to connect the call. 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 modem port to the LAN port.

The internal 56K modem in the Model RM356 router allows downstream data rates of up to 56 Kbps from your Internet service provider (ISP) and upstream rates of up to 33.6 Kbps.

Features

The Model RM356 Modem Router is a flexible, high-performance, easy-to-use router that provides a cost-effective solution for intelligent networking access across an analog telephone 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 RM356 Modem Router provides the following features:

- Internal high-speed analog modem
  - V.90 standard 56K modem operation to provide up to 56 Kbps downstream data rate from your ISP
- Dial-on-demand
  - Calls automatically placed and terminated as needed without user intervention
- Protocol Support
  - IP routing
  - 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
  - Password access control on management functions
  - Dial-in access control by Calling Line Identification (CLID) and Callback
  - PAP and CHAP authentication support
- Four-port twisted pair Ethernet hub
  - Four RJ-45 interfaces for connection to 10BASE-T workstations

- 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

V.90 Support

The Model RM356 router is designed to take advantage of the V.90 standard for transmission of data over analog telephone networks.

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

TCP/IP Support

The Model RM356 router supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP).

For further information about TCP/IP, refer to “Basic Router Concepts” on page 1-5.

IP Address Masquerading by Dynamic NAT+

The router 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 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 router 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 RM356 Modem 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 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 line. In some regions, CLID may not be available.

PAP and CHAP Authentication

For connecting to other routers, the Model RM356 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 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 RM356 Modem Router is a small office router that routes the IP protocol over a dial-up telephone 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 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 RM356 Modem 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.

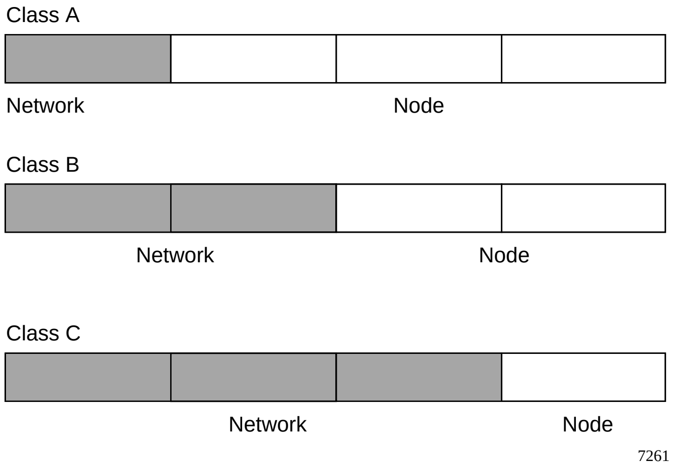


Figure 1-1. Three Main Address Classes

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 you 16 bits of node numbers translating to about 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.

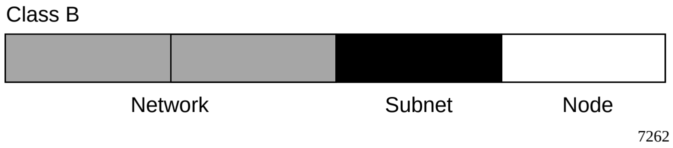


Figure 1-2. Example of Subnetting a Class B Address

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 mask-length formats.

Table 1-2. Netmask Formats

Dotted-Decimal	Mask-length
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
255.255.255.255	/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 RM356 Modem 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 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.

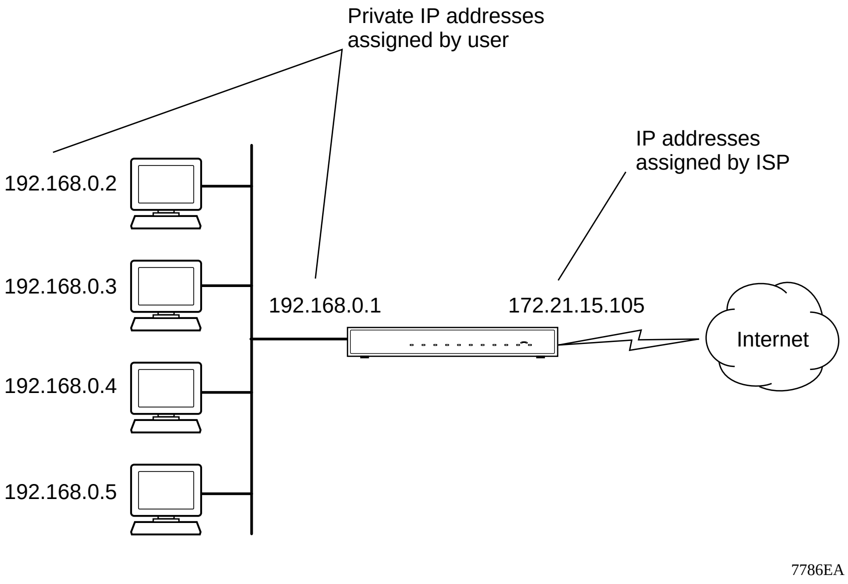


Figure 1-3. Single IP Address Operation Using NAT

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.baynetworks.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. A 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 RM356 Modem Router has the capacity to act as a DHCP server.

Chapter 2
Router Installation and Connection

This chapter provides instructions for installing the Model RM356 Modem 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 RM356 Modem Router
- AC power adapter, 16 V AC output
- 10-foot 10BASE-T Ethernet cable, straight-through wiring (white)
- telephone cable (black)
- 25-pin to RJ-45 serial cable
- 9-pin D-connector to 25-pin D-connector adapter
- This guide
- *Getting Started Using FirstGear for the Model RM356 Modem Router*
- 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 you need to return it for repair.

Checklists

Check the following lists to make sure that your network is correctly configured and all requirements are met. After your network is correctly configured and all requirements as defined by the following checklists are met, you are ready to configure and install your router.

Telephone Line Checklist

The Model RM356 Modem Router connects to the Public Switched Telephone Network (PSTN) using a standard analog voice line.

- Line Quality

  Though the modem is capable of 56 Kbps download performance, the condition of your telephone line and your local public telephone infrastructure may limit your actual data rate. For example:

  - FCC rules limit the data rate to 53 Kbps in the United States.
  - The use of repeaters between your premises and the central office will limit your performance to 33 Kbps.

  If your data rate is substantially less than 50 Kbps, you may want to consult your telephone company regarding the quality of your line.

- Calling Line Identification (CLID)

  If you require CLID for security, you must order CLID for your line from your local carrier.

ISP Checklist

If you will be contracting with an Internet service provider (ISP) for Internet access, you must choose between a single-user account and a multiuser LAN account. You can connect a multiuser network through a single-user account by using the Network Address Translator (NAT) feature of your router.

Single-User Account

In a single-user account, you are assigned only one registered Internet Protocol (IP) address. This address may be a permanent fixed address or it may be a different address assigned dynamically each time you log in to the account. The NAT feature of your router will map the IP addresses assigned to your network to this address for accessing the Internet. Some applications may be incompatible with NAT.

LAN Account

In a LAN account, you will be assigned a registered IP address for your router and for each PC or workstation in your local network. A LAN account is typically more expensive than a single-user account.

Account Information

Your ISP should give you the following basic information for your account whether it is a single-user or LAN account:

- A local phone number for accessing the ISP
- A login name
- A password
- IP address(es) unless they are to be dynamically assigned
- IP addresses of the ISP’s Domain Name Servers (DNS)

Network Checklist

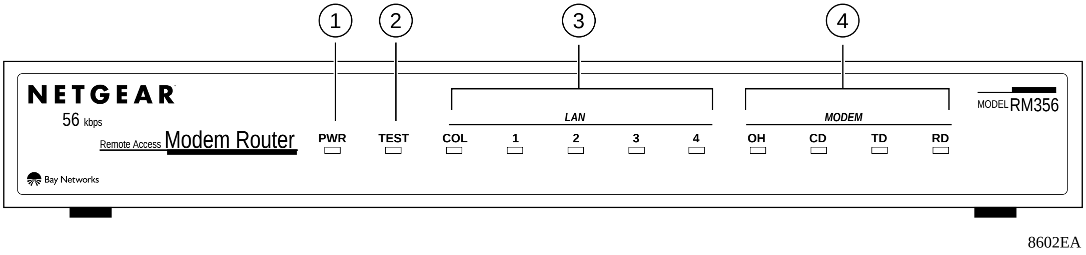
The Model RM356 Modem Router uses the Internet Protocol (IP). The IP configuration has the following requirements:

- All host devices must have TCP/IP installed and selected as the networking protocol.
- All host devices including the router must be assigned IP addresses. If your ISP or network administrator has not assigned these, use private addresses. If you are using the DHCP function of the router, you can have these addresses assigned automatically by the router.
- All host devices must have the IP address of the router defined either as the default gateway or as an entry in the static routes table. If you are using the DHCP function of the router, this gateway IP address is assigned automatically by the router.
- The network portion of the IP addresses 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 1-12 for more information about IP address masquerading. Refer to "IP Addresses and the Internet" on page 1-6 for more information about TCP/IP network configuration.

Connecting the Router

The front panel of the Model RM356 Modem Router, as illustrated in Figure 2-1, contains status LEDs. Refer to the illustration to locate the LEDs and to Table 2-1 for descriptions. You can use some of the LEDs to verify connections.



Key:
1 = PWR (Power) LED
2 = TEST LED
3 = LAN LEDs: Collision and per-port link/activity
4 = MODEM LEDs - Off Hook, Carrier Detect, Transmit Data, and Receive Data

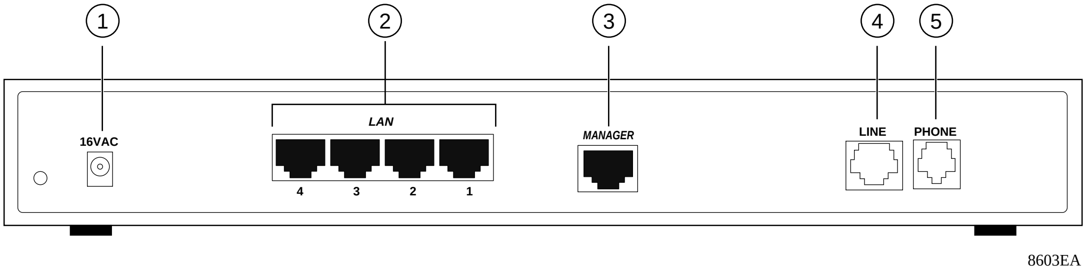
Figure 2-1. Front Panel of the Model RM356 Modem Router

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/Off	The router is functioning properly. This LED will blink during initialization and will then turn off.
LAN		
COL (Collision)	Blinking	Data collision is occurring on the LAN.
1-4	On	The numbered LAN port is synchronized with an attached device.
	Blinking	Data is being received on the port.
Modem		
OH (Off Hook)	On	The modem is in use.
CD (Carrier Detect)	On	A valid carrier is present on the line.
TX (Transmit)	Blinking	Data is being transmitted on the modem port.
RX (Receive)	Blinking	Data is being received on the modem port.

The rear panel of the Model RM356 Modem Router is shown in Figure 2-2. Refer to this diagram to identify all of the ports on the router when you attempt to make any connections.



Key:
1 = AC adapter outlet for connecting the AC adapter to the router
2 = LAN ports for connecting the router to workstations using UTP cable
3 = RJ-45 serial Manager port for connecting the router to the serial port of a PC using the RJ-45 to DB-25 cable
4 = Line port for connecting the router to the telephone line
5 = Phone port for connecting the router to a telephone, fax, or modem

Figure 2-2. Rear Panel of the Model RM356 Modem 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 the RJ-45 end of the 25-pin to RJ-45 serial cable into the port labeled MANAGER on the router. Plug the other end into a serial port (such as COM1 or COM2) of your PC. You must use the included 25-pin to 9-pin adapter if your PC has only a 9-pin port available.

Connecting to the Line Port

Plug one end of the black telephone cable into the connector labeled LINE on the router. Plug the other end into the telephone line wall jack.

Connecting to the Hub Ports

The Model RM356 Modem 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 RM356 Modem 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 the PHONE port for connecting your router to an analog telephone, fax, or modem. This port is an extension of the LINE port.

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 RM356 Modem Router.*

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 the Serial Port

You can access the built-in interface through the RJ-45 serial Manager 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 Manager 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 make sure that the router and workstation are connected to the LAN and you must set up your workstation to enable it 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.

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 serial 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 RM356 Modem 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 RM356 Modem Router*.

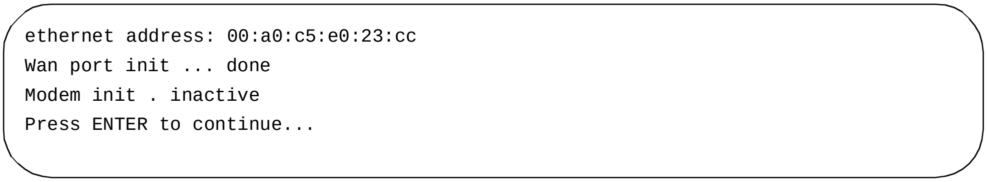
- Through the built-in Manager interface

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 the Serial Port" or "Connecting Through a Telnet Connection" on page 2-9 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. After the initialization, the start-up display appears, as illustrated in Figure 3-1.



```
ethernet address: 00:a0:c5:e0:23:cc
Wan port init ... done
Modem init . inactive
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.

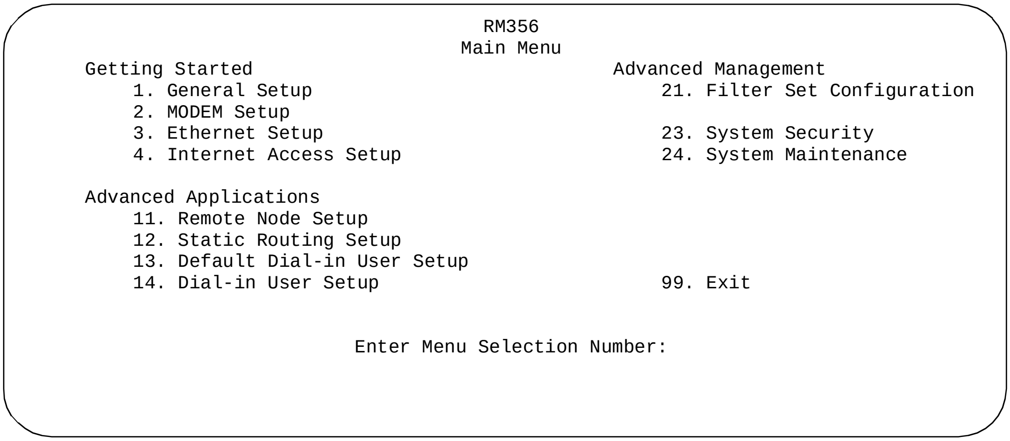
Navigating the Manager

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.



```
                                 RM356
                               Main Menu
    Getting Started                             Advanced Management
        1. General Setup                            21. Filter Set Configuration
        2. MODEM Setup
        3. Ethernet Setup                           23. System Security
        4. Internet Access Setup                    24. System Maintenance

    Advanced Applications
        11. Remote Node Setup
        12. Static Routing Setup
        13. Default Dial-in User Setup
        14. Dial-in User Setup                      99. Exit


                        Enter Menu Selection Number:
```

Figure 3-2. Manager Main Menu

Manager Menu Summary

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

Table 3-2. Manager Menu Summary

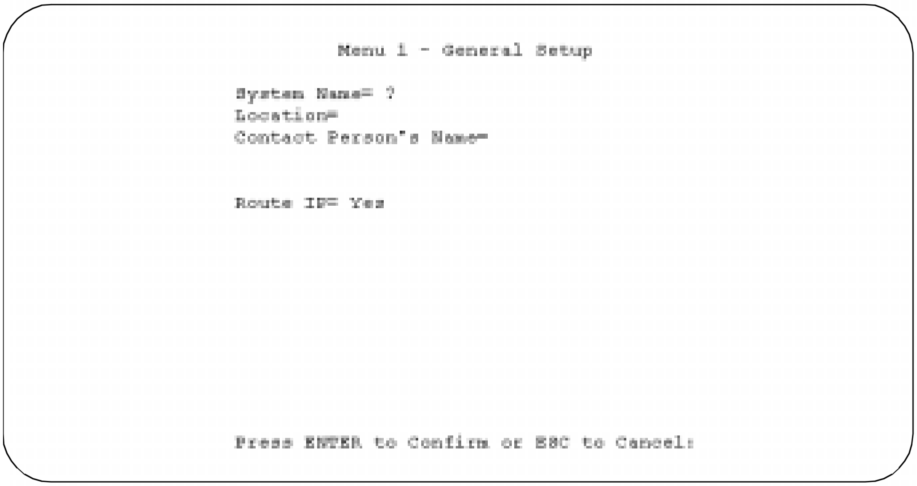
Number	Menu Title	Description
1	General Setup	This menu is accessed to set up general information (router name, for example).
2	MODEM Setup	This menu is accessed to set up modem port configuration.
3	Ethernet Setup	This menu is accessed to set up Ethernet configuration.
4	Internet Access Setup	This menu 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.
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 users.
14	Dial-in User Setup	This menu is accessed to set up remote dial-in users. The router supports eight remote dial-in user profiles.
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 Password	This menu is accessed to change the Manager access password.
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.**



```
                    Menu 1 - General Setup

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


      Route IP= Yes










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

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 RM356 or NewYork. 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.

MODEM Menus

Menu 2 is for configuring the internal 56K modem. Advanced MODEM setup is provided by a submenu, Menu 2.1.

MODEM Setup Menu

Use the commands and menus described in Table 3-1 and Table 3-2 to display the MODEM Setup menu. Table 3-3 lists and describes each field in the menu and how to enter the information in each field.

Table 3-3. MODEM Setup Menu Parameters

Field	**Description**	**Example**
Modem Name	Enter a descriptive name for the internal modem.	ModemA
Active	Set this field to Yes to activate the modem port. The router will initialize the internal modem. Deactivating a modem port has no effect on the operation of the router, but the profile of the modem port will remain in the database and can be activated in the future.	Press space-bar to toggle [Yes/No]
Direction	This field determines whether the router is allowed to place calls, accept calls, or both. Use the space bar to select Outgoing, Incoming, or Both.	Outgoing (default)
Phone Number	Enter the telephone number assigned to your modem line by your telephone company. Note that the router accepts only digits; do not include dashes and spaces in this field.	5551212 (example)
Advanced Setup	To edit the Advanced Setup for the internal modem, move the cursor to this field, use the space bar to select Yes, and press [Enter]. This step will bring you to Menu 2.1 - Advanced MODEM Setup.	[Yes/No]

Advanced MODEM Setup Menu

Use the commands described in Table 3-3 to display Menu 2.1 - Advanced MODEM Setup. When you finish entering the information for all the fields:

- 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 internal modem.

Table 3-4 lists and describes the fields for Menu 2.1 - Advanced MODEM Setup.

Table 3-4. Advanced MODEM Setup Menu Field Descriptions

Field	Description	Default
AT Command Strings:		
Dial	Enter the AT Command string to make a modem connection.	atdt
Init	Enter the AT Command string to initialize the modem.	at&fs0=0w2s95=1
Call Control:		
Dial Timeout (sec)	The router will time out if it cannot set up an outgoing modem call within the timeout value.	60
Retry Count	How many times a busy or no-answer phone number is retried before it is put on the blacklist (0 disables blacklisting).	0
Retry Interval (sec)	Elapsed time after a call fails before another call may be retried. Applies before a phone number is blacklisted.	10
Call Back Delay (sec)	Elapsed time between dropping a callback request call and dialing a callback call.	15

When you have completed this menu, press [Enter] to return to Menu 2. Be sure to press [Enter] again to exit Menu 2 in order to save changes made in both menus.

Ethernet Menu

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 allows the application of filter sets for filtering your Ethernet traffic. Filter sets are used to block certain packets in order to reduce bandwidth or to enhance security. Refer to Chapter 8, "Filter Configuration," for more information about configuring filters.

Filters that have been defined in Menu 21 may be applied here by entering their numbers in the appropriate fields in this menu. Up to four filter sets may be cascaded by listing the filter set numbers separated by commas.

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

Table 3-5. Ethernet General Setup Menu Filter Sets

Field	Description
Input and Output Filter Sets	Enter the filter set number(s) to apply a filter to packets received from the LAN (Input) or sent to the LAN (Output).

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 1-6 and "IP Configuration by DHCP" on page 1-14 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 provide the Primary DNS Server address to attached hosts, enter the address in this field.
Secondary DNS Server	If you want the router to provide 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	This parameter determines how the router handles RIP (Routing Information Protocol) with other routing devices on the LAN. 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 on the LAN. Usually, you should leave this parameter at the default (Both) and let RIP propagate the routing information automatically**.**
RIP Version	This field determines which version of RIP (Routing Information Protocol) will be used by the router. The following RIP options are supported by the Model RM356 Modem Router: • RIP-1—The router will accept and send RIP-1 messages only. • RIP-2B—The router will accept RIP-1 and RIP-2 messages (both broadcast and multicast) and send RIP-2 messages in broadcast format. • RIP-2M—The router will accept RIP-1 and RIP-2 messages (both broadcast and multicast) and send RIP-2 messages in multicast format. For most applications, the recommended version is RIP-2B. Select RIP-1 if other connected routers or workstations do not support RIP-2. Select RIP-2M only in a pure RIP-2 environment.

Manager Password Setup

To change the Manager password:

1. **Select option 23 (System Password) from the main menu to display Menu 23 - System Password.**
2. **Enter your previous system password and press [Enter].**
3. **Enter your new system password and press [Enter].**
4. **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 RM356 Modem 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 1-6.

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 Menus 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, MyISP).**

   This information is for identification purposes only.
3. **Enter the IP Address of the remote router at the point of presence (POP) of the ISP in the ISP Gateway 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 # 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. In addition to numbers, these fields accept pound sign (#), star (*), and comma (,). Use a comma to insert a pause (for example, to wait for a second dial tone).
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 1-12 and "Configuration for Single-User Account" on the next page for more information about the Single User Account field. The default is No.

8. **If you must use a script to log in to your account, use the space bar to toggle the Edit Script Options field to Yes and press [Enter].**

   Refer to "Editing Script Options" on page 5-5 for more information.

9. **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 RM356 Modem 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 feature

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

- Single User Account: Local IP Addr

  If your ISP assigns you a dynamic IP address, enter 0.0.0.0 here. If your ISP assigns you a static IP address, enter that IP address here.

- 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.

Backup ISP Accounts

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

Configuring for a Backup ISP

To configure a backup ISP account:

1. **Configure your primary ISP using Menu 4, as described earlier in this chapter.**
2. **Enter Menu 11, and then select the number of an unused remote node.**
3. **In Menu 11.1, choose a name for your backup ISP account; set the Active field to No; and then enter your outgoing login name, password, and phone number(s).**

   The Remote IP Address field should be set to 1.1.1.1.
4. **In Menu 11.3, set the subnet mask of the remote node to 0.0.0.0; then set RIP to None.**

   Save the new configuration.

Switching to a Backup ISP

If you need to switch from your primary ISP to a backup ISP:

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

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

Chapter 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 a wide-area network (WAN) connection. A remote node is required for placing calls to a remote network or answering calls from a remote network. One common type of remote node is an Internet service provider (ISP). When you use Menu 4 to configure your router for Internet access, the router automatically adds a remote node for you, using default values typical of an ISP.

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 option is enabled, 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 field is required if Call Direction is either Both or Out. Enter the login name your router uses when it calls this remote node.
My Password	This field is required 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: • 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). • PAP—Use PAP only. • CHAP—Use CHAP only.

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. In addition to numbers, these fields accept pound sign (#), star (*), and comma (,) where necessary.
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."
Edit Script Options	If the remote node requires a login script handshake, use the space bar to select Yes and press [Enter] to display Menu 11.4 - Remote Node Script. For more information about editing scripts, see "Editing Script Options" on page 5-5.
Telco Options:	
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.
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.

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: • Standard PPP—Standard PPP options are used (default). • CISCO PPP—Cisco Systems PPP options are used.
Compression	Allows the negotiation of data compression with the remote node router.

Editing Script Options

Some ISPs require login script handshaking during a call connection. The Model RM356 Modem Router provides six sets of programming scripts for this purpose. Each set of scripts is composed of an Expect string and a Send string. After capturing and verifying the string in the Expect field, the router will send out the string in the Send field. If both the Expect and Send fields are empty, the router will terminate script handshaking. The Script Options display is shown in Table 5-3.

Table 5-3. Script Options Display

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

Chapter 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 security and callback; 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, while 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, and how to set up individual profiles for dial-in users.

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: • None—No CLID is required (default). • Required—You must provide the CLID, or the call is disconnected. • Preferred—If the CLID is available, it is used to do authentication. If the CLID is not available, the call continues.
PPP Options:	
Recv Authen	This field sets the authentication protocol used for incoming calls. The four options for this field are: • CHAP/PAP—The router tries CHAP first, but PAP is used if CHAP is not available (default). • CHAP—Use CHAP only. • PAP—Use PAP only. • None—No authentication is required.
Compression	This field allows the negotiation of data compression with the equipment of the dial-in user.
Mutual Authen	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: • 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. • 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.
Callback Budget Management:	
Allocated Budget (min)	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.
Period (hr)	This field sets the time interval to reset the above callback budget control.

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

Field	Description
IP Address Supplied By:	
Dial-in User	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.
IP Pool	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. If this field is set to Yes, enter in IP Start Addr field the IP address that you want to assign the dial-in user.This field is active only if you selected Yes in the Dial-In IP Address Supplied By: IP Pool field. This field specifies the IP address that is available to be assigned to a dial-in user.
Session Options:	
Input Filter Sets and Output Filter Sets	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 sets 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 as many as four 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).
Idle Timeout	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 User 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: • No (default)—The router does not call back to the dial-in user. • Optional—The router will call back if the dial-in user requests it. • Mandatory—The router will always disconnect and call back to the dial-in user. 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	If this field is set to 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.
Callback Phone #	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 enabled, 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).

More On CLID

CLID allows the Model RM356 Modem Router to authenticate a caller before a call is answered, thus saving the cost of a connection. The router uses the caller ID information provided by the telephone company during call setup to match against the CLID in the database.

Besides authentication, another application of CLID is to combine it with callback. For example, if you enable both the CLID authentication and callback options for a dial-in user, all usage charges are incurred by the company instead of the employee. This application may simplify accounting and eliminate the necessity for reimbursement.

Chapter 7
TCP/IP Configuration

This chapter describes how to configure your Model RM356 Modem 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.

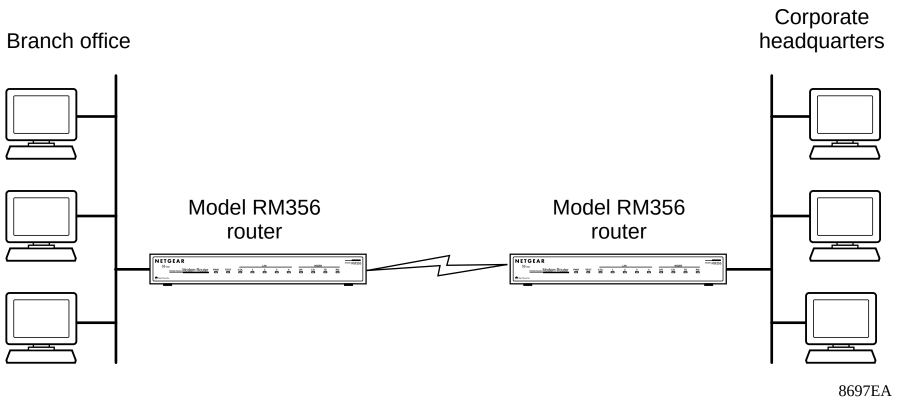


Figure 7-1. LAN-to-LAN Application

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.

> ➡ **Note:** 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, "Dial-In Configuration").

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 in Menu 11.3 described in Table 7-2 on page 7-3.**
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 1-12 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 its routing table to other routers and incorporates RIP broadcasts by other routers into its routing table. If set to In Only, the router will not broadcast its routing table but will accept RIP information from other routers. 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	This field determines which version of RIP (Routing Information Protocol) will be used by the router. The following RIP options are supported by the Model RM356 Modem Router: • RIP-1—The router will accept and send RIP-1 messages only. • RIP-2B—The router will accept RIP-1 and RIP-2 messages (both broadcast and multicast) and send RIP-2 messages in broadcast format. • RIP-2M—The router will accept RIP-1 and RIP-2 messages (both broadcast and multicast) and send RIP-2 messages in multicast format. For most applications, the recommended version is RIP-2B. Select RIP-1 if other connected routers or workstations do not support RIP-2. Select RIP-2M only in a pure RIP-2 environment.

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 opens. 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 1-9.
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 the WAN, 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 RM356 Modem Router.

The router uses filters to decide whether to allow passage of a data packet and/or to make a call over the phone 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 RM356 Modem 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.

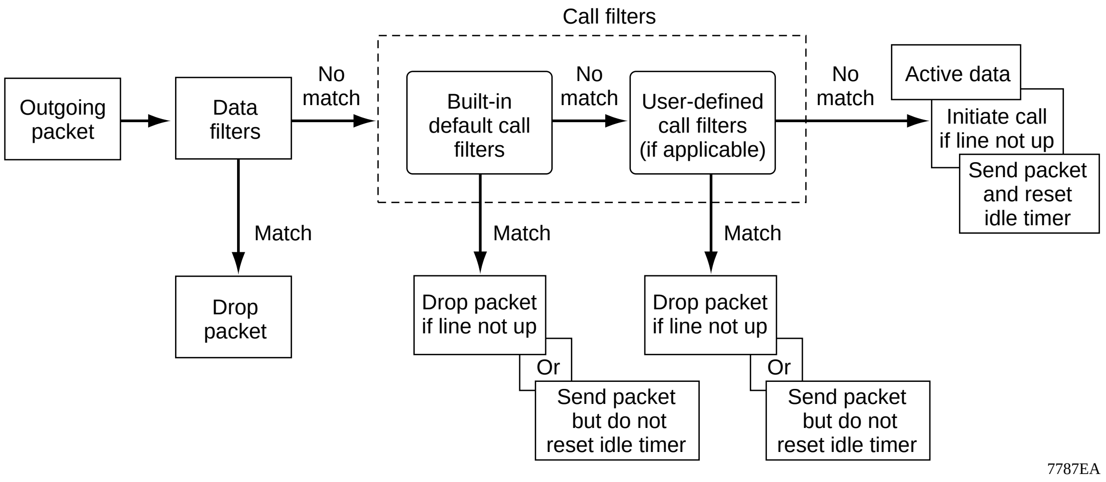

Call filters
Outgoing packet
Data filters
No match
Built-in default call filters
No match
User-defined call filters (if applicable)
No match
Active data
Initiate call if line not up
Send packet and reset idle timer
Match
Drop packet
Match
Drop packet if line not up
Or
Send packet but do not reset idle timer
Match
Drop packet if line not up
Or
Send packet but do not reset idle timer
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
DP	Destination port number

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 a generic type of filter rule, select Generic by pressing the space bar under the Filter Type field and then pressing [Enter] to display the menu for a generic filter rule.

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

Field	Description
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 protocol number. The value entered in this field should be a decimal number between 0 and 255 (for example, 17 refers to the UDP protocol). Refer to RFC1700, *Assigned Numbers*, for specific protocol numbers.
IP Source Route	Yes or No in this field determines whether to check the source route.
Destination:	
IP Addr	In this field, enter the destination IP address of the packet you want to filter. The address is written in dotted-decimal notation such as a.b.c.d where a, b, c, and d are numbers between 0 and 255.
IP Mask	In this field, enter the IP subnet mask that is used to mask the bits of the IP Address given in Destination: IP Addr. See “Netmask” on page 1-8 for information about IP subnet masks.
Port #	In this field, enter the destination port of the packets that you want to filter. The range of this field is 0 to 65535. For example, 47 refers to the FTP port. Refer to RFC1700, *Assigned Numbers*, for specific port numbers.
Port # Comp	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: • None (default) • Less • Greater • Equal • Not Equal
Source:	
IP Addr	In this field, enter the source IP address of the packet you want to filter. The IP address is written in dotted-decimal notation such as a.b.c.d where a, b, c, and d are numbers between 0 and 255.
IP Mask	In this field, enter the IP subnet mask that is used to mask the bits of the IP Address given in Source: IP Addr.
Port #	In this field, enter the source port of the packets that you want to filter. The range of this field is 0 to 65535.
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: • None (Default) • Less • Greater • Equal • Not Equal

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

Field	Description
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. Two options are available for this field: • Yes—Filter match only established TCP connections • No—Filter match both initial and established TCP connections (default)
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: • Yes • No (default) 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: • None—No packets are logged (default). • Action Matched—Only packets that match the rule parameters are logged. • Action Not Matched—Only packets that do not match the rule parameters are logged. Both—All packets are logged. • Check Next Rule (default) • Forward • Drop
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: • Check Next Rule (default) • Forward • Drop

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 entry 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 entry 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: • Yes • No (Default) 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: • None—No packets are logged (default). • Action Matched—Only packets that match the rule parameters are logged. • Action Not Matched—Only packets that do not match the rule parameters are logged. • Both—All packets are logged. • Check Next Rule (default) • Forward • Drop
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: • Check Next Rule (default) • Forward • Drop

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:

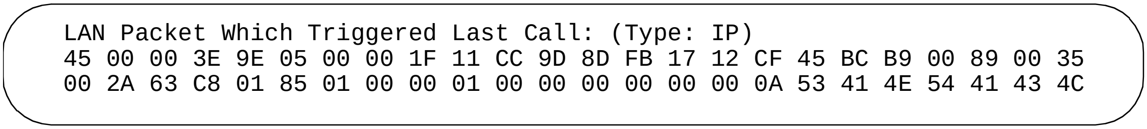
```
Call Filter Sets = 1,3,10
```

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 router, you may need to make some configuration changes to avoid having 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 RM356 Modem 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 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

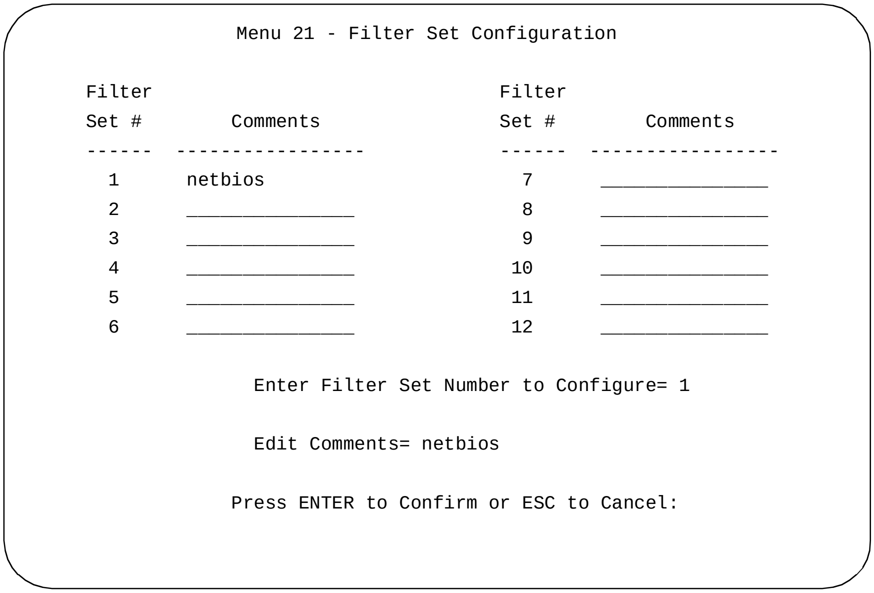
Implementing the Filter

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 #        Comments                 Set #        Comments
     ------  -----------------             ------  -----------------
       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.**

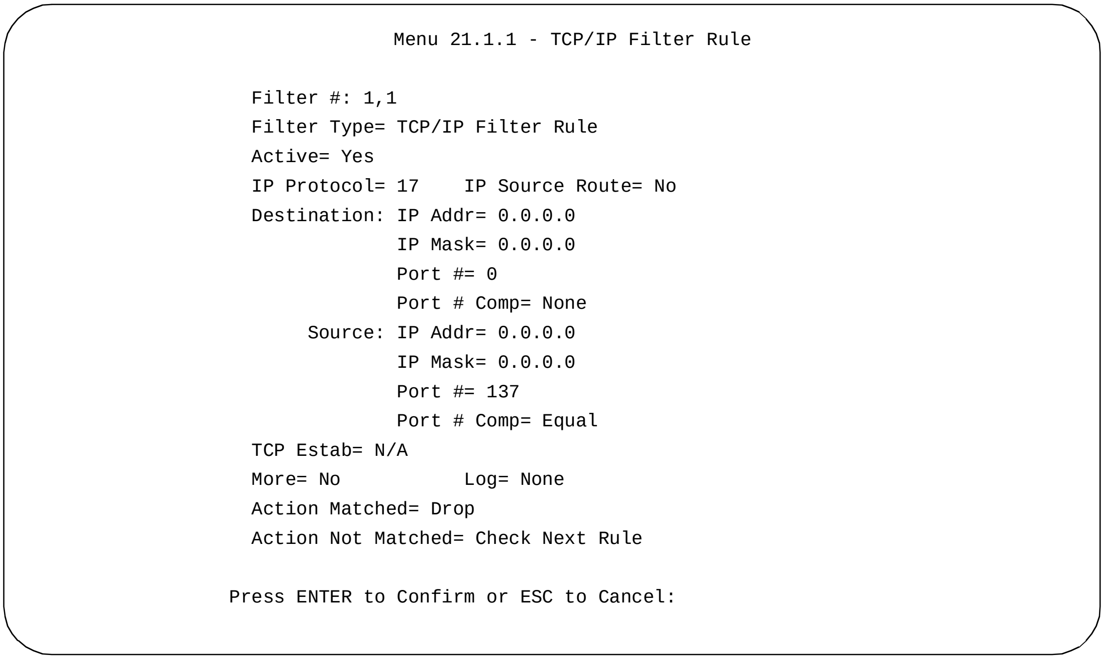
   You want your filter to ignore (drop) UDP and TCP packets originating from ports 137, 138, and 139. Because each protocol/port combination must be specified as a separate rule, there will be six rules. Each filter set contains six rules, so you will fill one entire set. Begin with rule 1, as illustrated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

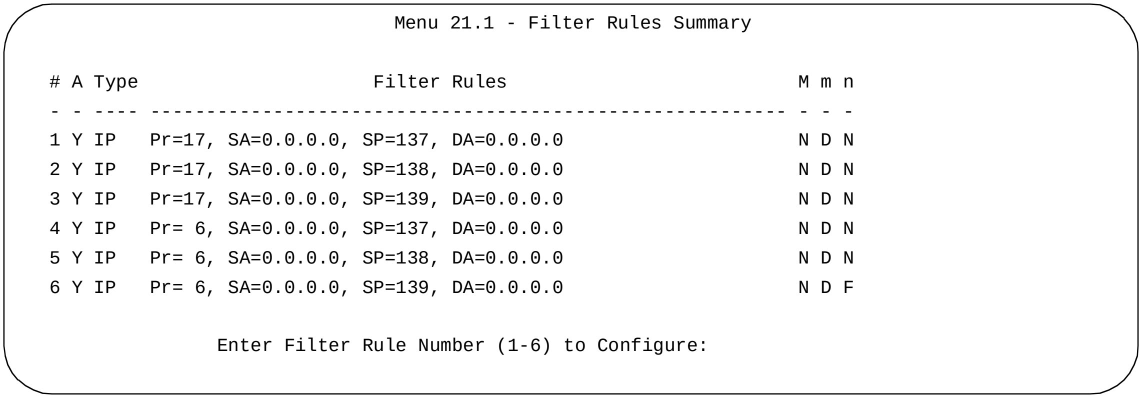
Figure 8-4. TCP/IP Filter Rule Menu

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.



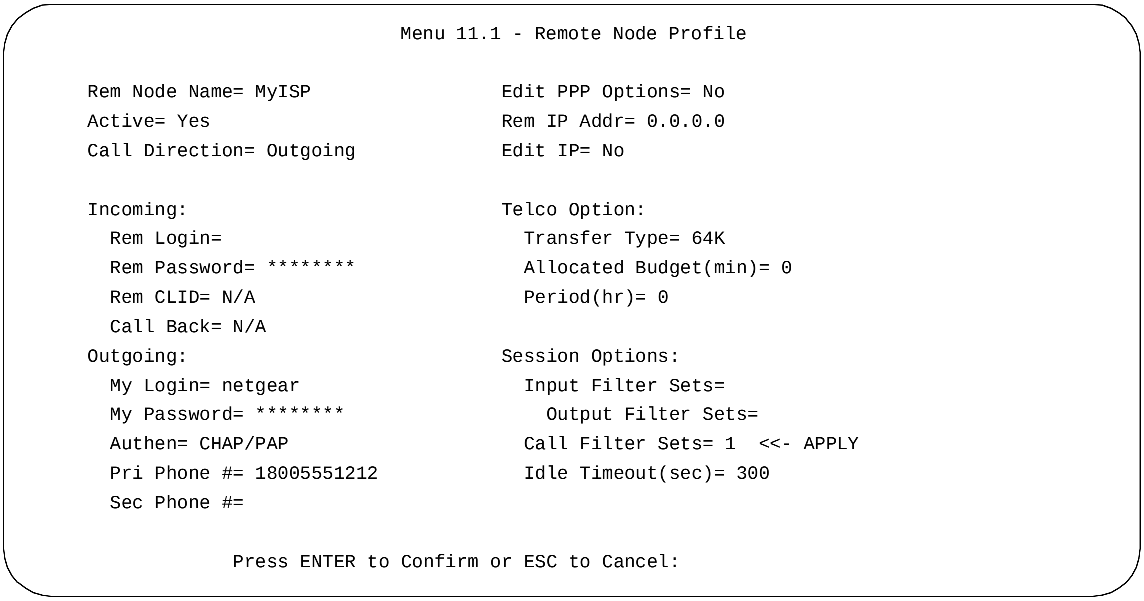
```
                               Menu 21.1 - Filter Rules Summary

 # 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 RM356 Modem Router provides diagnostic tools for maintenance. These diagnostic tools include displays of system status, modem 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 MODEM and Ethernet ports, 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

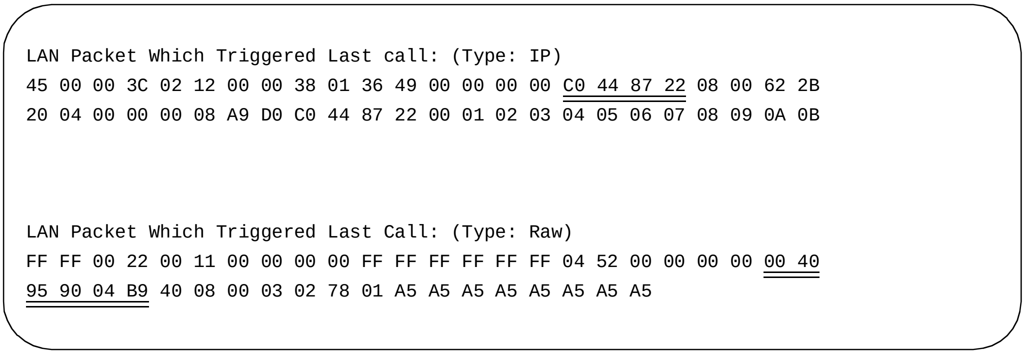
Command	Field Name	Description
Enter 1	Drop port 1	This field disconnects the current modem call.
Enter 9	Reset counters	This field resets the counters.
[Esc]		Pressing [Esc] exits this menu.

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
Port:	This field displays the WAN port number (1). For each channel the screen displays:
Status	The remote node the channel is currently connected to, or the status of the channel (Idle, Calling, or Answering).
Speed	The current connecting speed.
TX Pkts	The number of packets transmitted on this channel since reset or manual clear.
RX Pkts	The number of packets received on this channel since reset or manual clear.
Errors	The number of error packets on this channel since reset or manual clear.
Up Time	The time that this channel has been connected to the current remote node.
Total Outcall Time	The total outgoing call time for all WAN ports since the system has been powered on.
Ethernet:	For the LAN port, the screen displays:
Status	The current status of the LAN port.
TX Pkts	The number of packets transmitted to the LAN.
RX Pkts	The number of packets received from the LAN.
Collisions	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	The version of the current router software.
Ethernet Address	The Ethernet MAC address assigned to your router.
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, 38400, and 115200 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 to 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, 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 ISP connection
- Communicate directly with the MODEM port
- Test the TCP/IP configuration
- Reboot the system
- Change the interface mode to command-line mode

The diagnostic test options from Menu 24.4 - System Maintenance - Diagnostics are listed in Table 9-5.

Table 9-5. System Maintenance - Diagnostic Menu Fields

Field	**Command**	**Description**
MODEM		
Drop MODEM	1 [Enter]	This command hangs up the current MODEM call.
Reset MODEM	2 [Enter]	This command will reset the MODEM.
Manual Call	3 [Enter]	This command will cause the router to place a manual call to a Remote Node and log in to the account. A trace will be displayed on the screen showing the progress of the call setup and protocol negotiation.
Redirect to MODEM	4 [Enter]	This command will redirect the Manager terminal to the MODEM port so that AT commands may be sent directly to the internal MODEM.
TCP/IP		
Internet Setup Test	11 [Enter]	This command will cause the router to place a manual call to the ISP and log in to the account. A trace will be displayed on the screen showing the progress of the call setup and protocol negotiation.
Ping Host	12 [Enter]	This test pings the host, which determines the functionality of the TCP/IP protocol on your system.

Table 9-5. System Maintenance - Diagnostic Menu Fields (continued)

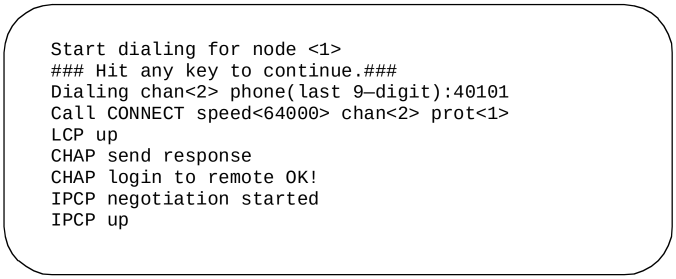
Field	Command	Description
System		
Reboot System	[Enter 21]	This option reboots the system, implementing any changes that may have been recently added to your system.
Command Mode	[Enter 22]	This option allows the user to enter the command mode. This mode allows you to diagnose and test your router using a specified set of commands.

Call Testing and TCP/IP Tools

Two test selections—Manual Call and Internet Setup Test—are available for testing call placement and session connection with remote hosts. Both tests cause a call to be placed to a remote node and display the progress of the connection. Manual Call (command 5) prompts the user to specify the desired remote node by its profile number in Menu 11. Internet Setup Test (command 11) automatically calls the remote node that has been specified as an ISP.

Enter 11 to select the Internet Setup Test, or enter 5 to select another remote node. This test checks to see if your Internet access or remote node configuration has been done correctly. The router dials the node, 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.

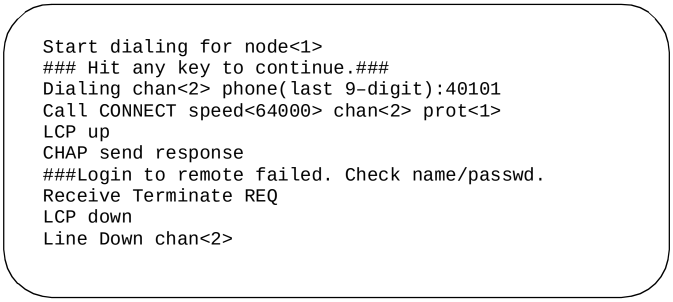
Figure 9-2 illustrates an example of a trace display for a successful call when using a TCP/IP protocol connection.



```
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

Another useful diagnostic tool for TCP/IP testing is Ping Host, which causes a packet to be sent to a specified host requesting an echo packet.

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 9-10.

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. Using Menu 24.7 - Software Update, you can update the main router (RAS) software or the configuration (ROM) area.

⛔	**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 RAS software:

1. **Select Menu 24 - System Maintenance.**
2. **Enter 7 to select Software Update.**
3. **Enter 1 to select Load RAS code.**

   A message is displayed showing further instructions and asking if you want to continue.
4. **Press y and wait for the Debug Mode command prompt.**
5. **Enter the command atur and wait.**

   After about 30 seconds, the router displays the Starting XMODEM upload... message.
6. **Transfer the new software file to the router using the XMODEM Protocol of your serial communications software.**
7. **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 RM356 Modem 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, 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. You can specify the number of attempts and the retry interval in Menu 2.1 - Advanced MODEM Setup.

Budget Management

The budget management function provides a way for you to set a limit on phone line 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)
- Number of calls
- Call time (maximum, minimum, and total)

This information is erased when the router is reset.

Chapter 10
Troubleshooting

This chapter gives information about troubleshooting your Model RM356 Modem Router. After each problem description, instructions are provided to help you diagnose and solve the problem.

Basic Functioning

When 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 15 seconds. After this self-test, the Test LED should begin to blink at a rate of about 0.5 Hz. After initialization is complete, the Test LED will turn off.

If an Ethernet connection is made to any LAN port, the LAN LED for that port number should be on. If the LAN LED is off, refer to "LAN Link LED," on page 10-1.

LEDS

If all 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. If the error persists, you have a hardware problem and should contact technical support.

LAN Link LED

If the LAN LED for any LAN port does not light when the Ethernet connection is made to that port, check the following:

- Physical Ethernet cables

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

- Connected hub or workstation

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

- Ethernet cable

  If you are connecting the router LAN port directly to a workstation or to the uplink (MDI) port of another hub, use a standard straight-through Ethernet cable such as the one provided.

- Connection to another hub

  If you are extending your network by connecting the router to another hub, verify that you are using the correct combination of cable and port. If you are connecting a LAN port of the Model RM356 Modem Router to the uplink (MDI) port of another hub, use a standard straight-through Ethernet cable such as the one provided. If there is a switch associated with the uplink port of the connecting hub, make sure that the switch is in the uplink (MDI) position. If you are connecting a LAN port of the Model RM356 Modem Router to a normal (MDI-X) port of another hub, you must use a crossover cable.

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 LED is on for the port attached to your PC. If the LAN LED is off, follow the instructions in "LAN Link LED" on page 10-1.
  - Check that the Link LED is on for the network interface card in your PC or workstation.
- 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 -t followed by the IP address of the remote device you are calling.

If the path is functioning correctly, the OH (offhook) LED on the router should turn on, indicating that a call is being placed. If the OH LED does 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.exe (for Windows NT, run ipconfig.exe). 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 call is being set up, your PC should display timeouts followed eventually by replies. If no replies are seen after one minute, the path is not functioning correctly. 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."

To cancel the pings, type Ctrl-C (while holding down the Ctrl key, press the letter c).

Troubleshooting a Remote Node or ISP Connection

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

- 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 #
- 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 protocol 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 “Using the Packet and Log Trace” on page 10-7.

Troubleshooting a Remote User Connection

To troubleshoot a remote user connection:

1. **Verify that you configured the authentication parameters in Menu 13. These parameters are:**
   - CLID Authen
   - Recv Authen
   - Mutual Authen

2. **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.

3. **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 "Using the Packet and Log Trace" on page 10-7.

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:

1. **Verify that the router is connected to the serial port of your terminal or computer using the included cable.**
2. **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

   – No flow control

If you cannot access the Manager by using the Telnet Protocol, refer to "Testing the LAN Path to Your Router," on page 10-2.

Restoring the Default Configuration and Password

The user can erase the current configuration and restore defaults by uploading the initialization file romfile0 or romdhcp, which can be found in the directory in which FirstGear was installed. These files are 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.

The two initialization files romfile0 and romdhcp differ in the initial IP address information and DHCP setup. The file romfile0 leaves the router with no IP address and with DHCP disabled. The file romdhcp leaves the router with an initial IP address of 192.168.0.1 and with DHCP enabled, allowing the router to assign initial IP configuration information to attached hosts.

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

To enter the BootModule debug mode:

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 of 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 (or romdhcp) using XMODEM transfer protocol. Wait for the following message:**

   ```
   Programming successful....
   ```

6. **Restart the router.**

Using the Packet and Log Trace

You can diagnose PPP connection failures using the packet trace feature of the Model RM356 Modem 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:**

   ```
   rm356> sys trcl cl
   ```

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

   ```
   rm356> sys trcl sw on
   ```

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

   ```
   rm356> sys trcp sw on
   ```

7. **Trace the call.**

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

   ```
   rm356> dev dial N
   ```

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

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

   ```
   rm356> sys trcl disp
       or
   sys trcp disp
   ```

The trace appears on the terminal screen. Use PageUp and PageDown to inspect the entire trace.

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 10-1 breaks down and defines the packet trace display for the preceding packet example.

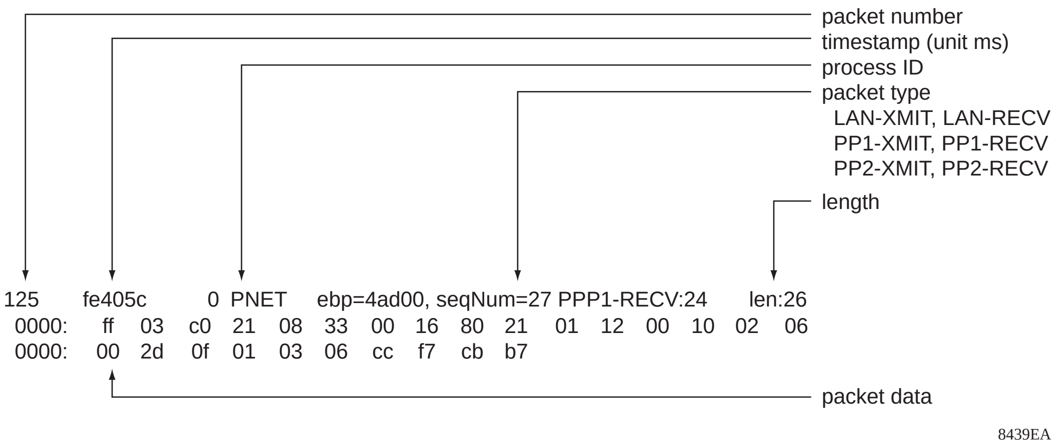

packet number
timestamp (unit ms)
process ID
packet type
LAN-XMIT, LAN-RECV
PP1-XMIT, PP1-RECV
PP2-XMIT, PP2-RECV
length
125 fe405c 0 PNET ebp=4ad00, seqNum=27 PPP1-RECV:24 len:26
0000: ff 03 c0 21 08 33 00 16 80 21 01 12 00 10 02 06
0000: 00 2d 0f 01 03 06 cc f7 cb b7
packet data
8439EA

Figure 10-1. 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 10-2 breaks down and defines the PPP message format for the preceding packet example.

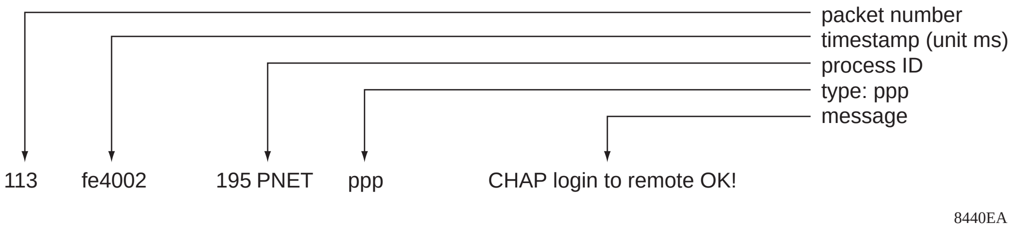


Figure 10-2. PPP Message Definitions

Appendix A
Technical Specifications

This appendix provides technical specifications for the Model RM356 Modem Router.

General Specification

Network Protocol and Standards Compatibility	
WAN Protocols:	PPP
Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP
Modem Standard:	V.90
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
Line:	RJ-11
Manager:	RS-232, RJ45

Index