Reference Guide for the Model RP114 Web Safe Router

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA
Phone 1-888-NETGEAR

SM-RP114NA-2
July 2001

Trademarks

NETGEAR and FirstGear are trademarks Netgear, 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 products described in this document without notice.

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

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

This 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 RP114 Web Safe 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 RP114 Web Safe Router gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

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

Certificate of the Manufacturer/Importer

It is hereby certified that the Model RP114 Web Safe 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.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the second 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

Refer to the Support Information Card that shipped with your Model RP114 Web Safe Router.

World Wide Web

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

Contents

Chapter 3
Preparing Your Network

Chapter 4
Basic Configuration of the Router

Chapter 5
Advanced Configuration of the Router

Chapter 6
Maintenance

Chapter 7
Using the Manager Interface for Initial Router Configuration

Chapter 8
Using the Manager Interface to Configure the Router for Internet Access

Chapter 9
Using the Manager Interface for Advanced System Maintenance

Chapter 10
Configuring Filters

Chapter 11
Troubleshooting

Appendix A
Technical Specifications

Appendix B
Network and Routing Basics

Glossary

Index

About This Guide

Congratulations on your purchase of the NETGEAR™ Model RP114 Web Safe Router.

The Model RP114 router provides connection for multiple personal computers (PCs) to the Internet through an external broadband access device (such as a cable modem or DSL modem) that is normally intended for use by a single PC.

➡ **Note:** If you are unfamiliar with networking and routing, refer to Appendix B, "Network and Routing Basics," to become more familiar with the terms and procedures used in this manual.

Technical Support

For help with any technical issues, contact Customer Support at 1-888-NETGEAR, or visit us on the Web at www.NETGEAR.com. The NETGEAR Web site includes an extensive knowledge base, answers to frequently asked questions, and a means for submitting technical questions online.

Related Publications

As you read this document, you may be directed to various RFC documents for further information. An RFC is a Request For Comment (RFC) published by the Internet Engineering Task Force (IETF), an open organization that defines the architecture and operation of the Internet. The RFC documents outline and define the standard protocols and procedures for the Internet. The documents are listed on the World Wide Web at *www.ietf.org* and are mirrored and indexed at many other sites worldwide.

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

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

Typographical 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.

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 there is the potential for incurring an electrical shock if you mishandle the equipment.

Chapter 1
Introduction

This chapter describes the features of the NETGEAR Model RP114 Web Safe Router and discusses planning considerations for installation. The software version described is v3.26.

About the Router

The Model RP114 Web Safe Router with 4-port switch connects your local area network (LAN) to the Internet through an external single-user access device such as a cable modem or DSL modem.

The Model RP114 router provides you with multiple Web content filtering options, plus browsing activity reporting and instant alerts -- both via e-mail. Parents and network administrators can establish restricted access policies based on time-of-day, Website addresses and address keywords, and share high-speed cable/DSL Internet access for up to 253 personal computers. Network Address Translation (NAT) protects you from hackers.

With minimum setup, you can install and use the router within minutes.

Key Features

The Model RP114 router provides the following features:

- Security
  - Parental control of web browsing and newsgroup access using Web Address (URL) keyword blocking
  - Auditing and e-mail reporting of web browsing activities
  - Blocking can be scheduled by day and time
  - Network Address Translation (NAT) hides local PCs from the Internet

  - Powerful packet filtering capabilities
  - Incoming port forwarding and DMZ for specific services
- Built in 4-port 10/100 Mbps Switch
  - Allows LAN connections at 10 megabits per second (Mbps) or 100 Mbps
  - Autosensing for Ethernet (10BASE-T) or Fast Ethernet (100BASE-Tx) transmissions
  - Auto Uplink™ (autosensing MDI/MDIX) configures each port for normal or uplink connection
  - Half-duplex or full-duplex operation
- Ethernet connection to a wide area network (WAN) device, such as a cable modem or DSL modem
  - RJ-45 interface allowing connection to a 10BASE-T device
- Protocol Support
  - IP routing
  - Dynamic extended Network Address Translation (NAT+) with port forwarding for operation with a single static or dynamic IP address
  - Dynamic Host Configuration Protocol (DHCP) server for dynamically assigning network configuration information to PCs on the LAN
  - DHCP client for dynamically obtaining configuration information from the Internet Service Provider (ISP)
  - DNS Proxy for simplified configuration
  - PPP over Ethernet (PPPoE) support
- Login capability

  Automatically executes user login for

  - RoadRunner cable modem service,
  - PPP over Ethernet accounts, PPTP login (for European service providers)
  - BigPond service (for Telstra Australia)
- Easy installation and management
  - Easy, web-based setup for configuration of most features
  - Built-in Manager interface for configuration of advanced features, accessible by Telnet Protocol

- Front panel LEDs for easy monitoring of status and activity
- Flash memory for firmware upgrade
- Five-year warranty, two years on power adapter
- Free technical support seven days a week, twenty-four hours a day

Content Filtering

With its content filtering features, the Model RP114 router prevents objectionable content from reaching your PCs. Its content filtering features include:

- Content filtering by domain or keyword
  The Model RP114 router uses content filtering to enforce your network’s Internet access policies. The router allows you to control access to Internet content by screening for keywords within Web URLs or newsgroup names.
- Logging of inappropriate use
  You can configure the Model RP114 router to log access to Web sites and to e-mail the log to you. You can also configure the router to send an immediate alert e-mail message to you whenever a local user attempts to access a blocked Web site.

Security

The Model RP114 router is equipped with several features designed to maintain security, as described in this section.

- PCs Hidden by NAT
  Network address translation (NAT) opens a temporary path to the Internet for requests originating from the local network. Requests originating from outside the LAN are discarded, preventing users outside the LAN from finding and directly accessing the PCs on the LAN.
- Port Forwarding with NAT
  Although NAT prevents Internet locations from directly accessing the PCs on the LAN, the router allows you to direct incoming traffic to specific PCs based on the service port number of the incoming request, or to one designated “DMZ” host computer. You can specify forwarding of single ports or ranges of ports.
- Packet Filtering
  The Model RP114 router provides extensive packet filtering capabilities. Packets are allowed or discarded based on their source or destination addresses, service port numbers, or raw data patterns within the packet.

Autosensing 10/100 Ethernet

With its internal, 4-port 10/100 switch, the Model RP114 router can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. The local LAN interface is autosensing and is capable of full-duplex or half-duplex operation.

The Model RP114 router incorporates Auto Uplink™ technology. Each LOCAL Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a 'normal' connection (e.g. connecting to a PC) or an 'uplink' connection (e.g. connecting to a router, switch, or hub). That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink™ will accommodate either type of cable to make the right connection.

TCP/IP

The Model RP114 router supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP).

For further information about TCP/IP, refer to Appendix B, “Network and Routing Basics.”

- IP Address Masquerading by Dynamic NAT+
  The Model RP114 router allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, an extension of Network Address Translation (NAT), is also known as IP address masquerading and allows the use of an inexpensive single-user ISP account.
- Automatic Configuration of Attached PCs by DHCP
  The Model RP114 router dynamically assigns 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 PCs.
- DNS Proxy
  When DHCP is enabled and no DNS addresses are specified, the router provides its own address as a DNS server to the attached PCs. The router obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.
- PPP over Ethernet (PPPoE)
  PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

Easy Installation and Management

You can install, configure, and operate the Model RP114 Web Safe Router within minutes after connecting it to the network. The following features simplify installation and management tasks:

- Browser-based management
  Browser-based configuration allows you to easily configure your router from almost any type of personal computer, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided and online help documentation is built into the browser-based Web Management Interface.
- Manager Interface
  The Manager Interface provides access to certain advanced features such as custom filters. You can access this interface from the network by using a Telnet client program.
- Visual monitoring
  The Model RP114 router's front panel LEDs provide an easy way to monitor its status and activity.

Maintenance and Support

NETGEAR offers the following features to help you maximize your use of the Model RP114 router:

- Flash memory for firmware upgrade
- Five-year warranty, two years on power adapter.
- Free technical support seven days a week, twenty-four hours a day

Chapter 2
Setting Up the Hardware

This chapter describes the Model RP114 Web Safe Router hardware and provides instructions for installing it.

Package Contents

The product package should contain the following items:

- Model RP114 Web Safe Router
- AC power adapter, 12 V DC output
- Category 5 (Cat 5) Ethernet cable, straight-through wiring
- *Model RP114 Resource* CD, including:
  - This guide
  - Application Notes
- *RP114 Cable/DSL Web Safe Router Installation Guide*
- Registration and Warranty Card
- Support Information Card

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the router for repair.

Local Network Hardware Requirements

The Model RP114 Web Safe Router is intended for use in a network of personal computers (PCs) that are interconnected by twisted-pair Ethernet cables.

PC Requirements

To install and run the Model RP114 router over your network of PCs, each PC must have the following:

- An installed Ethernet Network Interface Card (NIC).
- A connection to the network via a hub or switch. If all PCs on the network will not run at the same speed (10 Mbps or 100 Mbps), you need to use a dual-speed hub or switch. The Model RP114 router provides a 4-port switch capable of either 10 Mbps or 100 Mbps operation. Links operating at 100 Mbps must be connected with Category 5 cable.

Access Device Requirement

The shared broadband access device (cable modem or DSL modem) must provide a standard 10BASE-T Ethernet interface.

The Router’s Front Panel

The front panel of the Model RP114 Web Safe Router (Figure 2-1) contains port connections and status LEDs.

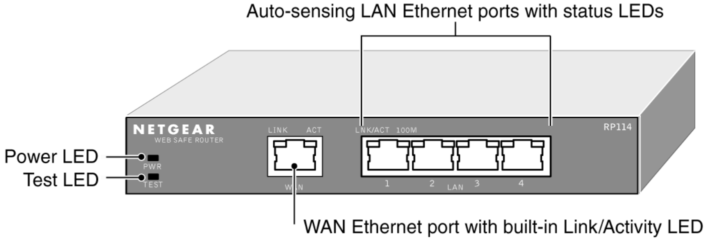

Auto-sensing LAN Ethernet ports with status LEDs
NETGEAR
WEB SAFE ROUTER
Power LED
Test LED
PWR
TEST
LINK
ACT
WAN
LNK/ACT
100M
1
2
LAN
3
4
RP114
WAN Ethernet port with built-in Link/Activity LED

Figure 2-1. RP114 Front Panel

You can use some of the LEDs to verify connections. 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 Off	Power is supplied to the router. Power is not supplied to the router.
TEST	On Off Blinking	The system is not ready or has failed to start up. The system is ready and running. The system is initializing.
WAN		
LNK	On	The WAN port has detected a link with an attached device.
ACT (Activity)	Blinking	Data is being transmitted or received by the WAN port.
LAN		
LNK/ACT (Link/Activity)	On Blinking	The LAN port has detected a link with an attached device. Data is being tranmitted or received by the LAN port.
100 (100 Mbps)	On Off	The LAN is operating at 100 Mbps. The LAN is operating at 10 Mbps.

The Router's Rear Panel

The rear panel of the Model RP114 router is shown in Figure 2-2.

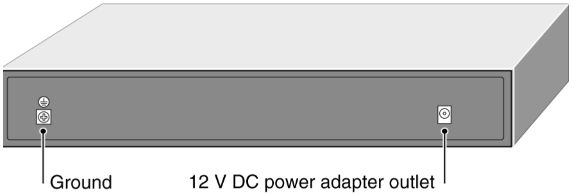


Figure 2-2. RP114 Rear Panel

The rear panel contains the following features:

- 12 VDC power adapter outlet
- Factory Default Reset pushbutton
- Ground lug

Connecting the Router

Before using your router, you need to do the following:

- Connect your local Ethernet network to the LAN port(s) of the router (described next).
- Connect your cable or DSL modem to the WAN port of the router (see page 2-5).
- Connect the power adapter (see page 2-5).

Connecting to your Local Ethernet Network

Your local network will attach to the router port or ports marked LAN. The LAN ports are capable of operation at either 10 Mbps (10BASE-T) or 100 Mbps (100BASE-Tx), depending on the Ethernet interface of the attached PC, hub, or switch. For any connection which will operate at 100 Mbps, you must use a Category 5 (CAT5) rated cable, such as the white Ethernet cable included with the router.

The Model RP114 router incorporates a four-port switch for connection to your local network. To connect the Model RP114 router to your LAN:

- Connect up to four PCs directly to any of the four LAN ports of the router using standard Ethernet cables.

If your local network consists of more than four hosts, you will need to connect your router to another hub or switch:

- Connect any LAN port of your Model RP114 router to any port of an Ethernet hub or switch using a standard or crossover Ethernet cable.

  Because the Model RP114 router is capable of automatically sensing the polarity of the Ethernet connection, you can connect to the other hub's normal or uplink port, using a standard or crossover Ethernet cable. The LAN port of your Model RP114 router will automatically configure itself for proper operation.

Connecting to Your Internet Access Device

To connect the router to the Internet (or WAN):

1. Connect the router's WAN port to the 10BASE-T Ethernet port on your existing Internet access device (your cable modem or DSL modem).

Note: The attached modem device must provide a standard 10BASE-T Ethernet connection. The Model RP114 router does not include a cable for this connection. Instead, use the Ethernet cable provided with your access device or any other standard 10BASE-T Ethernet cable. If you are using a DSL modem, the modem's connection to the phone line remains unchanged.

Note: The Ethernet cable supplied by your ISP for connecting to your cable or DSL modem may be an Ethernet crossover cable rather than a straight-through cable. It is important to use this cable to connect the modem to your router, not to connect your PCs to your router.

Connecting the Power Adapter

To connect the router to the power adapter:

1. Plug the connector of the power adapter into the 12 VDC adapter outlet on the rear panel of the router.
2. Plug the other end of the adapter into a standard wall outlet.
3. Verify that the PWR LED on the router is lit.

Verifying Power

After connecting the power adapter to the router and a power source, the router powers on automatically. Complete the following steps to verify that power is correctly applied to the router:

1. When power is first applied, verify that the PWR LED is on.
2. Verify that the TEST LED begins to blink within a few seconds.
3. After approximately 30 seconds, verify that:
    a. The TEST LED is not lit.
    b. The LAN LNK/ACT LEDs are lit for any local ports that are connected.
    c. The WAN LNK LED is lit.

       If a LNK or LNK/ACT LED is lit, a link has been established to the connected device.
4. If a LOCAL port is connected to a 100 Mbps device, verify that the 100 LED is lit.

You are now ready to begin configuration of your network, as described in the following chapter.

Chapter 3
Preparing Your Network

This chapter describes how to prepare your PC network to connect to the Internet through the Model RP114 Web Safe Router and how to order broadband Internet service from an Internet service provider (ISP).

Preparing Your Personal Computers for IP Networking

The Model RP114 Web Safe Router uses the Transmission Control Protocol/Internet Protocol (TCP/IP). In order to access the Internet through the router, each PC on your network must have TCP/IP installed and selected as the networking protocol.

Note: In this chapter, we use the term “PC” to refer to personal computers in general, and not necessarily Windows computers.

Most operating systems include the software components you need to install and use TCP/IP on your PC:

- Windows® 95 or later (including Windows NT®) includes the software components for establishing a TCP/IP network.
- Windows 3.1 does not include a TCP/IP component. You need to purchase a third-party TCP/IP application package such as NetManage Chameleon.
- Macintosh Operating System 7 or later includes the software components for establishing a TCP/IP network.
- All versions of UNIX or Linux include TCP/IP components.

Follow the instructions provided with your operating system or networking software to install TCP/IP on your computer. Although TCP/IP is built into the Windows operating system (starting with Windows 95), you need to enable and configure it as described in "Configuring Windows 95 or later for IP Networking" on page 3-2. To configure the Macintosh, see "Configuring the Macintosh for IP Networking on page 3-5.

In your IP network, all PCs and the router must be assigned IP addresses. Each PC must also have certain other IP configuration information such as a subnet mask (netmask), a domain name server (DNS) address, and a default gateway address. In most cases, you should install TCP/IP so that the PC obtains its specific network configuration information from a DHCP server during bootup. For a detailed explanation of the meaning and purpose of these configuration items, refer to "Appendix B, "Network and Routing Basics."

The Model RP114 router is shipped preconfigured as a DHCP server. The router assigns the following TCP/IP configuration information automatically when the PCs are rebooted:

- PC or workstation IP addresses—192.168.0.2 through 192.168.0.31
- Subnet mask—255.255.255.0
- Gateway address (the router)—192.168.0.1

These addresses are part of the IETF-designated private address range for use in private networks.

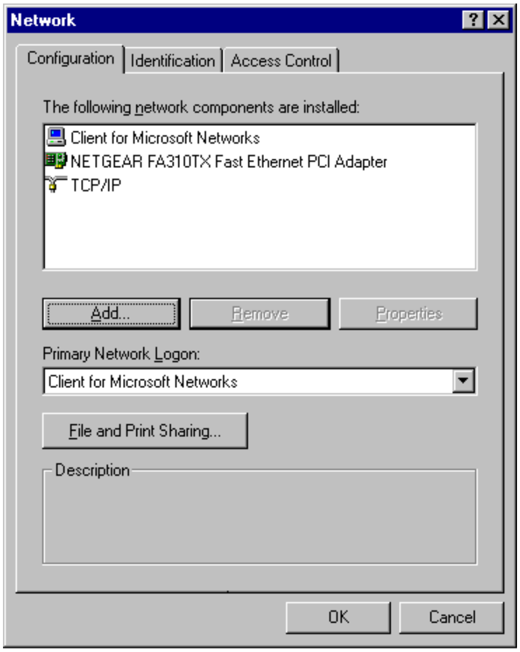
Configuring Windows 95 or later for IP Networking

As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

To configure Microsoft® Windows 95 or later for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.

   The Network window opens, which displays a list of installed components:



The following network components are installed:

Client for Microsoft Networks
NETGEAR FA310TX Fast Ethernet PCI Adapter
TCP/IP

Primary Network Logon: Client for Microsoft Networks

You must have an Ethernet adapter, the TCP/IP protocol, and Client for Microsoft Networks.

Note: It is not necessary to remove any other network components shown in the Network window in order to install the adapter, TCP/IP, or Client for Microsoft Networks.

If you need the adapter:

a. Click the Add button.

b. Select Adapter, and then click Add.

c. Select the manufacturer and model of your Ethernet adapter, and then click OK.

If you need TCP/IP:

a. Click the Add button.

b. Select Protocol, and then click Add.

c. Select Microsoft.

   d. Select TCP/IP, and then click OK.

   If you need Client for Microsoft Networks:

   a. Click the Add button.

   b. Select Client, and then click Add.

   c. Select Microsoft.

   d. Select Client for Microsoft Networks, and then click OK.

3. Restart your PC for the changes to take effect.

Configuring TCP/IP Properties

After the TCP/IP protocol components are installed, each PC must be assigned specific information about itself and resources that are available on its network. The simplest way to configure this information is to allow the PC to obtain the information from the internal DHCP server of the Model RP114 router.

> **Note:** If an ISP technician configured your PC during the installation of a broadband modem, or if you configured it using instructions provided by your ISP, you may need to copy the current configuration information for use in the configuration of your router. Refer to "Obtaining ISP Configuration Information (Windows)" on page 3-8 or "Obtaining ISP Configuration Information (Macintosh)" on page 3-9 for further information.

If you are using DHCP with the recommended default addresses, you can configure your PCs by following these steps:

1. Install TCP/IP on each PC, leaving the PC configured to obtain configuration settings automatically (by DHCP).
2. Physically connect the PCs and the router using a hub or a direct connection.
3. Restart the router and allow it to boot.
4. Restart each PC.

Verifying TCP/IP Properties (Windows)

After your PC is configured and has rebooted, you can check the TCP/IP configuration using the Windows 95, 98, and Millenium utility *winipcfg.exe* (for Windows NT systems, use *ipconfig.exe*).

To check your PC's TCP/IP configuration:

1. On the Windows taskbar, click the Start button, and then click Run.

   The Run window opens.

2. Type `winipcfg`, and then click OK.

   The IP Configuration window opens, which lists (among other things), your IP address, subnet mask, and default gateway.

3. Select your Ethernet adapter.

   The window is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

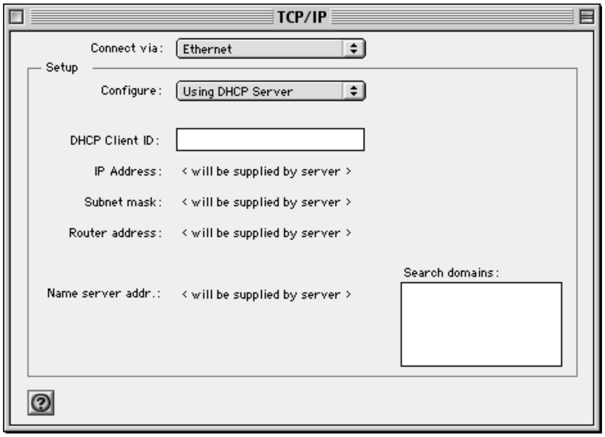
   - The IP address is between 192.168.0.2 and 192.168.0.31
   - The subnet mask is 255.255.255.0
   - The default gateway is 192.168.0.1

Configuring the Macintosh for IP Networking

Beginning with Macintosh Operating System 7, TCP/IP is already installed on the Macintosh. On each networked Macintosh, you will need to configure TCP/IP to use DHCP by following these steps:

1. From the Apple menu, select Control Panels, then TCP/IP.

   The TCP/IP Control Panel opens:



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Name server addr.: < will be supplied by server >

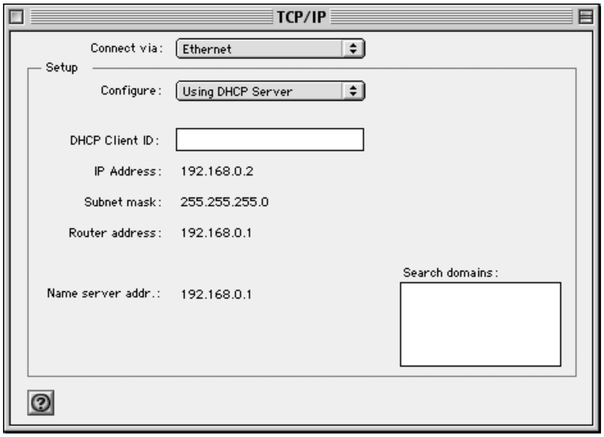
Search domains:

2. From the “Connect via” box, select your Macintosh’s Ethernet interface.
3. From the “Configure” box, select Using DHCP Server.

   You can leave the DHCP Client ID box empty.
4. Close the TCP/IP Control Panel.
5. Repeat this for each Macintosh on your network.

Verifying TCP/IP Properties (Macintosh)

After your Macintosh is configured and has rebooted, you can check the TCP/IP configuration by returning to the TCP/IP Control Panel. From the Apple menu, select Control Panels, then TCP/IP.



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: 192.168.0.2

Subnet mask: 255.255.255.0

Router address: 192.168.0.1

Search domains:

Name server addr.: 192.168.0.1

The panel is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

- The IP Address is between 192.168.0.2 and 192.168.0.31
- The Subnet mask is 255.255.255.0
- The Router address is 192.168.0.1

If you do not see these values, you may need to restart your Macintosh or you may need to switch the “Configure” setting to a different option, then back again to “Using DHCP Server”.

Your Internet Account

For access to the Internet, you need to contract with an Internet service provider (ISP) for a single-user Internet access account using an external broadband access device such as a cable modem or DSL modem. This modem must be a separate physical box (not a card) and must provide an Ethernet port intended for connection to a Network Interface Card (NIC) in a PC.

For a single-user Internet account, your ISP supplies TCP/IP configuration information for one PC. With a typical account, much of the configuration information is dynamically assigned when your PC is first booted up while connected to the ISP, and you will not need to know that dynamic information.

In order to share the Internet connection among several computers, your router takes the place of the single PC, and you need to configure it with the TCP/IP information that the single PC would normally use. When the router's WAN port is connected to the broadband modem, the router appears to be a single PC to the ISP. The router then allows the PCs on the local network to masquerade as the single PC to access the Internet through the broadband modem. The method used by the router to accomplish this is called Network Address Translation (NAT) or IP masquerading.

Login Protocols

Some ISPs require a special login protocol. In this case, you will need to know what type of protocol is used, and you will need a login name and password. Some common protocols are:

- PPP over Ethernet (PPPoE)
  Two common PPPoE clients are WinPOET and EnterNet.
- RoadRunner
  Not all RoadRunner service areas require a login protocol. If your ISP is RoadRunner, you should ask whether your PC must run a RoadRunner login program.
- PPTP
  PPTP is a VPN client, but it is also used in Europe by Alcatel's ANT system and others as an account login client.
- BigPond Authentication

After your network and router are configured, the router will perform the login task when needed, and you will no longer need to login from your PC.

Account Information

Unless these items are dynamically assigned by the ISP, your ISP should give you the following basic information for your account:

- An IP address and subnet mask
- A gateway IP address, which is the address of the ISP's router
- One or more domain name server (DNS) IP addresses
- Host name and domain suffix

  For example, your account's full server names may look like this:

  `mail.xxx.yyy.com`

  In this example, the domain suffix is `xxx.yyy.com`.

If any of these items are dynamically supplied by the ISP, your router automatically acquires them. If an ISP technician configured your PC during the installation of the broadband modem, or if you configured it using instructions provided by your ISP, you need to copy configuration information from your PC's Network TCP/IP Properties window (or Macintosh TCP/IP Control Panel) before reconfiguring your PC for use with the router. These procedures are described next.

Obtaining ISP Configuration Information (Windows)

As mentioned above, you may need to collect configuration information from your PC so that you can use this information when you configure the Model RP114 router. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the router for Internet access:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.

   The Network window opens, which displays a list of installed components.
3. Select TCP/IP, and then click Properties.

   The TCP/IP Properties dialog box opens.
4. Select the IP Address tab.

   If an IP address and subnet mask are shown, write down the information. If an address is present, your account uses a fixed (static) IP address. If no address is present, your account uses a dynamically-assigned IP address. Click "Obtain an IP address automatically".

5. Select the Gateway tab.

   If an IP address appears under Installed Gateways, write down the address. This is the ISP's gateway address. Select the address and then click Remove to remove the gateway address.

6. Select the DNS Configuration tab.

   If any DNS server addresses are shown, write down the addresses. If any information appears in the Host or Domain information box, write it down. Click Disable DNS.

7. Click OK to save your changes and close the TCP/IP Properties dialog box.

   You are returned to the Network window.

8. Click OK.

9. Reboot your PC at the prompt. You may also be prompted to insert your Windows CD.

Obtaining ISP Configuration Information (Macintosh)

As mentioned above, you may need to collect configuration information from your Macintosh so that you can use this information when you configure the Model RP114 router. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the router for Internet access:

1. From the Apple menu, select Control Panels, then TCP/IP.

   The TCP/IP Control Panel opens, which displays a list of configuration settings. If the "Configure" setting is "Using DHCP Server", your account uses a dynamically-assigned IP address. In this case, close the Control Panel and skip the rest of this section.

2. If an IP address and subnet mask are shown, write down the information.

3. If an IP address appears under Router address, write down the address. This is the ISP's gateway address.

4. If any Name Server addresses are shown, write down the addresses. These are your ISP's DNS addresses.

5. If any information appears in the Search domains information box, write it down.

6. Change the "Configure" setting to "Using DHCP Server".

7. Close the TCP/IP Control Panel.

Ready for Configuration

After configuring all of your PCs for TCP/IP networking and connecting them to the LOCAL network of your Model RP114 router, you are ready to access and configure the router. Proceed to the next chapter.

Chapter 4
Basic Configuration of the Router

This chapter describes how to perform the basic configuration of your Model RP114 Web Safe Router using the Setup Wizard, which walks you through the configuration process for your Internet connection. This chapter also describes the configuration for content filtering.

Configuring for Internet Access

In order to use the browser-based Web Configuration Manager, your PC must have a web browser program installed such as Microsoft Internet Explorer or Netscape Navigator. Because the Configuration Manager uses Java, your Web browser must be Java-enabled and support HTTP uploads. NETGEAR recommends using Netscape Navigator 3.0 or above. Free browser programs are readily available for Windows, Macintosh, or UNIX/Linux.

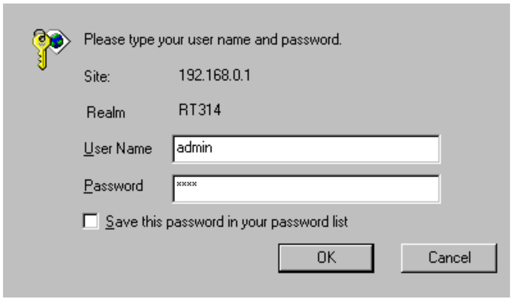
To configure for Internet access using your browser:

1. Turn on the router and wait for initialization to complete.

   Allow at least one minute and verify that the TEST LED is off.

2. Reboot your PC to obtain DHCP configuration from the router.
3. Launch your web browser.
4. In the Address box of your browser, type **http://192.168.0.1** and press ENTER.

A login window opens as shown in Figure 4-1 below:.



Please type your user name and password.

Site: 192.168.0.1

Realm RT314

User Name admin

Password ****

□ Save this password in your password list

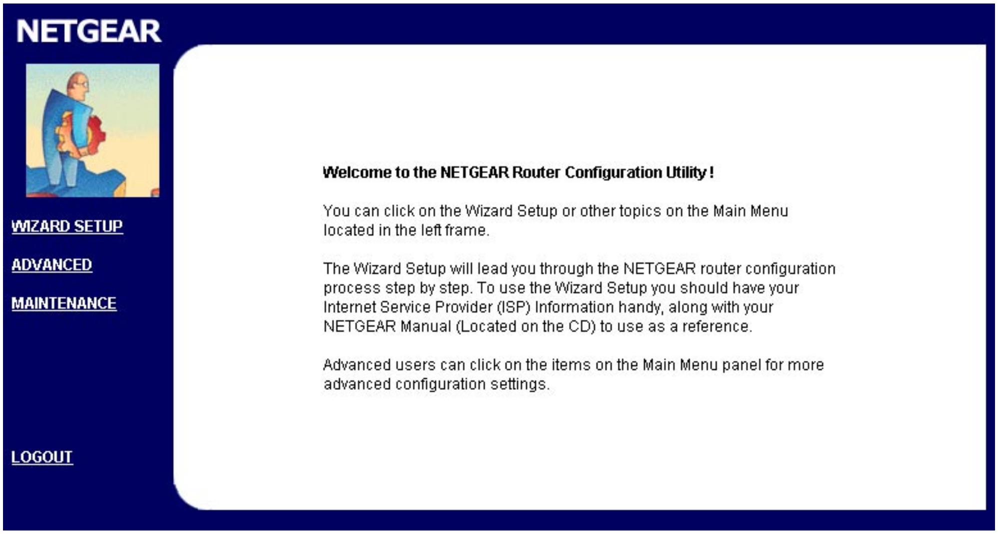
Figure 4-1. Login window

This screen may have a different appearance in other browsers.

5. Type **`admin`** in the User Name box, **`1234`** in the Password box, and then click OK.

   If your router password was previously changed, enter the current password.

6. In the opening screen, shown in Figure 4-2, select WIZARD SETUP.



Welcome to the NETGEAR Router Configuration Utility !

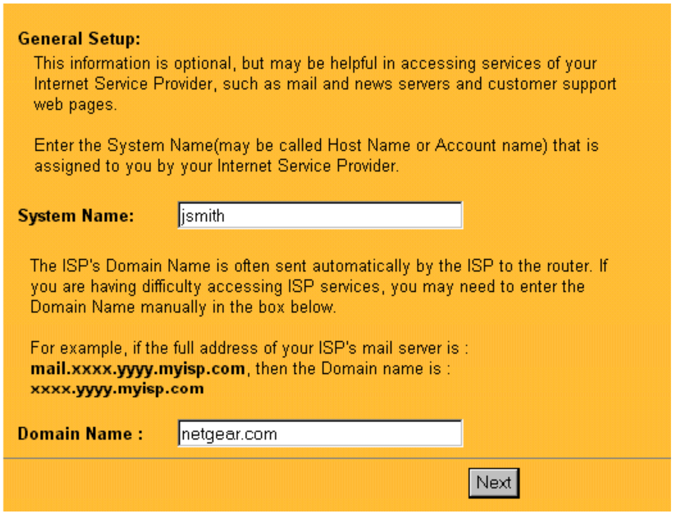
You can click on the Wizard Setup or other topics on the Main Menu located in the left frame.

The Wizard Setup will lead you through the NETGEAR router configuration process step by step. To use the Wizard Setup you should have your Internet Service Provider (ISP) Information handy, along with your NETGEAR Manual (Located on the CD) to use as a reference.

Advanced users can click on the items on the Main Menu panel for more advanced configuration settings.

Figure 4-2. Browser-based configuration main menu

7. In the first Wizard screen, enter your account's Host Name and Domain Name, as shown in Figure 4-3 below:



General Setup:

This information is optional, but may be helpful in accessing services of your Internet Service Provider, such as mail and news servers and customer support web pages.

Enter the System Name(may be called Host Name or Account name) that is assigned to you by your Internet Service Provider.

System Name: jsmith

The ISP's Domain Name is often sent automatically by the ISP to the router. If you are having difficulty accessing ISP services, you may need to enter the Domain Name manually in the box below.

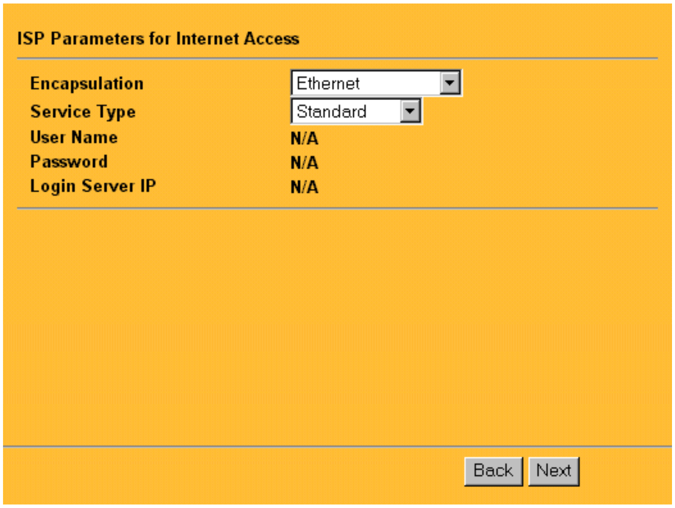
For example, if the full address of your ISP's mail server is : **mail.xxxx.yyyy.myisp.com**, then the Domain name is : **xxxx.yyyy.myisp.com**

Domain Name : netgear.com

Figure 4-3. Browser-based Setup Wizard, first screen

These parameters may be necessary to access your ISP's services such as mail or news servers. If you leave the Domain Name field blank, the router will attempt to learn the domain automatically from the ISP. If this is not successful, you will need to enter it manually.

8. Click on Next to go to the ISP Parameters screen, shown in Figure 4-4 below:



ISP Parameters for Internet Access

Encapsulation	Ethernet
Service Type	Standard
User Name	N/A
Password	N/A
Login Server IP	N/A

Figure 4-4. Browser-based Setup Wizard, second screen

This screen determines whether a login program will be run.

a. If your service provider does not require a login program, leave Encapsulation as Ethernet and proceed to Step 9.

b. If your service provider uses PPP over Ethernet (PPPoE), select Encapsulation as PPPoE, and enter these additional parameters:

- If your connection supports multiple ISPs, enter the Service Name of the one you use. Otherwise leave Service Name blank.
- Enter the PPPoE login user name and password provided by your ISP. These fields are case sensitive.
- If you wish to change the login timeout, enter a new value in seconds.

Proceed to Step 9.

c. (Europe) If your service provider uses Alcatel's ANT (ADSL Network Termination) with PPTP as a login method, select Encapsulation as PPTP, and enter these additional parameters:

- Enter the PPTP login user name and password provided by your ISP. These fields are case sensitive.
- If you wish to change the login timeout, enter a new value in seconds.

- If provided by your ISP, enter your PPTP IP Address and the Server IP Address of their PPTP Server.
- If provided by your ISP, enter the Connection ID/Name for your service. Otherwise leave this field blank.

Proceed to Step 9.

d. If your service provider is RoadRunner AND you are required to run a RoadRunner login program, leave Encapsulation as Ethernet and select Service Type as either RR-Manager or RR-Toshiba. Enter these additional parameters:.

- If your cable modem is Toshiba, select RR-Toshiba. Otherwise select RR-Manager.
- Enter the user name and password provided by your ISP. These fields are case sensitive.
- If RoadRunner provided an authentication server address, enter it as Login Server IP address. Otherwise, leave this field as 0.0.0.0.

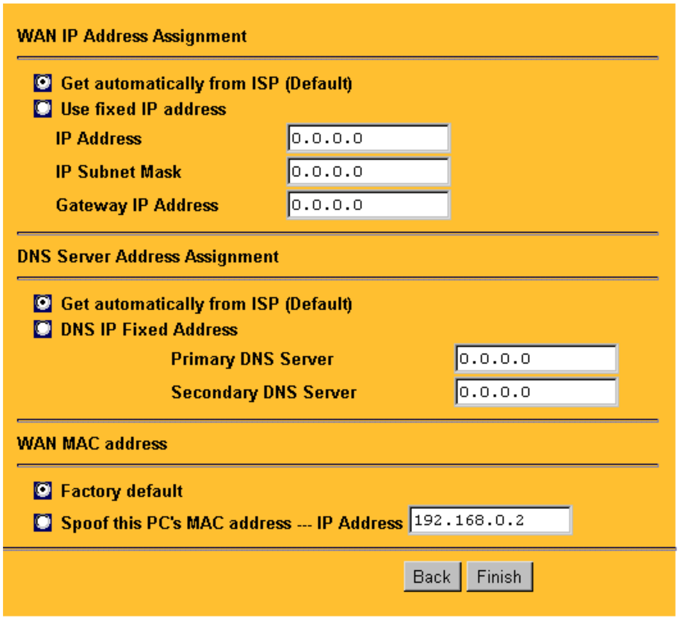
Not all RoadRunner regions require a login program. If your region does not require a login, leave Service Type as Standard.

Proceed to Step 9.

e. Australia only: If your service provider is Telstra Bigpond, select Service Type as Bigpond/Telstra, and enter these additional parameters:

- Enter the login user name and password provided by Bigpond. These fields are case sensitive.
- If Bigpond provided an authentication server address, enter it as Login Server IP address. Otherwise, leave this field as 0.0.0.0.

9. Click on Next to go to the final Wizard screen shown in Figure 4-5 below.



WAN IP Address Assignment

● Get automatically from ISP (Default)
○ Use fixed IP address

IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
Gateway IP Address	0.0.0.0

DNS Server Address Assignment

● Get automatically from ISP (Default)
○ DNS IP Fixed Address

Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0

WAN MAC address

● Factory default
○ Spoof this PC's MAC address --- IP Address 192.168.0.2

Figure 4-5. Browser-based Setup Wizard, third screen

This screen provides setup for the following parameters:

a. WAN IP Address Assignment: Unless your ISP has assigned a fixed permanent IP address for your use, select "Get automatically from ISP". Otherwise, enter your IP Address, Subnet Mask, and the IP Address of your ISP’s gateway router.

b. DNS Server Address Assignment: If you know that your ISP does not automatically transmit DNS addresses to the router during login, select “DNS IP Fixed Address” and enter the IP address of the ISP’s Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

   A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP transfers the IP addresses of one or two DNS servers to your router during login. If the ISP does not transfer an address, you must obtain it from the ISP and enter it manually here. If you enter an address here, you should reboot your PCs after configuring the router.

c. WAN MAC address: If your ISP allows access by only one specific PC’s Ethernet MAC address, select "Spoof this PC’s MAC address" and enter the IP address of that PC.

- For convenience, the IP address of the PC you are now using should already appear. If this is not the PC whose MAC address is to be used, enter that PC's IP address.
- Some ISPs will register the Ethernet MAC address of the network interface card in your PC when your account is first opened. They will then only accept traffic from the MAC address of that PC. This feature allows your router to masquerade as that PC by using its MAC address.

10. Click on Finish.
11. Click on the NETGEAR website address to test your Internet connection.

    If the NETGEAR website does not appear within one minute, refer to Chapter 11, "Troubleshooting".

Your router is now configured to provide Internet access for your network. When your router and PCs are configured correctly, your router automatically accesses the Internet when one of your LAN devices requires access. It is not necessary to run a dialer application such as Dial-Up Networking or RoadRunner Login to connect, log in, or disconnect. These functions are performed by the router as needed.

To access the Internet from any PC connected to your router, launch a browser such as Microsoft Internet Explorer or Netscape Navigator. You should see the router's Internet LED blink, indicating communication to the ISP. The browser should begin to display a Web page.

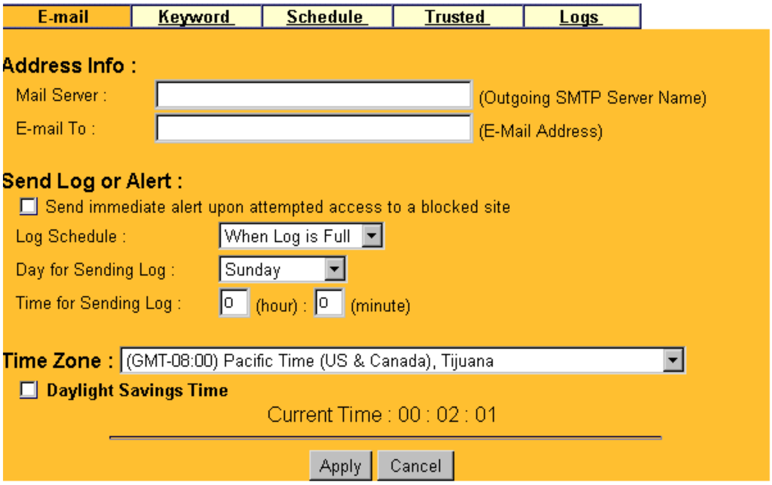
Configuring for Content Filtering

The Model RP114 Web Safe Router provides you with Web content filtering options, plus browsing activity reporting and instant alerts via e-mail. Parents and network administrators can establish restricted access policies based on time-of-day, web and newsgroup addresses and web and newsgroup address keywords.

To configure these features of your router, click on the Advanced heading in the Main Menu of the browser interface. From the subheadings shown, click on Content Filter. The tabs described below contain the settings for content filtering.

E-Mail

In order to receive logs and alerts by email, you must provide your email information in the E-Mail tab:



Address Info :

Mail Server : (Outgoing SMTP Server Name)

E-mail To : (E-Mail Address)

Send Log or Alert :

☐ Send immediate alert upon attempted access to a blocked site

Log Schedule : When Log is Full

Day for Sending Log : Sunday

Time for Sending Log : 0 (hour) : 0 (minute)

Time Zone : (GMT-08:00) Pacific Time (US & Canada), Tijuana

☐ **Daylight Savings Time**

Current Time : 00 : 02 : 01

- Mail Server
  Specifies the name of your outgoing (SMTP) mail server. You can enter either the server name (such as mail.myISP.com) or its IP Address. If you leave this box blank, log and alert messages are not sent via e-mail.
- E-mail To
  Specifies the e-mail address to which logs and alerts are sent. This e-mail address will be used as the From address. If you leave this box blank, the log is not sent via e-mail to any address.

You can specify that logs are automatically sent to the specified e-mail address with these options:

- Send immediate alert upon attempted access to a blocked site
  Check this box if you would like immediate notification of inappropriate access attempts.
- Log Schedule
  Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
- Day for Sending Log
  Specifies which day of the week to send the log. Relevant when the log is sent weekly or daily.
- Time for Sending Log
  Specifies the time of day to send the log, using 23:59 notation. Relevant when the log is sent daily.

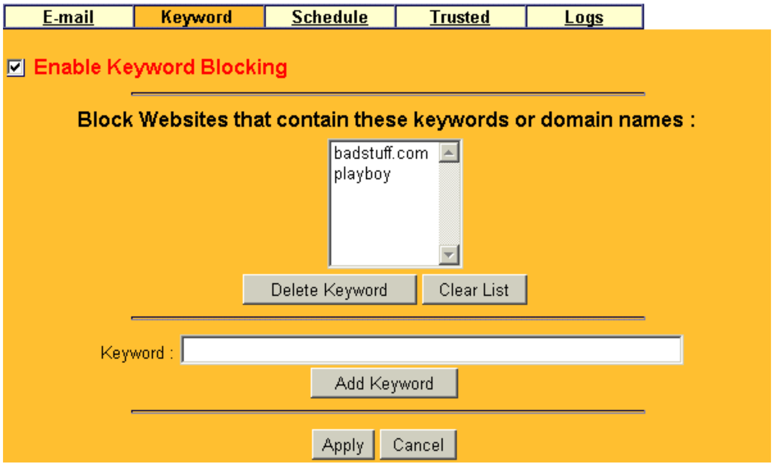
- Time Zone
  Specify your local time zone and click Apply. This setting will be used for the blocking schedule and also for time-stamping log entries.
- Daylight Savings Time
  Check this box if your time zone is currently under daylight savings time.

If the Weekly, Daily or Hourly option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, the log is cleared from the router’s memory. If the router cannot e-mail the log file, the log buffer may fill up. In this case, the router overwrites the log and discards its contents.

The Model RP114 router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet. This menu displays the current time.

Keyword

The Model RP114 router allows you to restrict access based on web and newsgroup addresses and web and newsgroup address keywords. Up to 255 entries are supported in the Keyword list. The Keyword tab is shown below:



☑ Enable Keyword Blocking

Block Websites that contain these keywords or domain names :

badstuff.com
playboy

Keyword :

To enable keyword blocking, check Enable Keyword Blocking, then click Apply. Be sure that a time period for blocking is specified on the Schedule setup screen.

To add a keyword or domain, type it in the Keyword box, click Add Keyword, then click Apply.

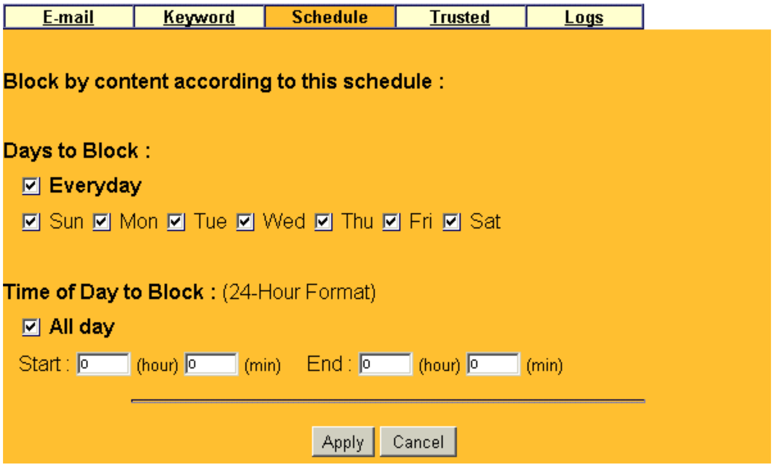
To delete a keyword or domain, select it from the list, click Delete Keyword, then click Apply.

Keyword application examples:

- If the keyword "XXX" is specified, the URL <http://www.badstuff.com/xxx.html> is blocked, as is the NNTP newsgroup alt.XXX.
- If the keyword “.com” is specified, only websites with other domain suffixes (such as .edu or .gov) can be viewed.
- If you wish to block all Internet browsing access during a scheduled period, enter the keyword “.” and set the schedule in the Schedule menu.

Schedule

The Model RP114 router allows you to specify when blocking will be enforced. The Schedule tab is shown below:



Block by content according to this schedule :

Days to Block :

☑ **Everyday**

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time of Day to Block : (24-Hour Format)

☑ **All day**

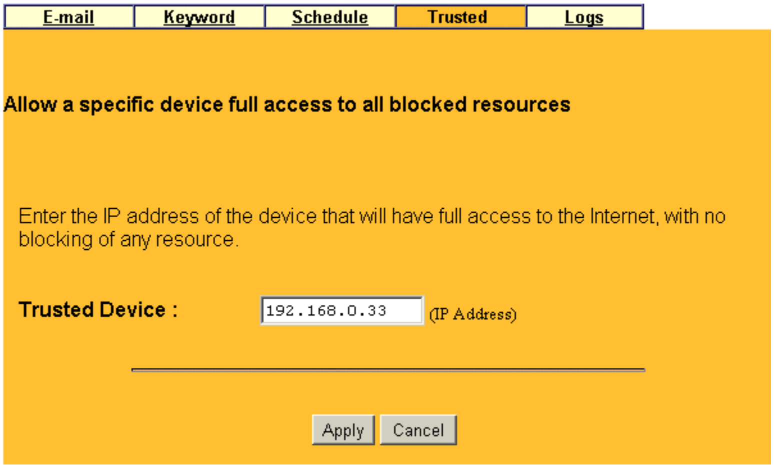
Start : 0 (hour) 0 (min) End : 0 (hour) 0 (min)

- Days to Block
  Select days to block by checking the appropraite boxes. Select Everyday to check the boxes for all days. Click Apply.
- Time of Day to Block
  Select a start and end time in 23:59 format. Select All day for 24 hour blocking. Click Apply.

Trusted

The Model RP114 router allows you to specify one Trusted User, which is a PC that will be exempt from blocking and logging. Since the Trusted User will be identified by an IP address, you should configure that PC with a fixed IP address.

The Trusted tab is shown below.



Allow a specific device full access to all blocked resources

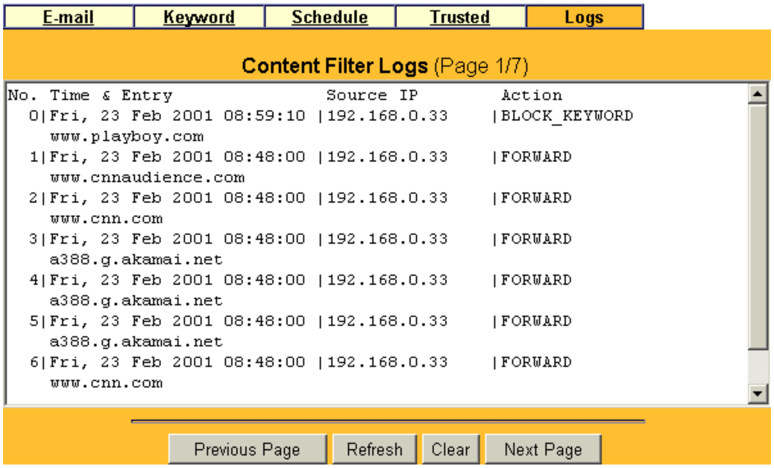
Enter the IP address of the device that will have full access to the Internet, with no blocking of any resource.

Trusted Device : 192.168.0.33 (IP Address)

To specify a Trusted User, enter that PC’s IP address in the Trusted User box and click Apply.

Logs

The log is a detailed record of what websites you have accessed or attempted to access. Up to 128 entries are stored in the log. Log entries will only appear when keyword blocking is enabled, and no log entries will be made for the Trusted User.



Content Filter Logs (Page 1/7)

```
No. Time & Entry                   Source IP         Action
  0|Fri, 23 Feb 2001 08:59:10 |192.168.0.33     |BLOCK_KEYWORD
    www.playboy.com
  1|Fri, 23 Feb 2001 08:48:00 |192.168.0.33     |FORWARD
    www.cnnaudience.com
  2|Fri, 23 Feb 2001 08:48:00 |192.168.0.33     |FORWARD
    www.cnn.com
  3|Fri, 23 Feb 2001 08:48:00 |192.168.0.33     |FORWARD
    a388.g.akamai.net
  4|Fri, 23 Feb 2001 08:48:00 |192.168.0.33     |FORWARD
    a388.g.akamai.net
  5|Fri, 23 Feb 2001 08:48:00 |192.168.0.33     |FORWARD
    a388.g.akamai.net
  6|Fri, 23 Feb 2001 08:48:00 |192.168.0.33     |FORWARD
    www.cnn.com
```

Log entries are described in Table 4-1

Table 4-1. Log entry descriptions

Field	Description
No.	The index number of the content filter log entries. 128 entries are available numbered from 0 to 127. The log will keep the record of the latest 128 entries.
Time and Entry	The time the log entry was recorded. Below the time is the name or IP address of the website visited or attempted to access.
Source IP	The IP address of the initiating device for this log entry.
Action	This field displays whether the packet was blocked, forwarded, or neither (BLOCK, FORWARD, or NONE). "NONE" means that no action is dictated by this rule.

Log viewing buttons are described in Table 4-2

Table 4-2. Log display buttons

Field	**Description**
Previous Page	Click this button to view the previous log page.
Refresh	Click this button to refresh the log screen.
Clear	Click this button to clear the log entries.
Next Page	Click this button to view the next log page.

Chapter 5
Advanced Configuration of the Router

This chapter describes how to configure the advanced features of your Model RP114 Web Safe Router. These features can be found by clicking on the Advanced heading in the Main Menu of the browser interface. One advanced feature, Content Filtering, is described in the previous chapter.

System Settings

The first feature category under the Advanced heading is System settings. These are general purpose settings.

System Tab

The System Tab contains fields for setting the System (Host) Name and Domain Name. These parameters may be necessary to access your ISP's services such as mail or news servers.

- System Name
  This is the host or account name given by your ISP for naming your PC. It is often the primary email name of your account.This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
- Domain Name
  This is the extended domain suffix that follows your ISP server names. For example, if your ISP's mail server is mail.sfbay.myISP.com, then your Domain Name is sfbay.myISP.com.

Dynamic DNS

Your router supports Dynamic Domain Name Service (DDNS). In a Dynamic DNS service, an IP registry server provides a public central database where dynamically-assigned IP addresses can be stored and retrieved by hostname lookup. The Dynamic DNS server also stores password-protected e-mail addresses along with IP addresses and hostnames and accepts queries based on e-mail addresses.

To utilize this service, you must register with the Dynamic DNS service provider, who will give you a password or key. At this time, the Model RP114 router only supports DynDNS service. For more information, visit www.dyndns.org.

The configuration fields for Dynamic DNS are shown in Table 5-1:

Table 5-1. Dynamic DNS configuration fields

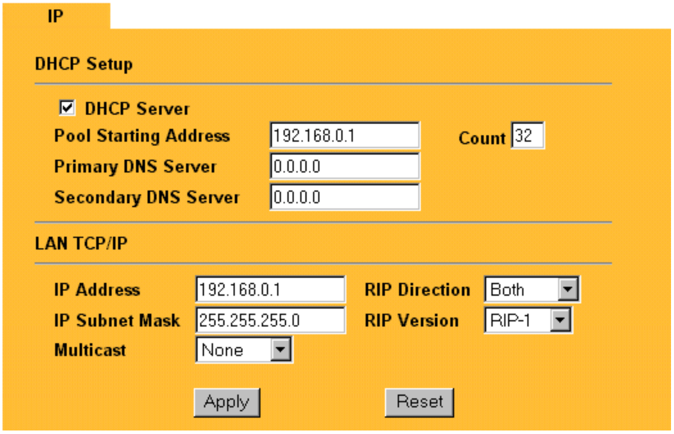
Field	Description
Active	Use this field to activate or deactivate dynamic DNS registration.
Service Provider	Select a dynamic DNS service provider.
Host Name	Enter the static host name that will link to your dynamic IP address.
E-Mail Address	Enter your email address for administrative contact.
User	Enter the user name of your dynamic DNS account.
Password	Enter the password of your dynamic DNS account.
Enable Wildcard	DynDNS.org allows the use of wildcards in resolving your URL. Enabling the wildcard feature for your host will cause ***.yourhost.dyndns.org** to be aliased to the same IP address as **yourhost.dyndns.org**.

Password

Select the Password tab to change your router’s management password. This is the password to access the router for configuration, not for Internet access. To change the password, first enter the old password, and then enter the new password twice. Click Apply.

LAN Setup

The second feature category under the Advanced heading is LAN Setup. This menu allows configuration of LAN IP services such as DHCP and RIP. From the Main Menu of the browser interface, under Advanced, click on LAN to view the LAN Setup menu, shown in Figure 5-1



IP

DHCP Setup

☑ DHCP Server

Pool Starting Address: 192.168.0.1 Count: 32

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

LAN TCP/IP

IP Address: 192.168.0.1 RIP Direction: Both

IP Subnet Mask: 255.255.255.0 RIP Version: RIP-1

Multicast: None

Figure 5-1. LAN Setup Menu

DHCP

The Model RP114 router have the capability to act as a DHCP server, allowing them to assign IP, DNS, and default gateway addresses to attached PCs. The assigned default gateway address is the LAN address of the router. IP addresses will be assigned to the attached PCs from a pool of addresses specified in this menu. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

See “IP Configuration by DHCP” on page B-10 for an explanation of DHCP and information about how to assign IP addresses for your network.

For most applications, the default DHCP and TCP/IP settings of the router are satisfactory. These default settings are:

- DHCP server enabled with 32 client addresses starting from 192.168.0.1.

Table 5-2 lists and describes the fields to use for setting up DHCP parameters..

Table 5-2. DHCP Setup Fields

Field	Description
DHCP Server:	If this box is checked, the router acts as a DHCP server. If this box is cleared, the router's DHCP server is disabled.
Pool Starting Address	The beginning of the range of IP addresses to assign.
Count	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 DNS address in this field. If this field is 0.0.0.0, the router assigns its own address as DNS Server, and performs a DNS Proxy if it can obtain a DNS address from the ISP.
Secondary DNS Server	If you want the router to assign the Secondary DNS Server address to attached hosts, enter the address in this field.

LAN TCP/IP

Table 5-3 lists and describes the fields to use for setting up TCP/IP parameters for the LAN...

Table 5-3. LAN TCP/IP Setup Fields

Field	Description
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, 192.168.0.1). 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.

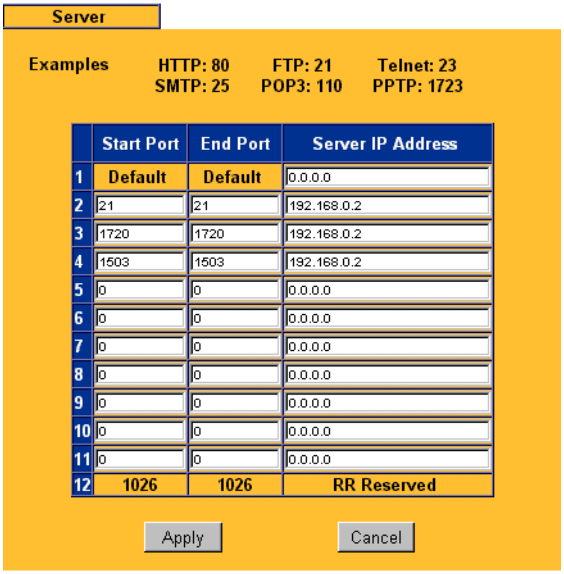
Table 5-3. LAN TCP/IP Setup Fields (continued)

Field	Description
RIP Direction	This parameter determines how the router handles RIP (Routing Information Protocol). RIP allows the router to exchange routing information with other routers. If set to None (default), the router does not participate in any RIP exchange with other routers. If set to Both, 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. Usually, you should leave this parameter at the default (None).
RIP Version	This field determines the format and broadcasting method of any RIP (Routing Information Protocol) transmissions by the router. The following RIP options are supported by the Model RP114 router: • RIP-1—The router sends RIP-1 messages only. • RIP-2B—The router sends RIP-2 messages in broadcast format. • RIP-2M—The router sends RIP-2 messages in multicast format. For most applications, the recommended version is RIP-1.
Multicast	Some streaming media applications (e.g. Cisco IP/TV, RealPlayer) now support IP Multicast. To enable Multicast routing, select either IGMP-v1 or IGMP-v2.

Note: If you change the LAN IP address of the router while connected through the browser or Telnet, you will be disconnected. You must then open a new connection to the new IP address and log in again.

Configuring for Port Forwarding to Local Servers

Although the router causes your entire local network to appear as a single machine to the Internet, you can make local servers for different services (for example, FTP or HTTP) visible and available to the Internet. This is done using the PORTS menu. From the Main Menu of the browser interface, under Advanced, click on PORTS to view the port forwarding screen, shown in Figure 5-2



Examples HTTP: 80 SMTP: 25 FTP: 21 POP3: 110 Telnet: 23 PPTP: 1723

	Start Port	End Port	Server IP Address
1	Default	Default	0.0.0.0
2	21	21	192.168.0.2
3	1720	1720	192.168.0.2
4	1503	1503	192.168.0.2
5	0	0	0.0.0.0
6	0	0	0.0.0.0
7	0	0	0.0.0.0
8	0	0	0.0.0.0
9	0	0	0.0.0.0
10	0	0	0.0.0.0
11	0	0	0.0.0.0
12	1026	1026	RR Reserved

Figure 5-2. Port Forwarding Menu

Requested services are identified by port numbers in an incoming IP packet. For example, a packet that is sent to the external IP address of your router and destined for port number 80 is an HTTP (Web server) request, and port 21 is an FTP request. Examples of port numbers are shown at the top of the PORTS menu, although you are not limited to these choices. See IETF RFC1700, "Assigned Numbers," for port numbers for common protocols..

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to the Acceptable Use Policy of your ISP.

Use the PORTS menu to configure the router to forward incoming protocols to IP addresses on your local network based on the port number. In addition to servers for specific protocols, you can also specify a Default (also called DMZ) Server to which all other incoming protocols are forwarded. To configure port forwarding to a local server:

1. Enter a port number in an unused Start Port box.
2. To forward only one port, enter it again in the End Port box. To specify a range of ports, enter the last port to be forwarded in the End Port box.
3. Enter the IP address of the local server in the corresponding Server IP Address box.
4. Click Apply at the bottom of the menu.

Local Web and FTP Server Example

If a local PC, with a private address of 192.168.0.33, acts as a Web and FTP server, configure the PORTS menu to forward ports 80 (HTTP) and 21 (FTP) to local address 192.168.0.33 as shown in Table 5-4.

Table 5-4. Port Table Entries (Example)

Port #	Server IP Address
Default	0.0.0.0
80 (HTTP)	192.168.0.33
21 (FTP)	192.168.0.33

In order for a remote user to access this server from the Internet, the remote user must know the IP address that has been assigned by your ISP. If this address is 172.16.1.23, for example, an Internet user can access your Web server by directing the browser to http://172.16.1.23. The assigned IP address can be found in the Maintenance Status Menu, where it is shown as the WAN IP Address.

Some considerations for this application are:

- If your account’s IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires.
- If the IP address of the local PC is assigned by DHCP, it may change when the PC is rebooted. To avoid this, change the configuration of your PCs to use fixed private addresses rather than DHCP-assigned addresses.

- Local PCs must access the local server using the PCs' local LAN address (192.168.0.33 in this example). Attempts by local PCs to access the server using the external IP address (172.16.1.23 in this example) will fail.

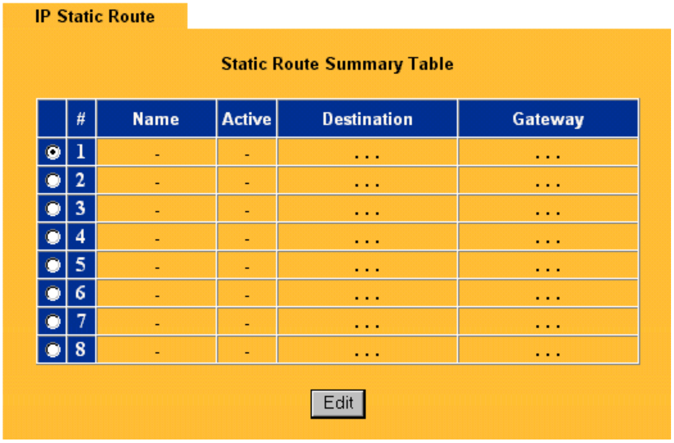
Local Game Host or Videoconference Example

Some online games and videoconferencing applications are incompatible with NAT. The Model RP114 router is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, one local PC can run the application properly if that PC's IP address is entered as the default in the PORTS Menu. If one local PC acts as a game or videoconference host, enter its IP address as the default.

Static Routes

The fourth feature category under the Advanced heading is Static Route, which allows configuration of additional routing information. Under normal circumstances, the router has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You must configure static routes only for unusual cases such as multiple routers or multiple IP subnets located on your network.

From the Main Menu of the browser interface, under Advanced, click on Static Route to view the Static Route menu, shown in Figure 5-3.



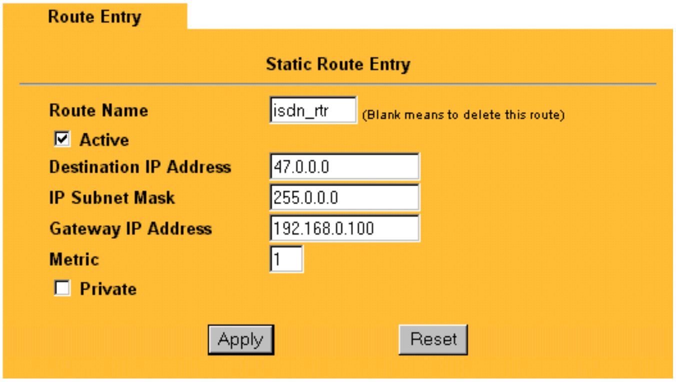
IP Static Route

Static Route Summary Table

	#	Name	Active	Destination	Gateway
●	1	-	-	. . .	. . .
○	2	-	-	. . .	. . .
○	3	-	-	. . .	. . .
○	4	-	-	. . .	. . .
○	5	-	-	. . .	. . .
○	6	-	-	. . .	. . .
○	7	-	-	. . .	. . .
○	8	-	-	. . .	. . .

Figure 5-3. Static Route Summary Table

To add or edit a Static Route, select a number and click the Edit button to open the Edit Menu, shown in Figure 5-4



Static Route Entry

Route Name: isdn_rtr (Blank means to delete this route)

☑ Active

Destination IP Address: 47.0.0.0

IP Subnet Mask: 255.0.0.0

Gateway IP Address: 192.168.0.100

Metric: 1

☐ Private

Figure 5-4. Static Route Entry and Edit Menu

Table 5-5 lists and describes the fields for the IP Static Route Edit menu.

Table 5-5. Edit IP Static Route Fields

Field	Description
Route Name	Enter a descriptive name for this route for identification purposes only.
Active	Use this field to activate or deactivate this static route.
Destination IP Address	Enter the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway to the destination network. The gateway is the next router that your router contacts in order to forward packets to the destination. On the LAN, the gateway must be a router on the same segment as the router. Over the WAN, the gateway will be the IP address of the router at your ISP.

Table 5-5. Edit IP Static Route Fields (continued)

Field	Description
Metric	Enter the cost in 'hops' 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	Use this field to determine whether 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.

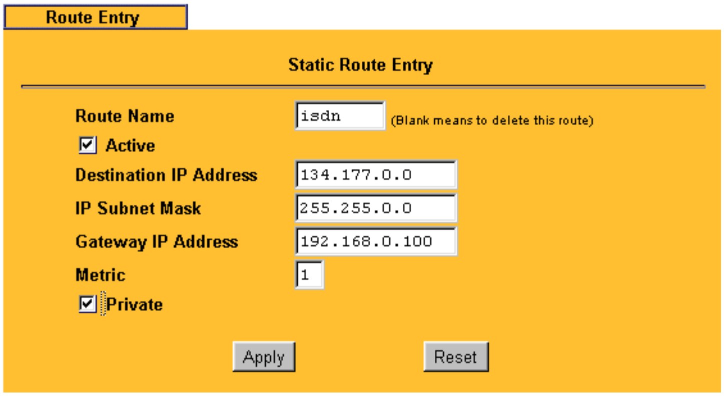
Static Route Example

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.0.100.
- Your company's network is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.x.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router will forward your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company's firewall.

In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.100. The static route would look like Figure 5-5.



Static Route Entry

Route Name: isdn (Blank means to delete this route)

☑ Active

Destination IP Address: 134.177.0.0

IP Subnet Mask: 255.255.0.0

Gateway IP Address: 192.168.0.100

Metric: 1

☑ Private

Figure 5-5. Static Route Example

In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Gateway IP Address fields specifies that all traffic for these addresses should be forwarded to the ISDN router at 192.168.0.100.
- A Metric value of either 1 or 2 will work.
- Private is selected only as a precautionary security measure in case RIP is activated.

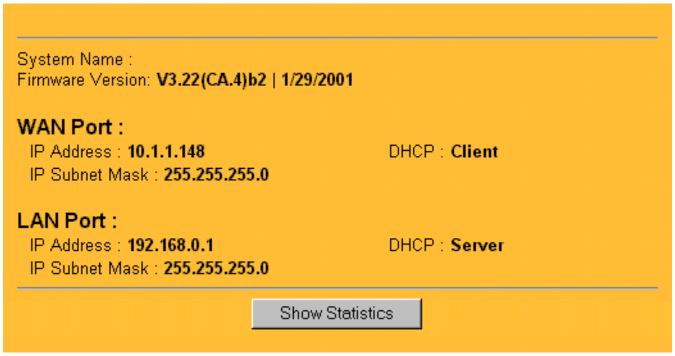
Chapter 6
Maintenance

This chapter describes how to use the maintenance features of your Model RP114 Web Safe Router. These features can be found by clicking on the Maintenance heading in the Main Menu of the browser interface.

System Status

The System Status menu provides a limited amount of status and usage information. From the Main Menu of the browser interface, click on Maintenance, then select System Status to view the System Status screen, shown in Figure 6-1

.



System Name :
Firmware Version: **V3.22(CA.4)b2 | 1/29/2001**

WAN Port :
IP Address : **10.1.1.148** DHCP : **Client**
IP Subnet Mask : **255.255.255.0**

LAN Port :
IP Address : **192.168.0.1** DHCP : **Server**
IP Subnet Mask : **255.255.255.0**

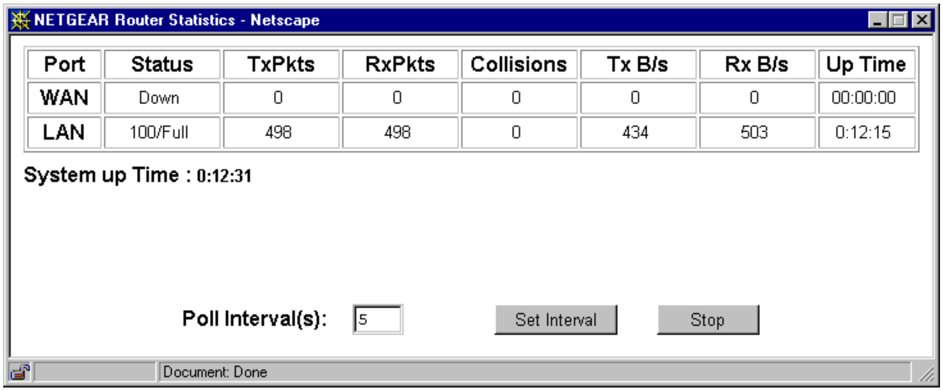
Figure 6-1. System Status screen

This screen shows the following parameters:

Table 6-1. Menu 3.2 - System Status Fields

Field	Description
System Name	This field displays the Host Name assigned to the router.
Router Firmware Version	This field displays the router firmware version.
WAN Port	These parameters apply to the Internet (WAN) port of the router.
IP Address	This field displays the IP address being used by the Internet (WAN) port of the router. If no address is shown, the router cannot connect to the Internet.
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Internet (WAN) port of the router.
DHCP	If set to None, the router is configured to use a fixed IP address on the WAN. If set to Client, the router is configured to obtain an IP address dynamically from the ISP.
LAN Port	These parameters apply to the Local (WAN) port of the router.
IP Address	This field displays the IP address being used by the Local (LAN) port of the router. The default is 192.168.0.1
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Local (LAN) port of the router. The default is 255.255.255.0
DHCP	If set to None, the router will not assign IP addresses to local PCs on the LAN. If set to Server, the router is configured to assign IP addresses to local PCs on the LAN.

Click on the “Show Statistics” button to display router usage statistics, as shown in Figure 6-2 below:



NETGEAR Router Statistics - Netscape

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Down	0	0	0	0	0	00:00:00
LAN	100/Full	498	498	0	434	503	0:12:15

System up Time : 0:12:31

Poll Interval(s): 5

Document: Done

Figure 6-2. Router Statistics screen

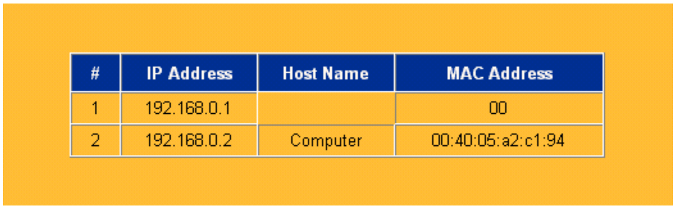
This screen shows the following statistics:.

Table 6-2. Router Statistics Fields

Field	Description
Port	The statistics for the WAN (Internet) and LAN (local) ports. For each port, the screen displays:
Status	The link status of the port.
TxPkts	The number of packets transmitted on this port since reset or manual clear.
RxPkts	The number of packets received on this port since reset or manual clear.
Collisions	The number of collisions on this port since reset or manual clear.
Tx B/s	The current line utilization—percentage of current bandwidth used on this port.
Tx B/s	The average line utilization —average CLU for this port.
Up Time	The time elapsed since this port acquired link.
System up Time	The time elapsed since the last power cycle or reset.
Poll Interval	Specifies the intervals at which the statistics are updated in this window. Click on Stop to freeze the display.

DHCP Table

The DHCP Table shows all IP address assignments that have been made by the router’s DHCP server. From the Main Menu of the browser interface, click on Maintenance, then select DHCP Table to view the table, shown in Figure 6-3



#	IP Address	Host Name	MAC Address
1	192.168.0.1		00
2	192.168.0.2	Computer	00:40:05:a2:c1:94

Figure 6-3. DHCP Table

For each PC client, the table shows the IP address, Ethernet MAC address, and NetBIOS Host Name. Note that if the router is rebooted, the table data is lost until each PC renews its DHCP lease.

Software Upgrade

The routing software of the Model RP114 router is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR. Upgrade files can be downloaded from Netgear's website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file before sending it to the router. The upgrade file can be sent to the router using your browser.

Note: The Web browser used to upload new firmware into the Model RP114 router must support HTTP uploads. NETGEAR recommends using Netscape Navigator 3.0 or above.

To reach the Upgrade menu, click Maintenance from the navigation bar on the left, and then click the Upgrade heading. To upload new firmware:

1. Download and unzip the new software file from NETGEAR.
2. In the Software Upgrade menu, click the Browse button and browse to the location of the binary (.BIN) upgrade file
3. Click Upload.

> **Note:** When uploading software to the Model RP114 router, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the software. When the upload is complete, your router will automatically restart.

In some cases, you may need to reconfigure the router after upgrading.

Configuration File Management

The configuration settings of the Model RP114 router are stored within the router in a configuration file. This file can be saved (backed up) to a user’s PC, retrieved (restored) from the user’s PC, or cleared to factory default settings.

To manage the configuration file, click on Maintenance in the Main Menu of the browser interface, then select Files. Three submenu tabs are available, and are described in the following sections.

Restore and Backup the Configuration

The Restore and Backup tabs in the Maintenance Files menu allow you to save and retrieve a file containing your router’s configuration settings.

To save your settings, select the Backup tab. Click the Backup button. Your browser will extract the configuration file, named‘rom-0’, from the router and will prompt you for a location on your PC to store the file.

To restore your settings, select the Restore tab. Enter the full path to the configuration file on your PC or click the Browse button to browse to the file. When you have located it, click on the Upload button to send the file to the router. The router will then reboot automatically.

Erase the Configuration

It is sometimes desirable to restore the router to a known blank condition. This can be done by using the Erase function, which will restore all factory settings. After an erase, the router's password will be 1234, the LAN IP address will be 192.168.0.1, and the router's DHCP client will be enabled.

To erase the configuration, click the Erase tab, then click the Erase button on the screen.

To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the router. See "Using the Default Reset button" on page 11-8.

Chapter 7
Using the Manager Interface for Initial Router Configuration

This chapter contains information about basic configuration for your Model RP114 Web Safe Router using the internal Manager interface. The initial configuration consists of:

– accessing the Manager,

– naming the router,

– and setting up the LAN interface, including DHCP parameters to be assigned to the attached PCs.

After you have performed basic router configuration, proceed to Chapter 8, “Using the Manager Interface to Configure the Router for Internet Access,” and Chapter 10, “Configuring Filters,” to configure Internet access and additional features.

➡	**Note:** You can also use the browser-based setup to configure most router features, and later use the Manager interface to configure more advanced features.

Connecting for Configuration

The Manager interface is accessible 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. The router is shippped with a default address of 192.168.0.1.

To establish a Telnet connection from the LAN, you must set up your workstation 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.

OR

- Add a route to the static routing table of the workstation to indicate that the router can be reached through the local LAN port.

To access the router by Telnet from a Windows PC:

1. From the Windows toolbar, select Start.
2. Select Run...
3. In the Open field, type:

   ```
   telnet 192.168.0.1
   ```

4. Click on OK.

   The router should respond with a “Password:” prompt. Type the current password to access the Manager interface. The default password is 1234.

.When using Telnet, consider the following restrictions:

- Single administrator

  To prevent confusion and discrepancy on the configuration, the router allows only one Telnet connection at any time.

- 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, the router automatically disconnects from the Telnet session. An exception is made for Menu 24.1, which displays current status and statistics. This menu will not time out.

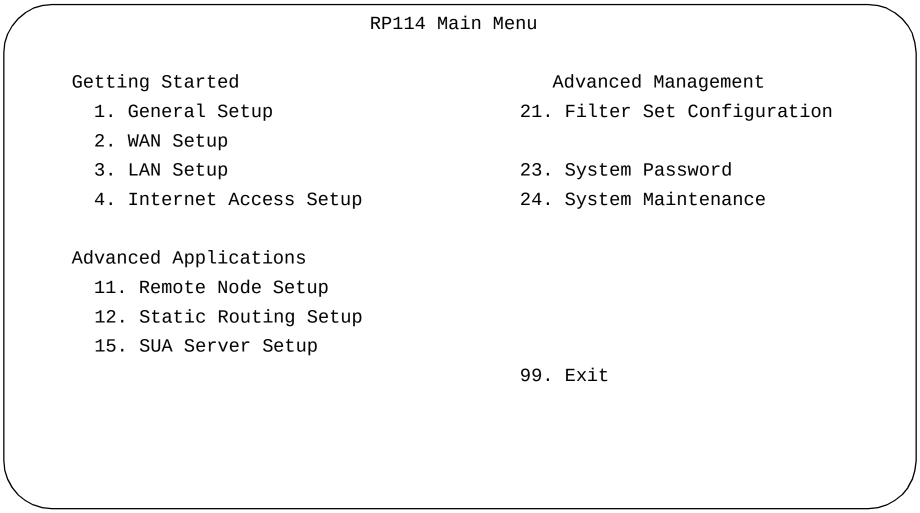
Using the Manager Interface

Login

When power is first applied to the router, several internal tests are performed by the router. The router will not accept a Telnet connection until initialization is complete as indicated by the TEST LED turning off. Log in to the Manager interface:

1. Open a Telnet session as described in the previous section, and log in.

   The Main Menu (Figure 7-1) of the Manager will appear.



```
                          RP114 Main Menu

   Getting Started                          Advanced Management
     1. General Setup                     21. Filter Set Configuration
     2. WAN Setup
     3. LAN Setup                         23. System Password
     4. Internet Access Setup             24. System Maintenance

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

Figure 7-1. Manager Main Menu

Navigating the Manager

The Manager is the interface that you use to configure your router. Table 7-1 lists and describes the commands that enable you to navigate through the Manager menus.

Table 7-1. 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 next fields, 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.

Manager Menu Summary

Table 7-2 describes the top-level Manager menus.

Table 7-2. Manager Menu Summary

Number	Menu Title	Description
1	General Setup	Specify a router name.
2	WAN Setup	Set full/half duplex to the external wide area network (WAN) connection. This connection is typically a broadband modem connected to the WAN port of the router. Also allows selection of the MAC address.
3	LAN Setup	Configure the local area network (LAN) parameters, including IP address and DHCP operation.

Table 7-2. Manager Menu Summary (continued)

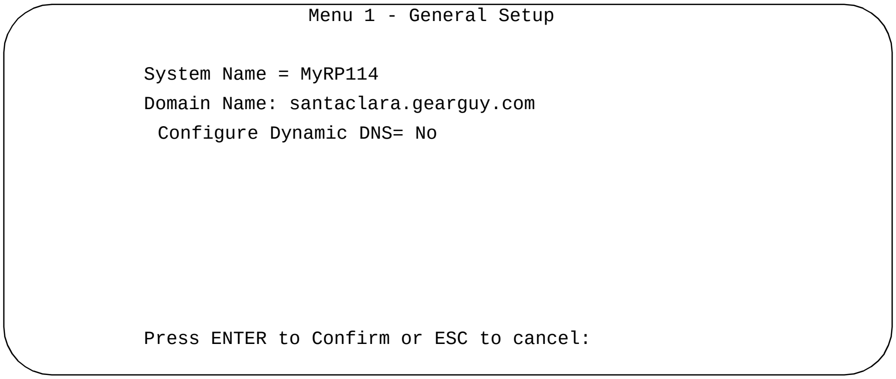
Number	Menu Title	Description
4	Internet Access Setup	Set up a basic Internet connection.
11	Remote Node Setup	Configure additional parameters of the Internet connection
12	Static Routing Setup	Manually configure static routes. The router supports eight static routes.
15	SUA Server Setup	Configure forwarding of specific incoming service requests to local hosts.
21	Filter Set Configuration	Set up filters to be used in Menu 3 and Menu 11 to provide security and traffic control.
23	System Password	Change password for Manager access.
24	System Maintenance	Provide system status, diagnostics, and firmware upload.
99	Exit	Exit from the Manager.

General Setup Menu

The General Setup Menu contains administrative and system-related information, such as the router name.

To enter administrative and system-related information:

1. Enter 1 from the Main Menu to display Menu 1 - General Setup, as illustrated in Figure 7-2.



```
                        Menu 1 - General Setup

          System Name = MyRP114
          Domain Name: santaclara.gearguy.com
           Configure Dynamic DNS= No








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

Figure 7-2. Menu 1 - General Setup

2. In the System Name field, enter a name for identifying the router.

   For identification purposes, choose a descriptive name for the router, such as MyRP114. If your ISP has assigned a host name for your PC, the System Name in some cases must be set to the host name. The System Name can include up to 30 alphanumeric characters. Spaces are not allowed, but dashes (-) and underscores (_) are acceptable.

3. (Optional) In the Domain Name field, enter the domain name of your Internet service.

   The Domain Name may be helpful in accessing some of the services of your ISP, such as email, news servers and customer support. If your account’s full server names look like this:

       mail.xxx.yyy.com

   your domain name is xxx.yyy.com.

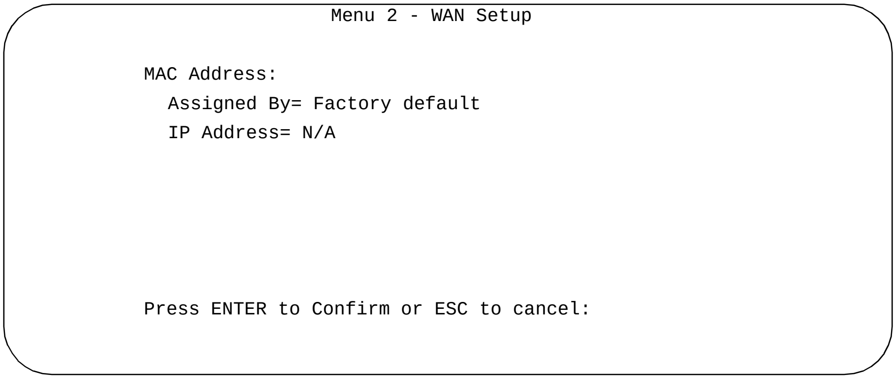
4. (Optional) Configure for Dynamic DNS.

   If you wish to use Dynamic DNS, refer to “Dynamic DNS“ on page 8-17.

WAN Setup

Menu 2 enables you to configure the 10 Mbps Ethernet port to a broadband modem device, such as a cable or DSL modem. This port is labeled WAN on the front panel of the router.

Figure 7-3 shows Menu 2 - WAN Setup.



```
                              Menu 2 - WAN Setup

            MAC Address:
              Assigned By= Factory default
              IP Address= N/A






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

Figure 7-3. Menu 2 - WAN Setup

Table 7-3 lists and describes the fields for Menu 2 - WAN Setup.

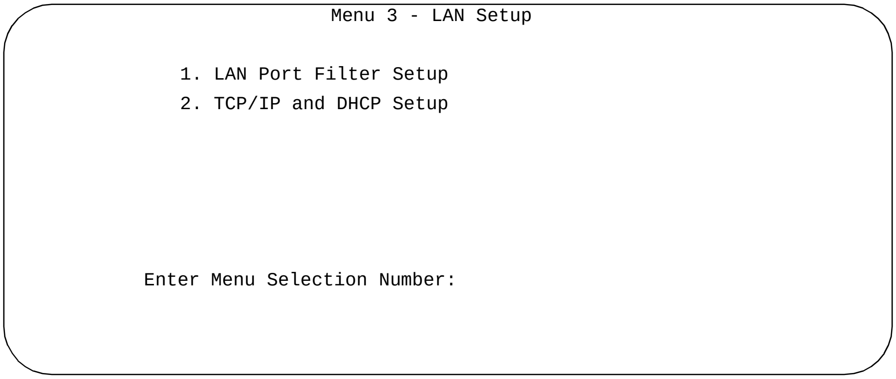
Table 7-3. WAN Setup Fields

Field	Description
MAC Address	The MAC Address is the 48-bit Ethernet address of the router's INTERNET port.
Assigned By	Set to Factory default to use the router's internal globally unique MAC address. Set to 'IP address attached on LAN' to acquire and substitute the MAC address of one of your PCs on the local network. Some ISPs will only accept traffic from the MAC address of one PC. This feature allows your router to masquerade as that PC by using its MAC address.
IP Address	If you selected IP address attached on LAN in the previous field, you must specify the IP address of the local PC with the MAC address to be used by the router.

LAN Setup

Menu 3 enables you to configure the Ethernet LAN parameters, including filters, DHCP, and IP address information. These parameters specify the behavior of the router's local port.

1. From the Main Menu, enter 3 to display Menu 3 - LAN Setup (Figure 7-4).



```
                             Menu 3 - LAN Setup

              1. LAN Port Filter Setup
              2. TCP/IP and DHCP Setup







           Enter Menu Selection Number:
```

Figure 7-4. Menu 3 - LAN Setup

2. Select one of the following submenus:
   - Menu 3.1 LAN Port Filter Setup
   - Menu 3.2 TCP/IP and DHCP Setup

   Refer to the following sections for descriptions of these submenus. Refer to Table 7-1 on page 7-4 for information about navigating through the menus.

LAN Port Filter Setup Menu

The LAN Port Filter Setup Menu allows you to apply filter sets to control your Ethernet traffic. Filters are used to block certain packets, to reduce traffic, and to prevent security breaches. You must first create these filter sets using Menu 21, and then apply them by number in this menu. Refer to Chapter 10, "Configuring Filters," for more information about configuring and applying filters.

Table 7-4 lists and describes the interface and filter choices in the LAN Port Filter Setup menu.

Table 7-4. Menu 3.1 - LAN Port Filter Setup Fields

Field	Description
Input and Output Filter Sets	Enter filter sets by number to filter packets coming from the LAN (Input) or going out to the LAN (Output).
Protocol Filters	Enter the numbers of one or more IP filter sets created in Menu 21.
Device Filters	Enter the numbers of one or more generic filter sets created in Menu 21.

TCP/IP and DHCP Setup

The Model RP114 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 B-2 and "IP Configuration by DHCP" on page B-10 for an explanation of DHCP and information about how to assign IP addresses for your network.

For most applications, the default DHCP and TCP/IP settings of the router are satisfactory. These default settings are:

- LAN IP address 192.168.0.1 with subnet mask 255.255.255.0.
- DHCP server enabled with 32 client addresses starting from 192.168.0.1.
- DNS Proxy enabled (the router address is assigned as a DNS server).

Table 7-5 lists and describes the fields to use for setting up TCP/IP and DHCP parameters in Menu 3.2. 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.

> **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.

.

Table 7-5. Menu 3.2 - TCP/IP and DHCP Setup Fields

Field	Description
DHCP:	If set to Server, the router acts as a DHCP server. If set to None, the router’s DHCP server is disabled.
DHCP Configuration:	
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 DNS address in this field. If this field is 0.0.0.0, the router assigns its own address as DNS Server, and performs a DNS Proxy if it can obtain a DNS address from the ISP.
Secondary DNS Server	If you want the router to assign the Secondary DNS Server address to attached hosts, enter the address in this field.
TCP/IP Setup:	
IP Address	Enter the IP address of the LAN interface of the router in dotted-decimal notation (four 8-bit numbers, between 0 and 255, separated by periods, for example, 192.168.0.1). 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.
RIP Direction	This parameter determines how the router handles RIP (Routing Information Protocol). RIP allows the router to exchange routing information with other routers. If set to None (default), the router does not participate in any RIP exchange with other routers. If set to Both, 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. Usually, you should leave this parameter at the default (None).

Table 7-5. Menu 3.2 - TCP/IP and DHCP Setup Fields (continued)

Field	Description
RIP Version	This field determines the format and broadcasting method of any RIP (Routing Information Protocol) transmissions by the router. The following RIP options are supported by the Model RP114 router: • RIP-1—The router sends RIP-1 messages only. • RIP-2B—The router sends RIP-2 messages in broadcast format. • RIP-2M—The router sends RIP-2 messages in multicast format. For most applications, the recommended version is RIP-1.
Multicast	Some streaming media applications (e.g. Cisco IP/TV, RealPlayer) now support IP Multicast. To enable Multicast routing, select either IGMP-v1 or IGMP-v2.

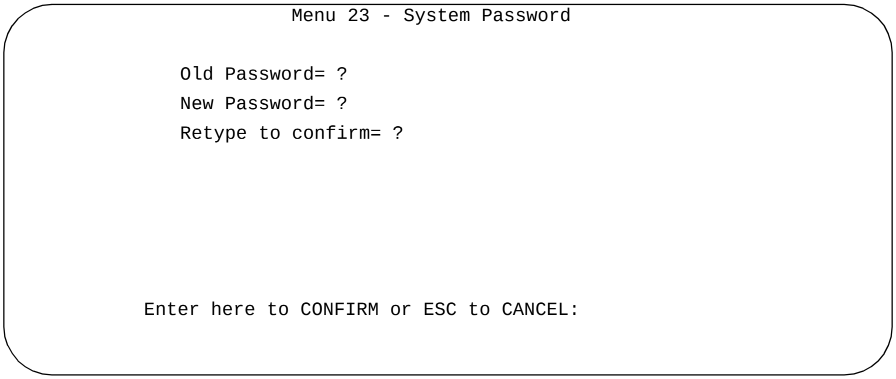
Manager Password Setup

For security, you should change the Manager password from the default value of 1234.

To change the Manager password:

1. Select option 23, System Password, from the main menu.

Menu 23 - System Password opens (Figure 7-5).



```
                         Menu 23 - System Password

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





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

Figure 7-5. 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 by a Telnet connection.

If you lose or forget the Manager password, you must clear the configuration of the router as described in Chapter 11, “Troubleshooting.” Clearing the configuration causes the Manager password to revert to the default, 1234.

Chapter 8
Using the Manager Interface to Configure the Router for Internet Access

This chapter describes how to configure your Model RP114 Web Safe Router for Internet access using the internal Manager interface. For information about using the Manager interface, refer to Chapter 7, "Using the Manager Interface for Initial Router Configuration."

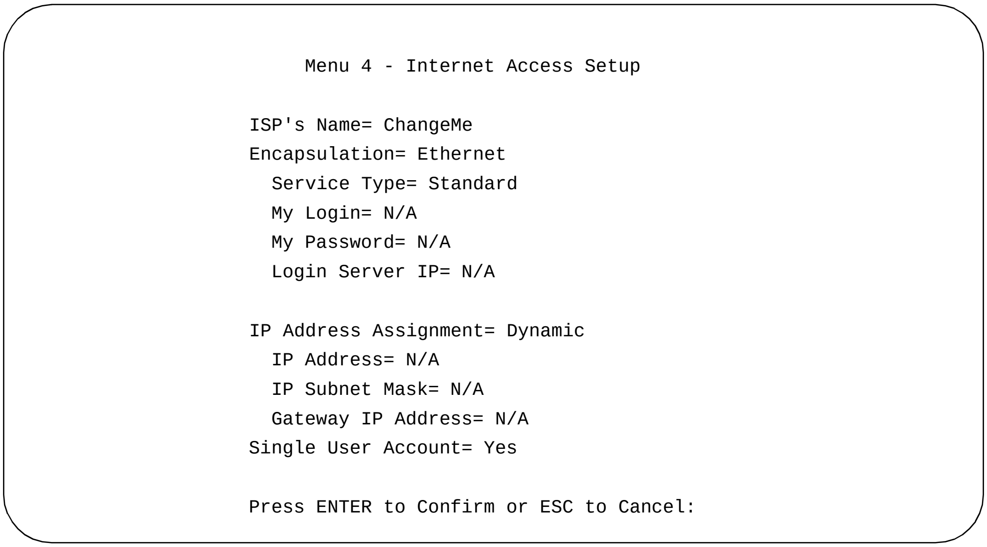
Internet Access Configuration

You can configure the router for basic access to your Internet service provider (ISP) using Manager Menu 4, Internet Access Setup. The configuration information required is either supplied directly by your ISP or must be obtained from your preconfigured PC as described in "Obtaining ISP Configuration Information (Windows)" on page 3-8. Additional configuration parameters are available in Menu 11, Remote Node Setup.

To configure your router for Internet access:

1. Enter 4 from the Main Menu to display Menu 4 - Internet Access Setup.

   Menu 4 - Internet Access Setup opens (Figure 8-1).



```
                  Menu 4 - Internet Access Setup

             ISP's Name= ChangeMe
             Encapsulation= Ethernet
               Service Type= Standard
               My Login= N/A
               My Password= N/A
               Login Server IP= N/A

             IP Address Assignment= Dynamic
               IP Address= N/A
               IP Subnet Mask= N/A
               Gateway IP Address= N/A
             Single User Account= Yes

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

Figure 8-1. Menu 4 - Internet Access Setup

2. Enter the name of your ISP in the ISP’s Name field (for example, myISP).

   This information is required for identification purposes only.

3. If your ISP uses PPP over Ethernet (PPPoE), use the space bar to toggle Encapsulation to PPPoE. Otherwise, leave it as Ethernet.

   PPP over Ethernet (PPPoE) is a type of connection that requires the use of a dialer program such as Microsoft Dial-Up Networking to access your DSL or cable modem. In this case, the router will perform this function, and it will not be necessary to run the dialer on your attached PCs.

   a. If your connection supports multiple ISPs, enter the Service Name of the one you use. Otherwise, leave Service Name blank.

   b. Enter your account’s login name as My Login.

   c. Enter your account’s password as My Password.

4. If you selected Ethernet Encapsulation, use the space bar to toggle the Service Type field to either RoadRunner or Standard.

   This field determines whether the RoadRunner login program will be run. If your service provider is not RoadRunner or if your RoadRunner region does not require the login program:

a. Select Standard.

If your Service Type is RoadRunner and your RoadRunner region requires the login program:

a. Select the RoadRunner login program used in your region.

b. Enter the login name and password provided by RoadRunner.

5. If RoadRunner provided an authentication server address, enter it as Login Server IP address. Otherwise, leave this field as 0.0.0.0.
6. Use the space bar to toggle the IP Address Assignment field to Static or Dynamic.

   If your service provider has assigned you an IP address to be manually configured in your PC, select Static. In this case, enter your assigned IP address, subnet mask, and gateway address (the address of the ISP's router). If you do not know the gateway address, leave this field as 0.0.0.0.
7. Use the space bar to toggle the Single User Account field to Yes.
8. Press [Enter] at the Press ENTER to Confirm... prompt to confirm your selections.

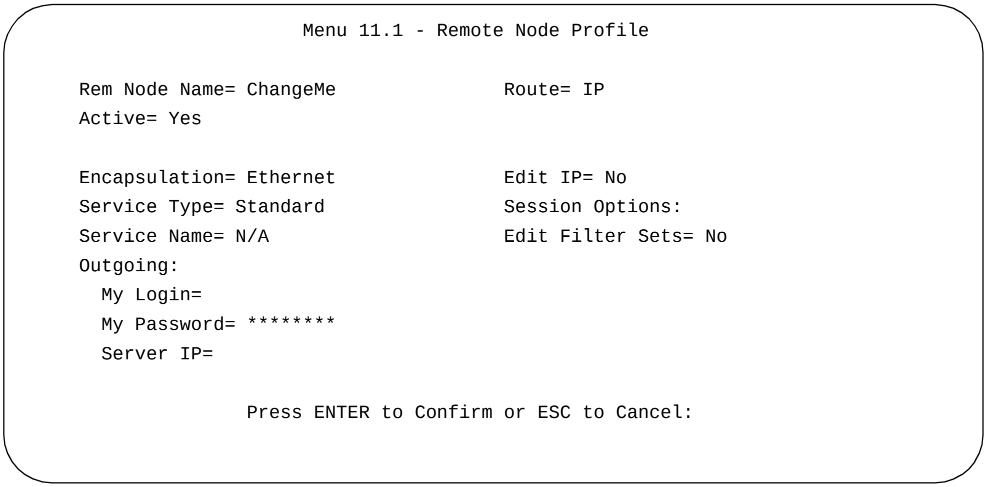
You can press [Esc] at any time to cancel your selections. When you save this menu, the router automatically creates a default static route to the ISP.

Remote Node Setup Menu

Additional settings for Internet Access connection are provided in Menu 11 - Remote Node Setup. To access Menu 11:

1. Enter 11 from the Main Menu to display Menu 11 - Remote Node Setup.

   Menu 11.1 - Remote Node Profile opens as shown in Figure 8-2.



```
                     Menu 11.1 - Remote Node Profile

     Rem Node Name= ChangeMe                     Route= IP
     Active= Yes

     Encapsulation= Ethernet                     Edit IP= No
     Service Type= Standard                      Session Options:
     Service Name= N/A                           Edit Filter Sets= No
     Outgoing:
       My Login=
       My Password= ********
       Server IP=

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

Figure 8-2. Menu 11.1 - Remote Node Profile

2. Edit the remote node settings with the desired changes.
3. At the bottom of Menu 11.1, press Enter to save Menu 11.1.

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

Table 8-1 lists and describes the fields in the Remote Node Profile menu and explains how to enter the information in each field.

Table 8-1. 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. .
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.

Table 8-1. Remote Node Profile Fields (continued)

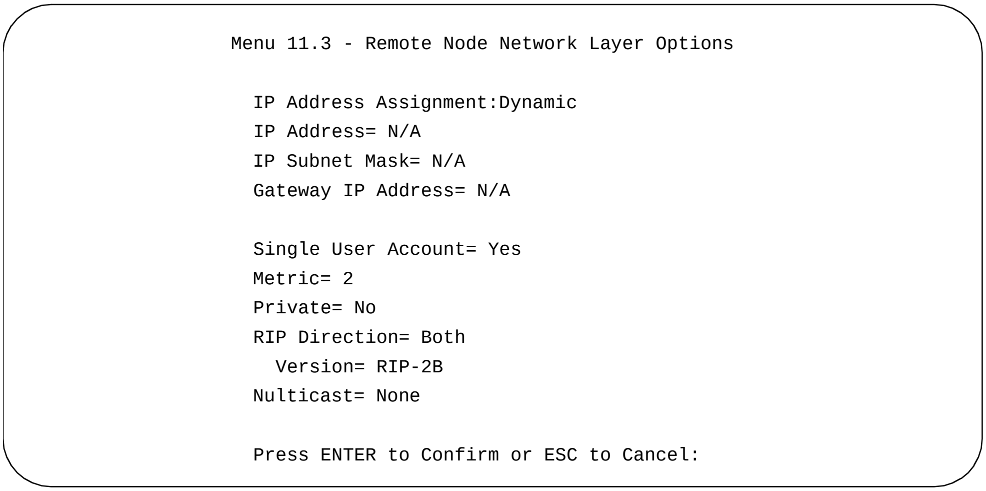
Field	Description
Encapsulation	Choose from Ethernet, PPPoE, or PPTP. If your service provider does not require a login program, leave Encapsulation as Ethernet. If your service provider uses PPP over Ethernet (PPPoE), select Encapsulation as PPPoE, and enter these additional parameters: • Enter the PPPoE login user name and password provided by your ISP. These fields are case sensitive. European versions only: If your service provider uses Alcatel's ANT (ADSL Network Termination) with PPTP as a login method, select Encapsulation as PPTP, and enter these additional parameters: • Enter the PPTP login user name and password provided by your ISP. These fields are case sensitive.
Service Type	Choose from Standard, RR-Toshiba (RoadRunner Toshiba authentication method) or RR-Manager (RoadRunner Manager authentication method). Choose a RoadRunner flavor if your ISP is Time Warner's RoadRunner; otherwise choose Standard.
Service Name	If your connection supports multiple ISPs, enter the the Connection ID/Name for the one you use. Otherwise leave Service Name blank.
Outgoing:	
My Login Name	If your service provider requires a login program, enter the login name assigned to your account.
My Password	If your service provider requires a login program, enter the password assigned to your account.
Server IP	If your service provider provided an authentication server address, enter it as Server IP address.
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 configuring IP options, see "Editing IP Options" on page 8-6.
Session Options:	
Edit Filter Sets	Select Yes and press [Enter] to display Menu 11.5, Remote Node Filter if you have configured a filter in Menu 21 and wish to apply it as a Call Filter or Data filter for the node. For more information about configuring filter options, see "Editing Filter Sets" on page 8-8.

Editing IP Options

To edit IP options:

1. Select Yes in the Edit IP Options field of Submenu 11.1 - Remote Node Profile.
2. Press [Enter] to display Menu 11.3 - Remote Node Network Layer Options.

   Menu 11.3 - Remote Node Network Layer Options opens as shown in Figure 8-3.



```
                    Menu 11.3 - Remote Node Network Layer Options

                      IP Address Assignment:Dynamic
                      IP Address= N/A
                      IP Subnet Mask= N/A
                      Gateway IP Address= N/A

                      Single User Account= Yes
                      Metric= 2
                      Private= No
                      RIP Direction= Both
                        Version= RIP-2B
                      Nulticast= None

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

Figure 8-3. Menu 11.3 - Remote Node Network Layer Options

3. Edit the options described in Table 8-2.
4. Press [Enter] at the Press ENTER to Confirm... prompt to confirm your selections, and return to the previous menu.

   Press [Esc] at any time to cancel your selections.
5. Continue to the end of Menu 11.1 and press [Enter] to save the selections you made in Menu 11.3.

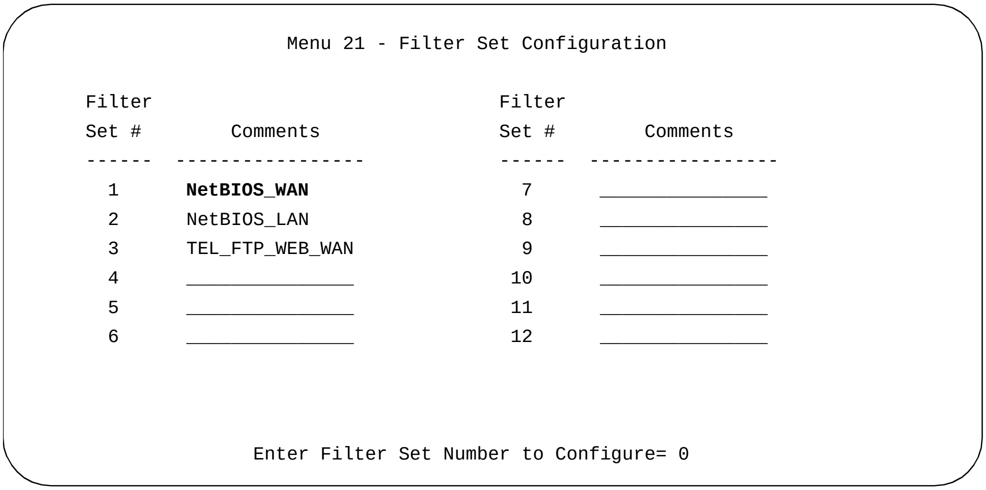
Table 8-2 lists and describes the fields for Menu 11.3 - Remote Node Network Layer Options.

Table 8-2. Remote Node Network Layer Options Fields

Field	**Description**
IP Address Assignment	Selects whether the WAN IP address will be static (fixed) or assigned dynamically.
IP Address	If you are using a fixed address, enter that IP address in this field. This is the address assigned to the local router, not the remote router.
IP Subnet Mask	This field displays 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.
Gateway IP Address	If you are using a fixed address, enter the IP address of the remote router to which your router will connect.
Single User Account	If this field is set to Yes, the router performs NAT (IP Address Masquerading) to this node.
Metric	Enter a number in this field that approximates the cost for this link. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. 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.
RIP: RIP Direction	This parameter determines how the router handles RIP (Routing Information Protocol). If set to Both (default), the router broadcasts the routing table of the router on the LAN and incorporates RIP broadcasts by other routers into its routing table. If set to In Only, the router broadcasts its routing table on the LAN. If set to Out Only, the router broadcasts its routing table, but it ignores any RIP broadcast packets that it receives. If set to None, the router does not participate in any RIP exchange with other routers. Usually, you should leave this parameter at the default (Both) and let RIP propagate the routing information automatically.
RIP Version	This field determines the format and broadcasting method of any RIP (Routing Information Protocol) transmissions by the router. The following RIP options are supported by the Model RP114 router: • RIP-1—The router sends RIP-1 messages only. • RIP-2B—The router sends RIP-2 messages in broadcast format. • RIP-2M—The router sends RIP-2 messages in multicast format. For most applications, the recommended version is RIP-1.
Multicast	Some streaming media applications (e.g. Cisco IP/TV, RealPlayer) now support IP Multicast. To enable Multicast routing, select either IGMP-v1 or IGMP-v2

Editing Filter Sets

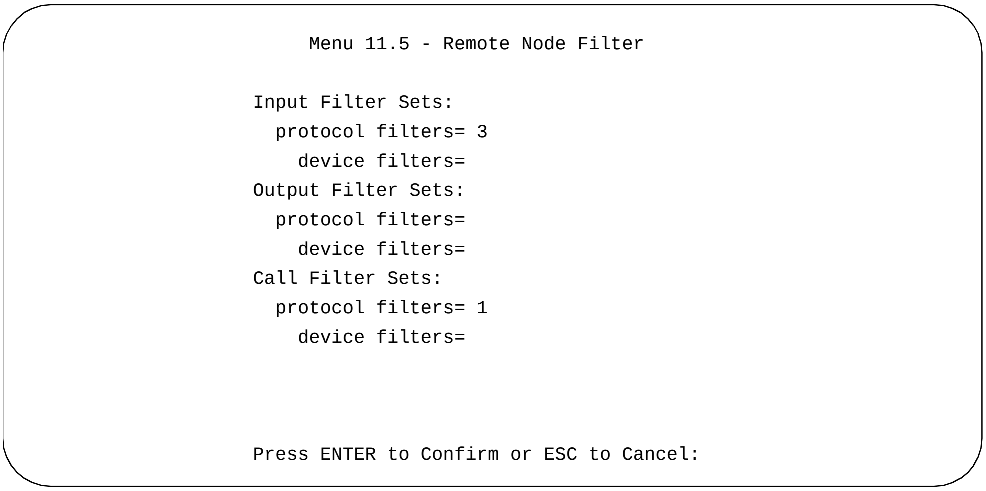
You can apply filters to incoming or outgoing data in a Remote Node connection and also use filters to cause or prevent the placement of outgoing calls to the Remote Node. To use filters, start by defining the filters using Menu 21 - Filter Set Configuration as shown in Figure 8-4.



```
                         Menu 21 - Filter Set Configuration


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



                      Enter Filter Set Number to Configure= 0
```

Figure 8-4. Menu 21 - Filter Set Configuration

After defining filters in Menu 21, apply the filters to the Remote Node by entering the filter number in Menu 11.5 - Remote Node Filters. You can cascade up to four filter sets by entering the numbers of the desired filter sets, separated by commas and with no spaces between them. Menu 11.5 - Remote Node Filters is shown in Figure 8-5.



```
                         Menu 11.5 - Remote Node Filter

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



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

Figure 8-5. Menu 11.5 - Remote Node Filters

Table 8-3 describes the fields of the Remote Node Filters display.

Table 8-3. Remote Node Filters Fields

Field	Description
Input, Output, and Call Filters	These categories allow the application of filters to incoming data or outgoing data, and they cause or prevent the placement of outgoing calls.
Protocol Filters	Enter the filter numbers of IP packet format filters defined in Menu 21.
Device Filters	Enter the filter numbers of generic packet format filters defined in Menu 21.

For more information on using filters, refer to Chapter 10, “Configuring Filters.”

Configuration for Local Servers

Although NAT causes your entire local network to appear as a single machine to the Internet, you can make local servers for different services (for example, FTP or HTTP) visible and available to the Internet. Requested services are identified by port numbers in an incoming IP packet. For example, a packet that is sent to the external IP address of your router and destined for port number 80 is an HTTP (Web server) request, and port 21 is an FTP request. Examples of port numbers are shown at the bottom of Menu 15, although you are not limited to these choices. See IETF RFC1700, “Assigned Numbers,” for port numbers for common protocols..

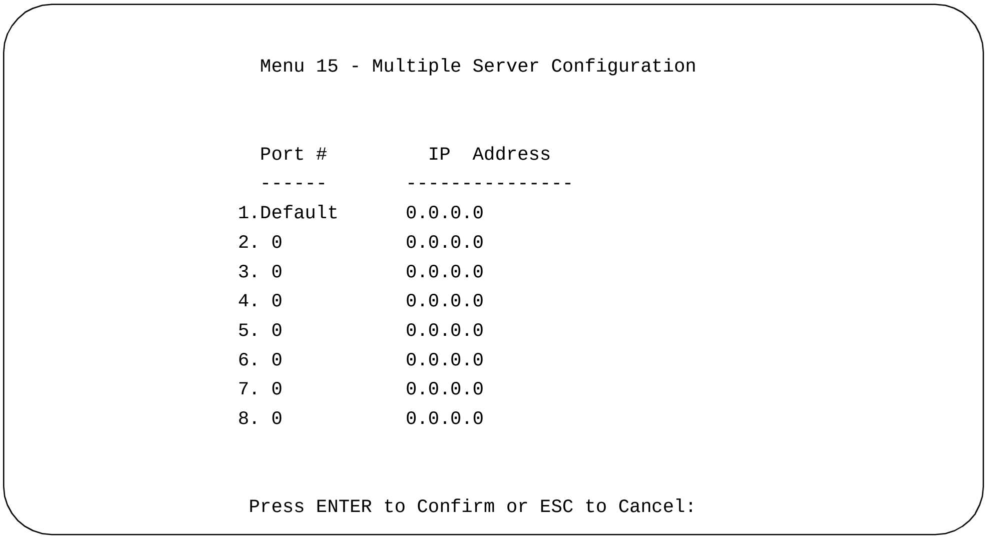
➡ **Note:** Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to the Acceptable Use Policy of your ISP.

Use Menu 15, SUA Server Setup, to configure the router to forward incoming protocols to IP addresses on your local network based on the port number. In addition to servers for specific protocols, you can also specify a default (DMZ) server to which all other incoming protocols are forwarded. To configure port forwarding to a local server:

1. Enter a port number in an unused Start Port row.
2. To forward only one port, enter it again in the End Port row. To specify a range of ports, enter the last port to be forwarded in the End Port row.
3. Enter the IP address of the local server in the corresponding IP Address row.
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.

Menu 15 - SUA Server Setup is shown in Figure 8-6.



```
                      Menu 15 - Multiple Server Configuration


                      Port #         IP  Address
                      ------       ---------------
                    1.Default      0.0.0.0
                    2. 0           0.0.0.0
                    3. 0           0.0.0.0
                    4. 0           0.0.0.0
                    5. 0           0.0.0.0
                    6. 0           0.0.0.0
                    7. 0           0.0.0.0
                    8. 0           0.0.0.0


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

Figure 8-6. Menu 15 - SUA Server Setup

Local Web and FTP Server Example

If a local PC, with a private address of 192.168.0.3, acts as a Web and FTP server, configure Menu 15 to forward ports 80 (HTTP) and 21 (FTP) to local address 192.168.0.3 as shown in Table 8-4.

Table 8-4. Menu 15 Field Entries (Example)

Port #	IP Address
Default	0.0.0.0
80 (HTTP)	192.168.0.3
21 (FTP)	192.168.0.3

In order for a remote user to access this server from the Internet, the remote user must know the IP address that has been assigned by your ISP. If this address is 172.16.1.23, for example, an Internet user can access your Web server by directing the browser to http://172.16.1.23. The assigned IP address can be found in Menu 24.1, in the WAN IP Address field.

Some considerations for this application are:

- If your account’s IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires.
- If the IP address of the local PC is assigned by DHCP, it may change when the PC is rebooted. To avoid this, change the configuration of your PCs to use fixed private addresses rather than DHCP-assigned addresses.
- Local PCs must access the local server using the PCs’ local LAN address (192.168.0.3 in this example). Attempts by local PCs to access the server using the external IP address (172.16.1.23 in this example) will fail.

Local Game Host or Videoconference Example

Some online games and videoconferencing applications are incompatible with NAT. The Model Model RP114 router is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, one local PC can run the application properly if that PC’s IP address is entered as the default in Menu 15. If one local PC acts as a game or videoconference host, enter its IP address as the default.

Setting Static Routes

Under normal circumstances, the router has adequate routing information after you configure the Internet access information, and you do not need to configure additional static routes. You must configure static routes only for unusual cases such as multiple routers or multiple IP subnets located on your network.

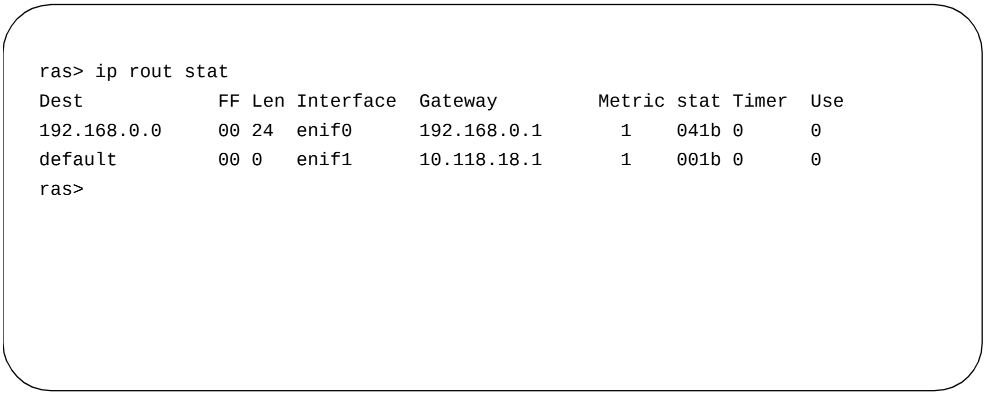
To view the routes in the routing table:

1. In the Manager interface, open Menu 24 - System Maintenance.
2. Type 8 and press [Enter] to change to the Command Interpreter Mode.
3. At the command prompt, type:

   ```
   ip route stat
   ```

4. Press [Enter].

   The command interpreter displays the static IP routing table as shown in the example in Figure 8-7.



```
ras> ip rout stat
Dest            FF Len Interface  Gateway         Metric stat Timer  Use
192.168.0.0     00 24  enif0      192.168.0.1       1    041b 0      0
default         00 0   enif1      10.118.18.1       1    001b 0      0
ras>
```

Figure 8-7. IP Static Routing Table Example

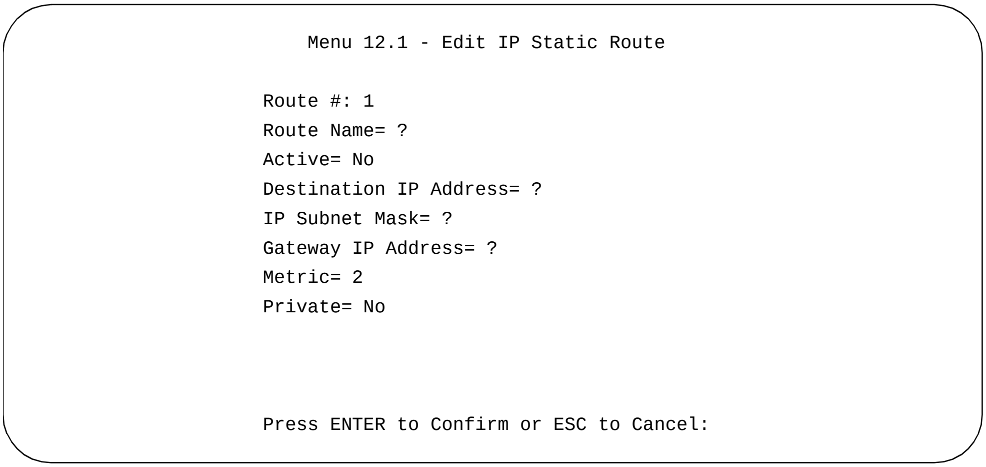
In this example, the first route shown is the local Ethernet subnet connected to the LAN interface (enif0). The second route is the default route, through the WAN interface (enif1). All traffic from the LAN to a destination outside the LAN will be sent to the default route and will be handled by the ISP.

5. After viewing the table, type “exit” to return to the menus.

To create additional static routes for IP:

1. In the Manager interface, open Menu 12 - IP Static Route Setup.
2. Select an unused number from the menu and press [Enter].

   Menu 12.1 - Edit IP Static Route opens as shown in Figure 8-8.



```
            Menu 12.1 - Edit IP Static Route

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



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

Figure 8-8. Menu 12.1 - Edit IP Static Route

3. Enter settings for the static route entry.

   Table 8-5 lists and describes the fields for Menu 12.1 - Edit IP Static Route.

Table 8-5. Edit IP Static Route Fields

Field	**Description**
Route Name	Enter a descriptive name for this route for identification purposes only.
Active	Use this field to activate or deactivate this static route.
Destination IP Address	Enter the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway to the destination network. The gateway is the next router that your router contacts in order to forward packets to the destination. On the LAN, the gateway must be a router on the same segment as the router. Over the WAN, the gateway will be the IP address of the router at your ISP.

Table 8-5. Edit IP Static Route Fields (continued)

Field	Description
Metric	Enter 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	Use this field to determine whether 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.

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

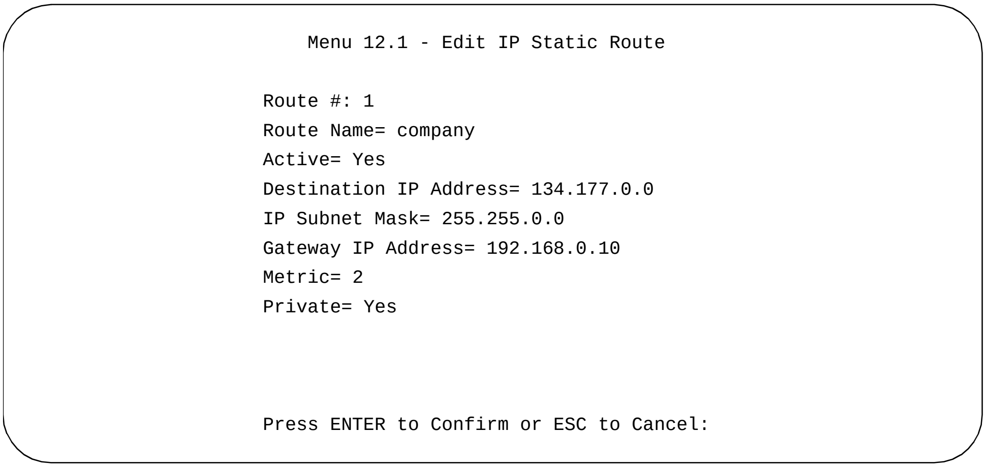
Static Route Example

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router’s address on your LAN is 192.168.0.10.
- Your company’s network is 134.177.0.0.

When you first configured your Model RP114 router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.x.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router will forward your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company’s firewall.

In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.10. The static route would look like Figure 8-9.



```
                    Menu 12.1 - Edit IP Static Route

                Route #: 1
                Route Name= company
                Active= Yes
                Destination IP Address= 134.177.0.0
                IP Subnet Mask= 255.255.0.0
                Gateway IP Address= 192.168.0.10
                Metric= 2
                Private= Yes



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

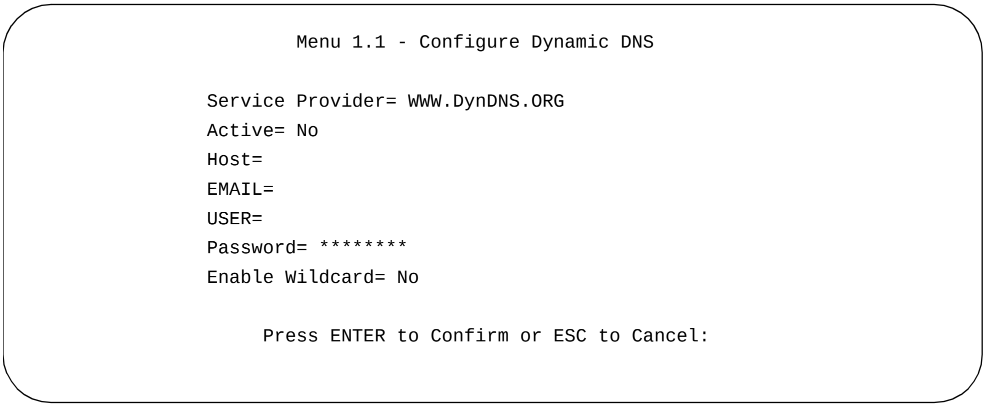
Figure 8-9. Static Route Example

In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Gateway IP Address fields specifies that all traffic for these addresses should be forwarded to the ISDN router at 192.168.0.10.
- A Metric value of either 1 or 2 will work.
- Private is set to Yes only as a precautionary security measure in case RIP is activated.

Dynamic DNS

You can configure your router to register its dynamically assigned IP address with a dynamic DNS service by configuring Menu 1.1, shown in Figure 8-10. To use this feature, you must have an account with DynDNS.org. Refer to www.dyndns.org for more information.



```
                Menu 1.1 - Configure Dynamic DNS

        Service Provider= WWW.DynDNS.ORG
        Active= No
        Host=
        EMAIL=
        USER=
        Password= ********
        Enable Wildcard= No

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

Figure 8-10. Menu 1.1 - Configure Dynamic DNS

Table 8-6 lists and describes the fields for Menu 1.1 - Configure Dynamic DNS.

Table 8-6. Dynamic DNS Configuration Fields

Field	**Description**
Service Provider	Select your dynamic DNS service provider.
Active	Use this field to activate or deactivate dynamic DNS registration.
Host	Enter the static host name that will link to your dynamic IP address.
EMAIL	Enter your email address for administrative contact.
USER	Enter the user name of your dynamic DNS service account.
Password	Enter the password of your dynamic DNS service account.
Enable Wildcard	DynDNS.org allows the use of wildcards in resolving your URL. Enabling the wildcard feature for your host will cause ***.yourhost.dyndns.org** to be aliased to the same IP address as **yourhost.dyndns.org**.

Chapter 9
Using the Manager Interface for Advanced System Maintenance

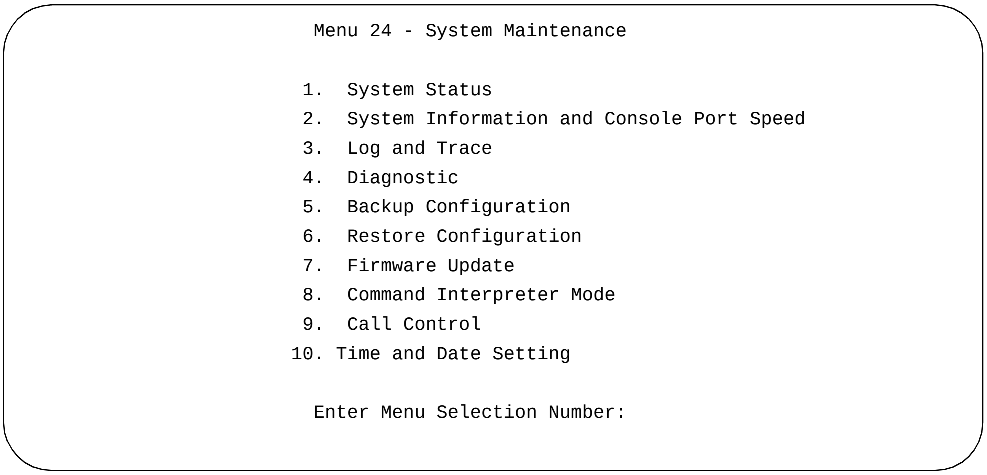
The Model RP114 Web Safe Router provides tools for maintenance and diagnostics. These tools include displays of system status and connections, log and trace capabilities, and upgrades to the system software. This chapter describes the use of these tools.

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 LAN and WAN Ethernet ports and the number of packets sent and received. The system software version is also displayed.

To access the System Maintenance Status Menu:

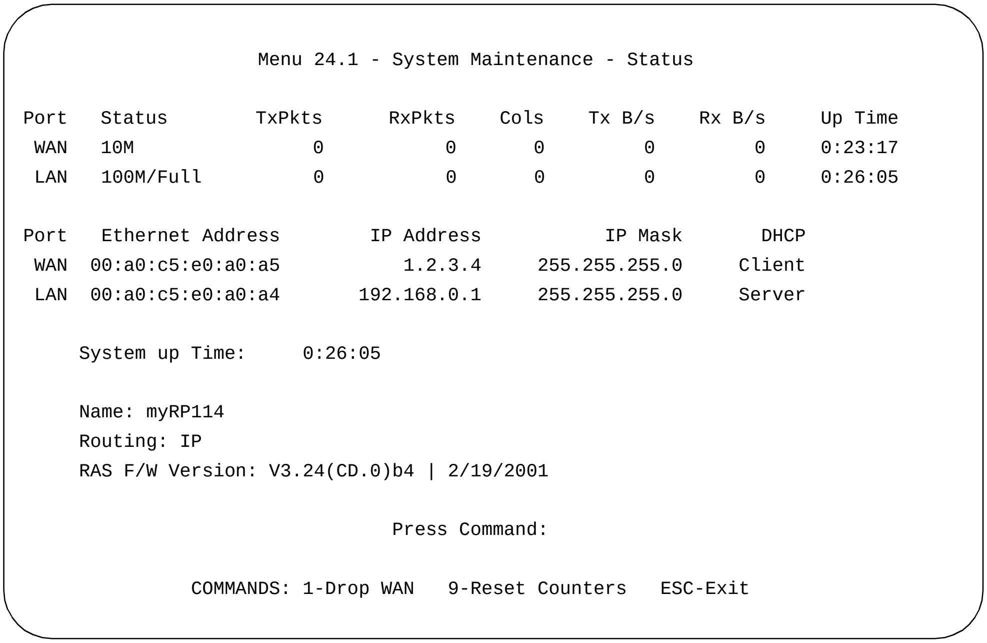
1. **Enter 24 from the Main Menu to display the System Maintenance menu (Figure 9-1).**



```
                          Menu 24 - System Maintenance

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

                          Enter Menu Selection Number:
```

Figure 9-1. Menu 24 - System Maintenance

2. **Enter 1 to display Menu 24.1 - System Maintenance - Status menu (Figure 9-2).**



```
                     Menu 24.1 - System Maintenance - Status

Port   Status        TxPkts      RxPkts    Cols    Tx B/s    Rx B/s     Up Time
 WAN   10M                0           0       0         0         0     0:23:17
 LAN   100M/Full          0           0       0         0         0     0:26:05

Port   Ethernet Address        IP Address           IP Mask       DHCP
 WAN  00:a0:c5:e0:a0:a5           1.2.3.4     255.255.255.0     Client
 LAN  00:a0:c5:e0:a0:a4       192.168.0.1     255.255.255.0     Server

     System up Time:     0:26:05

     Name: myRP114
     Routing: IP
     RAS F/W Version: V3.24(CD.0)b4 | 2/19/2001

                                 Press Command:

               COMMANDS: 1-Drop WAN   9-Reset Counters   ESC-Exit
```

Figure 9-2. Menu 24.1 - System Maintenance - Status

Table 9-1 lists the commands used in the System Maintenance - Status menu.

Table 9-1. System Maintenance Status

Command	Field Name	Description
Enter 1	Drop WAN	Log out of PPPoE or RoadRunner session.
Enter 9	Reset counters	Resets the counters.
[Esc]		Exits the screen.

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

Table 9-2. System Maintenance Status Fields

Field	Description
Statistics	The statistics for the WAN and LAN ports. For each port, the screen displays:
Status	The link status of the port.
TxPkts	The number of packets transmitted on this port since reset or manual clear.
RxPkts	The number of packets received on this port since reset or manual clear.
Cols	The number of collisions on this port since reset or manual clear.
Tx B/s	The current line utilization—percentage of current bandwidth used on this port.
Tx B/s	The average line utilization —average CLU for this port.
Up Time	The time elapsed since this port acquired link or logged in.
Address information	For the WAN and LAN ports, the screen displays:
Ethernet address	The Ethernet MAC address of the port.
IP address	The IP address assigned to the port.
IP mask	The IP subnet mask assigned to the port.
DHCP	The DHCP status of the port (Client, Server, or None).
System up Time	The time elapsed since the last power cycle or reset.
Name	The name of your router, which you configured in Menu 1 - General Setup.
RAS S/W Version	The version of the current router software.

Log and Trace

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

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

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

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

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

View Error Log

To use the View Error Log:

1. **Open Menu 24.3 - System Maintenance - Log and Trace.**
2. **Select the first option on Menu 24.3.**

   The Error log displays. The Error Log is a 64-entry circular buffer. Use the space bar to scroll this screen if necessary.
3. **After each display, you are prompted with an option to clear the Error Log. Enter the appropriate choice and press [Enter].**

Syslog

Syslog can be configured in Menu 24.3.2 - System Maintenance - UNIX Syslog. 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 - UNIX Syslog 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. The log facility allows the message to be logged to different files in the server. Refer to your UNIX manual for more detail.
Types CDR Packet triggered Filter log PPP log	For each type, press the space bar to toggle between yes and no.	Enable logging for: Call detail record (CDR) Packet trigger Filter event (match or not match) PPP event

To configure the router for logging with the syslogd program on a local host:

1. **Go to Menu 24.3.2 - System Maintenance - UNIX Syslog.**
2. **Set Active to Yes.**
3. **In the Syslog IP Address field, enter the IP address of the syslogd host PC.**
4. **Select a number for Log Facility.**

   You can choose any facility number, but the syslogd program must be set to the same number.
5. **Select the type of activity that you would like to log.**

   You can enable the router to send the following types of syslog messages:

   - Call detail record (CDR)
   - Packet trigger

  - Filter event log
  - PPP event log

6. **Save this menu.**

To configure the syslogd program on the local host PC:

1. **Edit the** ***/etc/syslog.conf*** **file to add the line:**

   ```
   localn.*                /name_of_log_file
   ```

   for example:

   ```
   local6.*                /var/log/rt311.log
   ```

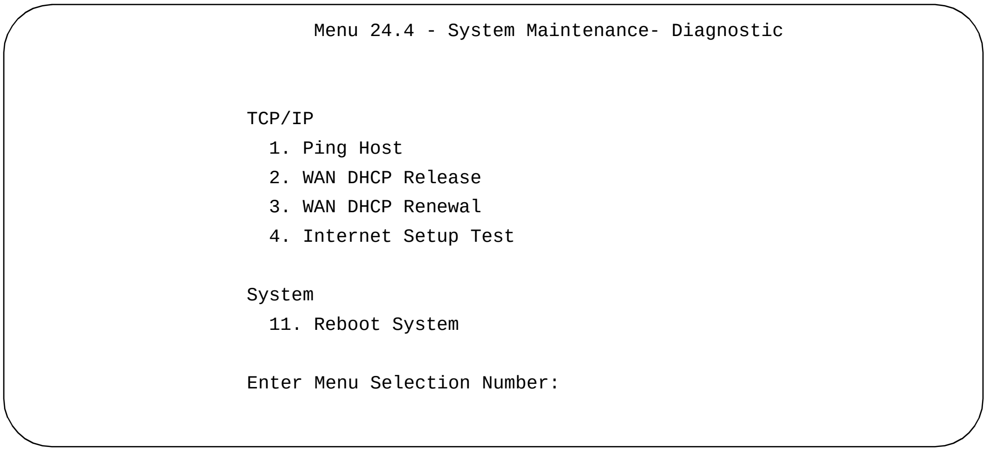
2. **In the syslogd startup script, add the -r option to enable logging from a remote host.**

Diagnostic Menu

The diagnostic menu allows you to:

- Ping another location from your router.
- Release or renew DHCP parameters received from the ISP.
- Test the login to the ISP (for PPPoE only).
- Reboot the router.

From the Main Menu, enter 24 to display Menu 24 - System Maintenance. Enter 4 to display Menu 24.4 - System Maintenance - Diagnostic, shown in Figure 9-3.



```
                           Menu 24.4 - System Maintenance- Diagnostic



                     TCP/IP
                       1. Ping Host
                       2. WAN DHCP Release
                       3. WAN DHCP Renewal
                       4. Internet Setup Test

                     System
                       11. Reboot System

                     Enter Menu Selection Number:
```

Figure 9-3. Menu 24.4 - System Maintenance - Diagnostic

From the Main Menu, enter 24 to display Menu 24 - System Maintenance. Enter 4 to display Menu 24.4 - System Maintenance - Diagnostic. The available commands are listed in Table 9-5.

Table 9-5. System Maintenance - Diagnostic Fields

Field	Command	Description
Ping host	[Enter 1]	This diagnostic test pings a local or remote host. You are prompted for the IP address of the host.
WAN DHCP Release	[Enter 2]	Release the DHCP-assigned parameters received from the ISP.
WAN DHCP Renew	[Enter 3]	Issue a new DHCP request to the ISP for configuration parameters.
Intenet Setup Test	[Enter 4]	Attempt to login to the ISP, showing progress messages.
Reboot system	[Enter 11]	Your system is rebooted, implementing any changes that may have been recently added to your system.

Back Up and Restore Configuration

You can save the router configuration settings to a disk as a binary file. You can also restore the settings from the file at a later time. Saving and restoring the router configuration lets you restore the router to working order if the configuration information in the router is lost or damaged. You can also use the configuration file to configure a new router of the same type if it becomes necessary to replace the router.

NETGEAR highly recommends backing up your router configuration after the router is functioning. You can perform the backup and restore operations through the browser or by using an FTP program. The browser procedure is described in "Configuration File Management" on page 6-5. The FTP procedure is described in the following section.

Backing Up and Restoring the Configuration Using FTP

To back up or restore the configuration file over the LAN, you must have an FTP client program. Windows includes an MS-DOS FTP client program that can be accessed from an MS-DOS prompt. Other FTP client programs are available through many software retailers and shareware sites.

To back up or restore the configuration:

1. **If you are sending a configuration file to the router, first rename it to *rom-0*.**
2. **Establish an FTP connection to the LAN IP address of the router.**

   No login name is necessary. The password is the current Manager password. The factory default password is 1234.
3. **Select binary (not ascii) transfer mode.**
4. **Use your FTP program to get (back up) or put (restore) the file named *rom-0* in the router.**

Software Update

You can update the router software through the browser or by using an FTP program. The browser procedure is described in "Software Upgrade" on page 6-4. The FTP procedure is described in the following section.

Updating Router Software Using FTP

You can update the router software over the LAN or WAN using an FTP client program. Windows includes an FTP client program that can be accessed using the Start button and Run menu. Other FTP client programs are available through many software retailers and shareware sites.

To update the router software:

1. **Rename the new software file to *ras*.**
2. **Establish an FTP connection to the router.**

   No login name is necessary. The password is the current Manager password. The factory default password is 1234.
3. **Select binary (not ascii) transfer mode.**
4. **Use your FTP program to put the file named *ras* in the router.**

After the data transfer is finished, the router programs the upgraded firmware into flash memory and reboots itself, dropping the FTP session.

Command Interpreter Mode

To enter the 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 specified set of commands. To see a list of valid commands, type "help" at the command prompt. For more detailed information, go to the NETGEAR Web site, *www.netgear.com*.
- **Type exit to exit the command interpreter mode.**

Remote Management

Although the router is normally configured by a PC on the local network, it can also be configured and managed over the Internet if remote management is enabled.

To enter the remote management menu:

- **Select option 11 from Menu 24, Maintenance, to enter the Remote Management menu.**
- **Determine which management protocol (Telnet, FTP, or HTTP) will be enabled.**
- **If a non-standard port number will be used for that service, enter that port number as Server Port.**

  The default port (protocol) number is shown.
- **Use the space bar to toggle Server Access to allow access from the LAN only, WAN only, either (ALL), or none (Disable).**
- **If you will manage the router from a particular IP address on the Internet, enter that address as Secured Client IP. If management will be allowed from any IP address, leave it as 0.0.0.0.**

  Note: When remote management is enabled, security for the remote connection is provided by the manager password and the remote manager's IP address, if specified. If you do not specify an IP address, any Internet host who can guess your password will have access to your router.
- **Press ENTER at the bottom of the menu to save your settings.**

Chapter 10
Configuring Filters

This chapter provides information about configuring and using filters for your Model RP114 Web Safe Router.

Filters are used to block certain packets, reduce traffic, and prevent security breaches. The router uses packet filters to determine whether to allow or deny passage of each data packet, based on information found in the packet. A filter is defined by rules declaring what information is to be checked and what action is to be taken (forward or discard) when a match is found. Two types of packet filters are supported by the router: IP protocol filters and generic or “device” filters. An IP protocol filter screens the packet based on IP address and port information contained in the packet. A generic filter looks for a specified pattern of bits at a specified location in the packet.

In the configuration of IP filters, it is necessary to specify ports and protocols by their assigned numbers instead of names. 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.

The Model RP114 router allow you to customize filter sets according to your needs. The following sections describe how to configure the filter sets for your 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 address, or port number. 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.

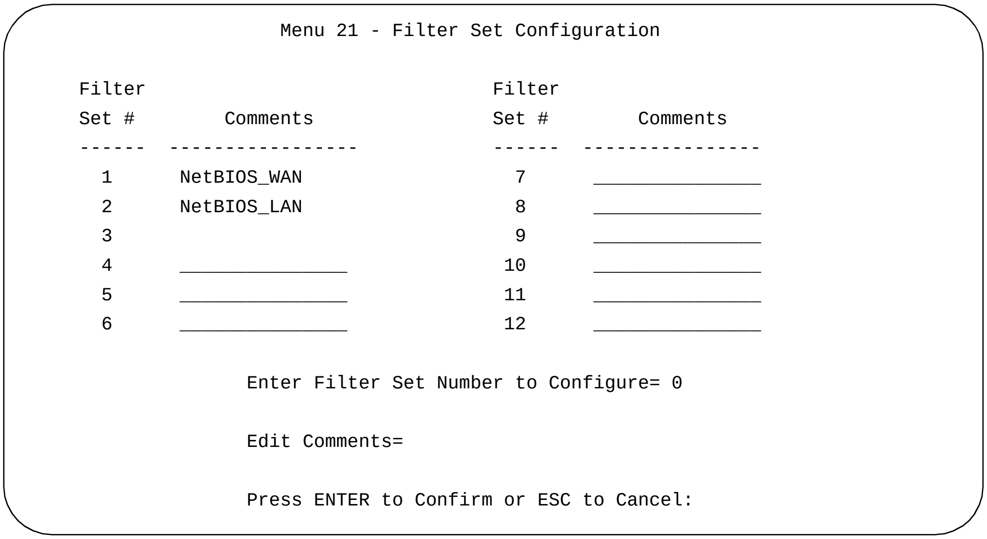
When implementing these filter sets, you can link up to four of the filter sets to screen the data packet. Therefore, with each filter set having up to six rules, you can have a maximum of 24 rules active for a single filtering application.

Configuring a Filter Set

To configure a filter set:

1. **Select option 21 from the Main Menu.**

   The Menu 21 - Filter Set Configuration (Figure 10-1) opens.



```
                  Menu 21 - Filter Set Configuration

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

               Enter Filter Set Number to Configure= 0

               Edit Comments=

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

Figure 10-1. Menu 21 - Filter Set Configuration

   From this menu, you can choose from 12 filter sets.

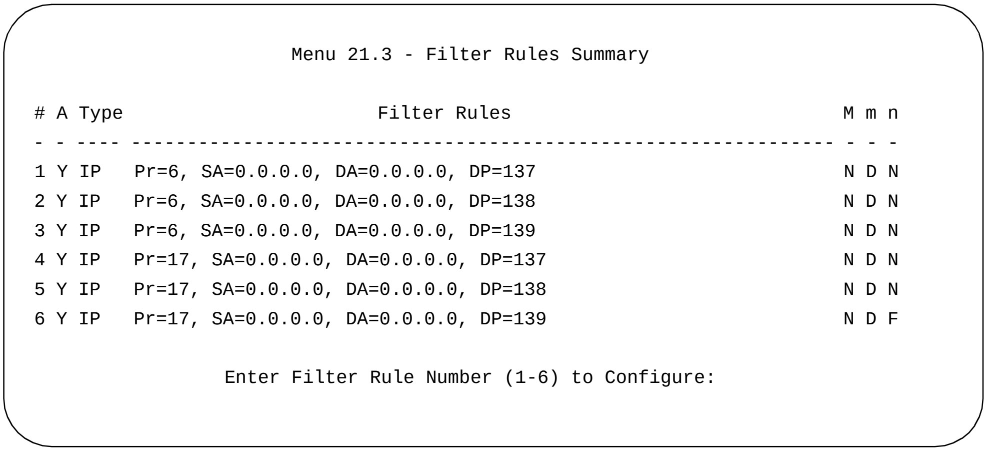
2. **Select the filter that you want to configure or choose an unused set to create a new filter.**

   In order to distinguish between the 12 filter sets, each filter set should have a name or description. When you select a set for editing, you are prompted to provide descriptive text to be displayed in the comment field of Menu 21 next to the filter number.

3. **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 is displayed in the read-only section of Menu 21 - Filter Set Configuration.

4. **Press [Enter] to display Menu 21.1 - Filter Rules Summary (Figure 10-2).**



```
                       Menu 21.3 - Filter Rules Summary

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

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

Figure 10-2. Menu 21.1 - Filter Rules Summary

The information in this menu is read-only; the parameters of each rule that you configured for that set are displayed.

Table 10-1 lists and describes the abbreviations used in Menu 21.1 - Filter Rules Summary.

Table 10-1. 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.

Table 10-1. Abbreviations Used in Menu 21.1 - Filter Rules Summary (continued)

Abbreviation	Description
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 10-6.

If the filter type is IP (TCP/IP), the abbreviations listed in Table 10-2 are used.

Table 10-2. Abbreviations Used if Filter Type Is IP

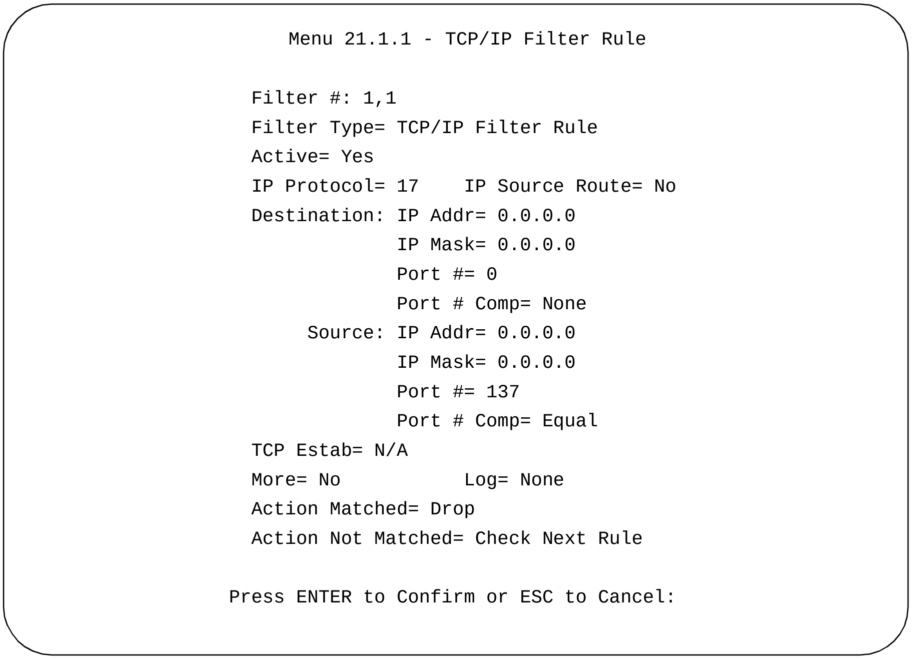
Abbreviation	Description
Pr	Protocol
SA	Source Address
SP	Source Port number
DA	Destination Address

If the filter type is GEN (generic), the abbreviations listed in Table 10-3 are used.

Table 10-3. 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 (Figure 10-3).



```
     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 10-3. Menu 21.1.1 - TCP/IP Filter Rule

Configuring a Filter Rule

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

TCP/IP Filter Rule

This section provides information about how to configure a TCP/IP filter rule for your router. The fields in the menu are given in Table 10-4. 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 10-4 lists and describes the TCP/IP Filter Rule menu fields.

Table 10-4. TCP/IP Filter Rule Fields

Field	**Descriptions**
Active	Make the filter rule active (Yes) or inactive (No).
IP Protocol	Protocol refers to the IP-specific number of the protocol. The range for the value entered in this field should be between 0 and 255 (for example, 6 refers to the TCP protocol).
IP Source Route	Yes or No in this field determines whether to check the source route.
Destination:	
IP Addr	Enter the destination IP address of the packet you want to filter. The address is usually written in dotted-decimal notation such as a.b.c.d where a, b, c, and d are numbers between 0 and 255.
IP Mask	Enter the IP subnet mask that will be used to mask the bits of the IP address given in Destination: IP Addr. Refer to Chapter 1, “Introduction,” for more information.
Port #	Enter the destination port of the packets that you want to filter. The range of this field is 0 to 65535.
Port # Comp	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	Enter the source IP address of the packet you want to filter. The IP address is usually written in dotted-decimal notation such as a.b.c.d where a, b, c, and d are numbers between 0 and 255.
IP Mask	Enter the IP subnet mask that is used to mask the bits of the IP address given in Source: IP Addr. See“Netmask” on page B-4 for information about IP subnet masks.
Port #	Enter the source port of the packets that you want to filter. The range of this field is 0 to 65535.
Port # Comp	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 10-4. TCP/IP Filter Rule Fields (continued)

Field	**Descriptions**
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). Determine what type of TCP packets to filter, from the following two options: • Yes—Filter match only established TCP connections • No—Filter match both initial and established TCP connections (Default)
More	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	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. There are three options 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 10-5 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 10-5. Generic Filter Rule Fields

Field	**Description**
Active	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	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	Specify (in hexadecimal format) the value that the router should logically qualify and the data in the packet. Because length is given in bytes, enter a hexadecimal number that is twice the specified length for numbers in this field. For example, if length is 4, a valid Mask must have 8 hexadecimal numbers (1155ABF8).
Value	Specify (in hexadecimal format) the value that the router should use to compare with the masked packet. The value should align with Offset. Because length is given in bytes, you need to enter twice the length in hexadecimal numbers for this field. For example, if length is 4, a valid value must have 8 hexadecimal numbers (1155ABF8). If the result from the masked packet matches Value, the packet is considered matched.
More	Determine whether to pass the packet through the next filter rule before an action is taken. There are two options: • Yes • No (Default) If Yes is selected, Action Matched and Action Not Matched will be N/A.

Table 10-5. Generic Filter Rule Fields (continued)

Field	Description
Log	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: • 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: • Check Next Rule (default) • Forward • Drop

Applying a Filter Set

After configuring a filter set in Menu 21, you must specify how the filter will be used. Filters are applied at the LAN interface in Menu 3.1 or at the WAN interface in Menu 4.1. You must specify whether the filter is applied to incoming or outgoing packets, and whether filter sets are used alone or combined. You can apply up to four filter sets to the same port by entering the numbers of the desired filter sets separated by commas, with no spaces. In the following example, the user specifies that filter sets 1, 3, and 10 are to be applied to packets entering the router from the LAN:

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

In cascading filter sets, you may need to modify all but the last set in order to have each set continue to the next set rather than terminate. In the example above, you may need to modify Sets 1 and 3 so that they continue to Set 10. On the last rule of a standalone filter set, you normally set "Action if Matched" and "Action if Not Matched" to either "forward"or "drop." However, if you cascade the filter set to another filter set, one of these actions must be "Check Next Rule."

Default Filters

The Model RP114 router is preconfigured with the filters shown in Figure 10-1 on page 10-2 and in this section.

Filter 1: NetBIOS_WAN

The NetBIOS_WAN filter is an IP protocol filter used to prevent the sending of Windows NetBIOS name service packets to the ISP. The ports used by NetBIOS name service are:

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

This filter is applied in Menu 11.5 - Remote Node Filter as an Output Filter set.

Filter 2: NetBIOS_LAN

The NetBIOS_LAN filter is an IP protocol filter used to block NetBIOS name service requests from a local PC to the DNS server of the ISP. These requests are UDP packets having a source port of 137 (NNS) and a destination port of 53 (DNS).

This filter is applied in Menu 3.1 - LAN Port Filter as an Input Filter set.

Filter 3: TEL_FTP_WEB_WAN

The TEL_FTP_WEB_LAN filter is an IP protocol filter used to block Telnet, HTTP, and FTP requests to the router from the Internet. The filter blocks TCP packets with a destination port of 21 (FTP), 23 (Telnet), or 80 (HTTP).

This filter is not used, but can be applied in Menu 11.5 - Remote Node Filter as an Input Filter set.

Chapter 11
Troubleshooting

This chapter gives information about troubleshooting your Model RP114 Web Safe Router. After each problem description, instructions are provided to help you diagnose and solve the problem.

Basic Functioning

After you turn on power to the router, the following sequence of events should occur:

- The PWR LED lights.
- The router performs a self-test for 30 seconds, during which the Test LED should blink at a rate of about 0.5 Hz and then turn off.
- If the LAN and WAN Ethernet connections are correctly made to operational devices, each LNK or LNK/ACT LED should be on.
- If a LAN Ethernet port is connected to a device that operates at 100 Mbps, the 100 LED should be on.

If any of these conditions does not occur, refer to the appropriate following section.

PWR LED Not On

If the PWR and other LEDs are off when your router is turned on:

- Make sure that the power cord is properly connected to your router and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12 V DC power adapter supplied by NETGEAR for this product.

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

Test LED Never Blinks or LED Stays On

When the router is turned on, the Test LED blinks for about 30 seconds at a rate of approximately 0.5 Hz and then turns off. If the Test LED does not blink, or if it stops blinking and stays on, there is a fault within the router.

If you experience problems with the Test LED:

- Cycle the power to see if the router recovers and the LED blinks for the correct amount of time.

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

LNK/ACT LEDs Not On

If either the LAN LNK/ACT LED or WAN LNK LED does not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable:
  - When connecting the router’s WAN port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable may be a standard straight-through Ethernet cable or an Ethernet crossover cable.

Troubleshooting the Web Configuration Interface

If you are unable to access the router’s Web Configuration interface from a PC on your local network, check the following:

- Check the Ethernet connection between your PC and the router as described in the previous section.
- Make sure your PC’s IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your PC’s address should be in the range of 192.168.0.2 to 192.168.0.32. Refer to “Verifying TCP/IP Properties (Windows)“ on page 3-4 or “Verifying TCP/IP Properties (Macintosh)“ on page 3-6 to find your PC’s IP address. Follow the instructions in Chapter 3 to configure your PC.

Note: Recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the Ethernet connection from the PC to the router and reboot your PC.

- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.
- Make sure you are using the correct login information. The factory default login name is “admin” and the password is “1234”. Make sure that CAPS LOCK is off when entering this information.
- Try quitting the browser and launching it again.
- If your router’s IP address has been changed and you don’t know the current IP address, clear the router’s configuration to factory defaults. This will set the router’s IP address to 192.168.0.1.

If the router does not save changes you have made in the Web Configuration Interface, check the following:

- When entering configuration settings, be sure to click the APPLY button before moving to another menu or tab, or your changes are lost.
- Click the Refresh or Reload button in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

Troubleshooting the ISP Connection

If your router is unable to access the Internet, you should first determine whether the router is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your router must request an IP address from the ISP. You can determine whether the request was successful using either the browser interface or the Manager interface.

To check the WAN IP address from the browser interface:

1. **Launch your browser and select an external site such as www.netgear.com**
2. **Access the Main Menu of the router’s configuration at http://192.168.0.1**
3. **Under the Advanced heading, click on Maintenance**
4. **Check that an IP address is shown for the WAN Port**

   If 0.0.0.0 is shown, your router has not obtained an IP address from your ISP.

To check the WAN IP address from the Manager interface:

1. **If your system uses a login script such as PPPoE or RoadRunner, go to Manager interface Menu 24.4 - System Maintenance - Diagnostic and select Internet Setup Test.**

   This will cause your router to attempt to login to the ISP.

2. **Go to Manager interface Menu 24.1 - System Maintenance - Status**
3. **Check that an IP address is shown for the WAN Port**

   If 0.0.0.0 is shown, your router has not obtained an IP address from your ISP.

If your router is unable to obtain an IP address from the ISP, you may need to force your cable or DSL modem to recognize your new router by performing the following procedure:

1. Turn off power to the cable or DSL modem.
2. Turn off power to your router.
3. Wait five minutes and reapply power to the cable or DSL modem.
4. When the modem’s LEDs indicate that it has reacquired sync with the ISP, reapply power to your router.

If your router is still unable to obtain an IP address from the ISP, the problem may be one of the following:

- Your ISP may require a login program.

  Ask your ISP whether they require PPP over Ethernet (PPPoE) or a RoadRunner login.

- If you have selected a login program, you may have incorrectly set the login name and password.
- Your ISP may check for your PC's host name.

  Assign the PC Host Name of your ISP account to the router as System Name in Manager Menu 1, or as Host Name in the browser-based Setup Wizard.

- Your ISP only allows one MAC address to connect to Internet, and may check for your PC’s MAC address.

  Inform your ISP that you have bought a new network device, and ask them to use the router’s MAC address.

  OR

  Configure your router to spoof your PC’s MAC address. This can be done in Manager Menu 2, or in the browser-based Setup Wizard.

If your router can obtain an IP address, but your PC is unable to load any web pages from the Internet:

- Your PC may not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your PC and verify the DNS address as described in "Verifying TCP/IP Properties (Windows)" on page 3-4. Alternatively, you may configure your PC manually with DNS addresses, as explained in your operating system documentation.

- Your PC may not have the router configured as its TCP/IP gateway.

  If your PC obtains its information from the router by DHCP, reboot the PC and verify the gateway address as described in "Verifying TCP/IP Properties (Windows)" on page 3-4.

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

You can ping the router from your PC to verify that the LAN path to your router is set up correctly.

To ping the router from a PC running Windows 95 or later:

1. **From the Windows toolbar, click on the Start button and select Run.**
2. **In the field provided, type Ping followed by the IP address of the router, as in this example:**

   ping 192.168.0.1
3. **Click on OK.**

   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 LNK/ACT LED is on. If the LNK/ACT LED is off, follow the instructions in "LNK/ACT LEDs Not On" on page 11-2.
  - — Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
- Wrong network configuration
  - — Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
  - — Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your PC to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device:

- **From the Windows run menu, type PING -n 10 followed by the IP address of a remote device such as your ISP's DNS server.**

  If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

  — Check that your PC has the IP address of your router listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in the control panel network utility. Go to the Run… window and run winipcfg. The IP address of the router should appear as the Default Gateway.

  — Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.

  — Check internal Manager Menu 24.1 to verify the WAN status. If the menu indicates the WAN status as down, check that your cable or DSL modem is connected and functioning.

  — Check the error log in Menu 24.3.1 for any indication of problems.

  — If your ISP assigned a host name to your PC, enter that host name as the router name in Menu 1.

  — Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Most broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure Menu 2 to allow the router to "borrow" or "spoof" the MAC address from the authorized PC. Refer to "WAN Setup" on page 7-7.

Troubleshooting the Manager Interface

If you cannot access the Manager interface by using the Telnet Protocol:

- Verify the Ethernet connection between your PC and the router. Refer to "Testing the LAN Path to Your Router," on page 11-5.
- If you are attempting to telnet from the WAN side, you must disable the factory default Telnet filter that prevents Telnet access from the WAN. Refer to Chapter 10, "Configuring Filters," for information about setting and clearing filters.

- If your router’s IP address has been changed and you don’t know the current IP address, clear the router’s configuration to factory defaults. This will set the router’s IP address to 192.168.0.1.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the Manager password to 1234 and the IP address to 192.168.0.1. You can erase the current configuration and restore factory defaults in several ways:

- Use the Erase function of the Web Manager (see “Erase the Configuration“ on page 6-5).
- Upload the default config file *romfile0.114*, which can be found on the *Model RP114 Resource* CD. This config file is also available on the NETGEAR Web site. The config file can be uploaded through the Web Manager (see “Configuration File Management“ on page 6-5), or by ftp (see “Backing Up and Restoring the Configuration Using FTP“ on page 9-8).
- Use the Default Reset button on the rear panel of the router. Use this method for cases when the Manager password or IP address is not known.

Using the Default Reset button

To restore the factory default configuration settings without knowing the Manager password or IP address, you must use the Default Reset button on the rear panel of the router.

1. Press the Default Reset button for 10 seconds, then release it.

   If the TEST LED begins to blink, the defaults have been restored and the router is now rebooting. Otherwise, go to step 2.

2. Disconnect the power from the router.
3. While depressing the Default Reset button, reconnect power to the router.

   The TEST LED will begin to blink, then will flicker very quickly after about 10 or 15 seconds. This indicates that the defaults have been restored and the router is now rebooting.

4. Release the Default Reset button and wait for the router to reboot.

Appendix A
Technical Specifications

This appendix provides technical specifications for the Model RP114 Web Safe Router.

General Specifications

Network Protocol and Standards Compatibility	
Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP PPP over Ethernet (PPPoE)
Power Adapter	
North America:	120V, 60 Hz, input
United Kingdom, Australia:	240V, 50 Hz, input
Europe:	230V, 50 Hz, input
Japan:	100V, 50/60 Hz, input
All regions (output):	12 V DC @ 1.2A output, 30W maximum

Physical Specifications	
Dimensions:	159 by 102 by 32 mm 6.25 by 4 by 1.3 in.
Weight:	2.75 kg 1.25 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 B
	EN 55 022 (CISPR 22), Class B
Interface Specifications	
LAN:	10BASE-T or 100BASE-Tx, RJ-45
WAN:	10BASE-T, RJ-45

Appendix B
Network and Routing Basics

This chapter provides an overview of IP networks and routing.

Basic Router Concepts

Large amounts of bandwidth can be provided easily and relatively inexpensively in a local area network (LAN). However, providing high bandwidth between a local network and the Internet can be very expensive. Because of this expense, Internet access is usually provided by a slower-speed wide-area network (WAN) link such as a cable or DSL modem. In order to make the best use of the slower WAN link, a mechanism must be in place for selecting and transmitting only the data traffic meant for the Internet. 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, the router chooses the best path for forwarding network traffic.

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support. The Model RP114 Web Safe Router is a small office router that routes the IP protocol over a single-user broadband 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). Using RIP, routers periodically update one another and check for changes to add to the routing table.

The Model RP114 router supports both the older RIP-1 and the newer RIP-2 protocols. Among other improvements, RIP-2 supports subnet and multicast protocols. RIP is not required for most home applications.

IP Addresses and the Internet

Because TCP/IP networks are interconnected 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). You can contact IANA at www.iana.org.

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 following binary address:

```
11000011  00100010  00001100  00000111
```

is normally written as:

```
195.34.12.7
```

The latter version 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 follow figure shows the three main address classes, including network and host sections of the address for each address type.

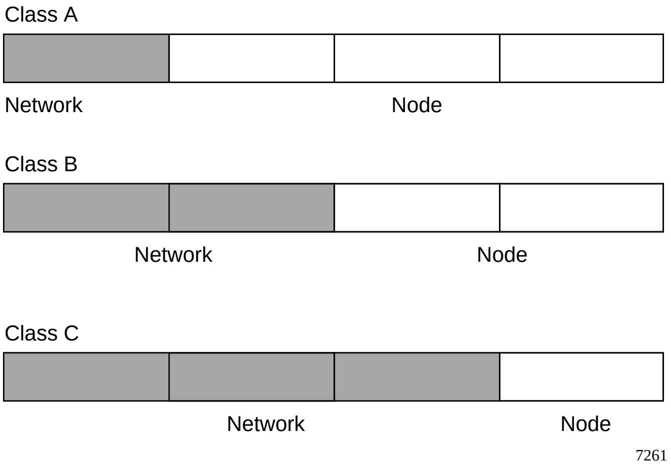


Figure B-1. Three Main Address Classes

The five address classes are:

- Class A
  Class A addresses can have up to 16,777,214 hosts on a single network. They use an eight-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
  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
  Class C addresses can have 254 hosts on a network. Class C addresses use 24 bits for the network address and eight bits for the node. They are in this range:

  `192.0.1.x to 223.255.254.x.`

- Class D
  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
  Class E addresses are for experimental use.

This addressing structure allows IP addresses 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 simultaneously sending a packet to all hosts with the same network address.

Netmask

In each of the address classes previously described, 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 combined (using an AND operator) 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 combined (using an AND operator) with the Class C netmask, as shown here, only the network portion of the address remains:

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

combined with:

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

Equals:

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

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

Subnet Addressing

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

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

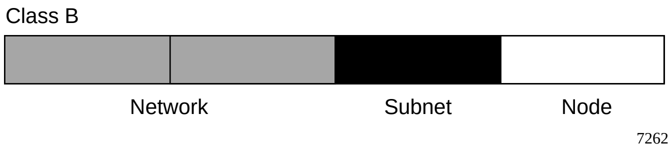


Figure B-2. Example of Subnetting a Class B Address

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 eight 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 one 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. The number 192.68.135.128 is not assigned because it is the network address of the second subnet.

The following table 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 example, to partition your Class C network with subnet mask 255.255.255.0 into 16 subnets (4 bits), the new subnet mask becomes 255.255.255.240.

Table B-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

The following table displays several common netmask values in both the dotted-decimal and the masklength formats.

Table B-2. Netmask Formats

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

Table B-2. Netmask Formats

255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/32

NETGEAR strongly recommends that you configure all hosts on a LAN segment to 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 recognizes which addresses are local and which are remote

Private IP Addresses

If your local network is isolated from the Internet (for example, when using NAT), 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 range. The DHCP server of the Model RP114 router is preconfigured to automatically assign private addresses.

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*. The Internet Engineering Task Force (IETF) publishes RFCs on its Web site at www.ietf.org.

Single IP Address Operation Using NAT

In the past, if multiple PCs on a LAN needed to access the Internet simultaneously, you had to obtain a range of IP addresses from the ISP. This type of Internet account is more costly than a single-address account typically used by a single user with a modem, rather than a router. The Model RP114 router employs an address-sharing method called Network Address Translation (NAT). This method allows several 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)*.

The following figure illustrates a single IP address operation.

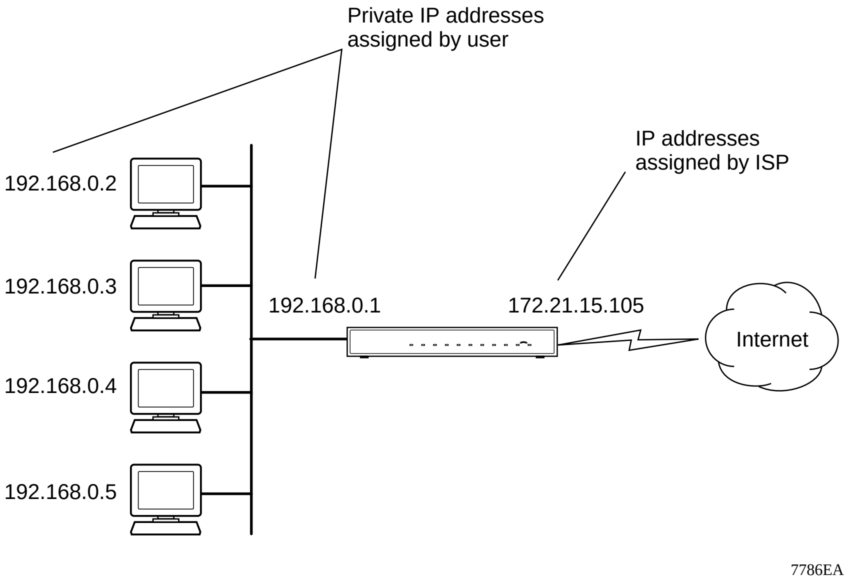


Figure B-3. Single IP Address Operation Using NAT

This scheme offers the additional benefit of firewall-like 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. However, using port forwarding, you can allow one PC (for example, a Web server) on your local network to be accessible to outside users.

MAC Addresses and Address Resolution Protocol

An IP address alone cannot be used to deliver data from one LAN device to another. To send data between LAN devices, 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 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. Internet Protocol uses the Address Resolution Protocol (ARP) to resolve MAC addresses.

If a device sends data to another station on the network and the destination MAC address is not yet recorded, ARP is used. An ARP request is broadcast onto the network. All stations on the network 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. All other stations discard the request.

The station with the correct IP address responds with its own MAC address directly to the sending device. The receiving station provides the transmitting station with the required destination MAC address. The IP address data and MAC address data for each station are held in an ARP table. The next time data is sent, the address can be obtained from the address information in the table.

Domain Name Server

Many of the resources on the Internet can be addressed by simple descriptive names such as *www.NETGEAR.com*. 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 a telephone directory maps names to phone numbers, or as an ARP table maps IP addresses to MAC addresses, a domain name system (DNS) server maps descriptive names of network resources to IP addresses.

When a PC accesses a resource by its descriptive name, it first contacts a DNS server to obtain the IP address of the resource. The PC sends the desired message using the IP address. Many large organizations, such as ISPs, maintain their own DNS servers and allow their customers to use the servers to look up addresses.

IP Configuration by DHCP

When an IP-based local area network is installed, each PC must be configured with an IP address. If the PCs 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 PC on the network can automatically obtain this configuration information. A device on the network may act as a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server stores a list or pool of IP addresses, along with other information (such as gateway and DNS addresses) that it may assign to the other devices on the network. The Model RP114 router has the capacity to act as a DHCP server.

The Model RP114 router also functions as a DHCP client when connecting to the ISP. The router can automatically obtain an IP address, subnet mask, DNS server addresses, and a gateway address if the ISP provides this information by DHCP.

Ethernet Cabling

Although Ethernet networks originally used thick or thin coaxial cable, most installations currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. A normal "straight-through" UTP Ethernet cable follows the EIA568B standard wiring and pinout as described in Table B-3.

Table B-3. UTP Ethernet cable wiring, straight-through

Pin	Wire color	Signal
1	Orange/White	Transmit (Tx) +
2	Orange	Transmit (Tx) -
3	Green/White	Receive (Rx) +
4	Blue	
5	Blue/White	
6	Green	Receive (Rx) -
7	Brown/White	
8	Brown	

Uplink Switches, Crossover Cables, and MDI/MDIX Switching

In the wiring table above, the concept of transmit and receive are from the perspective of the PC, which is wired as Media Dependant Interface (MDI). In this wiring, the PC transmits on pins 1 and 2. At the hub, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X). When connecting a PC to a PC, or a hub port to another hub port, the transmit pair must be exchanged with the receive pair. This exchange is done by one of three mechanisms:

- Uplink switch
  Most hubs provide an Uplink switch which will exchange the pairs on one port, allowing that port to be connected to another hub using a normal Ethernet cable.
- Crossover cable
  A crossover cable is a special cable in which the transmit and receive pairs are exchanged at one of the two cable connectors. Crossover cables are often unmarked as such, and must be identified by comparing the two connectors. Since the cable connectors are clear plastic, it is easy to place them side by side and view the order of the wire colors on each. On a straight-through cable, the color order will be the same on both connectors. On a crossover cable, the orange and blue pairs will be exchanged from one connector to the other.
- Auto MDI/MDI-X switching
  Some Ethernet switch products, such as the Model RP114 router, are able to sense the polarity of a connection and automatically adapt to the proper mating polarity.

Cable Quality

A twisted pair Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or "Cat 5", by the Electronic Industry Association (EIA). This rating will be printed on the cable jacket. A Category 5 cable will meet specified requirements regarding loss and crosstalk. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

Glossary

10BASE-T IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.

100BASE-Tx IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.

CAT5 Category 5. An Electronic Industry Association (EIA) rating for twisted pair cable that meets specified loss and crosstalk requirements for high-speed networking. The cable rating is printed on the cable jacket.

DHCP *See* Dynamic Host Configuration Protocol.

DNS *See* Domain Name Server.

Domain Name Server A Domain Name Server (DNS) resolves descriptive names of network resources (such as www.netgear.com) to numeric IP addresses.

Dynamic Host Configuration Protocol An Ethernet protocol that provides a centralized administration point for assigning network configuration information.

IP *See* Internet Protocol.

IP Address A 4-byte number uniquely defining each host on the Internet. Ranges of addresses are assigned by Internic, an organization formed for this purpose. Usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57).

IPSec Internet Protocol Security. IPSec is a series of guidelines for securing private information transmitted over public networks. IPSec is a VPN method providing a higher level of security than PPTP.

IPX *See* Internet Packet Exchange.

ISP Internet service provider.

Internet Packet Exchange Novell’s internetworking protocol.

Internet Protocol The main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

LAN *See* local area network.

local area network A communications network serving users within a limited geographical area, such as one floor of a building, controlled by a network operating system and using a transport protocol.

MAC address Media Access Control address. A unique 48-bit hardware address assigned to every Ethernet node. Usually written in the form 01:23:45:67:89:ab.

MSB *See* Most Significant Bit or Most Significant Byte.

MRU *See* Maximum Receive Unit.

Maximum Receive Unit The size in bytes of the largest packet that can be sent or received.

Most Significant Bit or Most Significant Byte The portion of a number, address, or field that is farthest left when written as a single number in conventional hexadecimal ordinary notation. The part of the number having the most value.

NAT *See* Network Address Translation.

netmask A number that explains which part of an IP address comprises the network address and which part is the host address on that network. It can be expressed in dotted-decimal notation or as a number appended to the IP address. For example, a 28-bit mask starting from the MSB can be shown as 255.255.255.192 or as /28 appended to the IP address.

Network Address Translation A technique by which several hosts share a single IP address for access to the Internet.

PPP *See* Point-to-Point Protocol.

PPP over Ethernet (PPPoE) PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPTP Point-to-Point Tunneling Protocol. A method for establishing a virtual private network (VPN) by embedding Microsoft's network protocol into Internet packets.

PSTN Public Switched Telephone Network.

packet A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

Point-to-Point Protocol PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.

RFC Request For Comment. Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFCs can be found at www.ietf.org.

RIP *See* Routing Information Protocol.

router A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

Routing Information Protocol A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.

subnet mask *See* netmask.

UTP Unshielded twisted pair. The cable used by 10BASE-T and 100BASE-Tx Ethernet networks.

VPN Virtual Private Network. A method for securely transporting data between two private networks by using a public network such as the Internet as a connection.

WAN *See* wide area network.

wide area network A long distance link used to extend or connect remotely located local area networks.

Windows Internet Naming Service WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses. If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using Network Neighborhood.

WINS *See* Windows Internet Naming Service.

Index