

# Reference Manual for the Model HR314 802.11a Hi-Speed Wireless Router

## **NETGEAR**

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

SM-HR314NA-0  
July 2002

© 2002 by NETGEAR, Inc. All rights reserved.

## **Trademarks**

NETGEAR is a trademark of 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.

## **Federal Communications Commission (FCC) Radiation Exposure Warning**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

## **Radio Frequency Interference Requirements**

This device is restricted to indoor use due to its operation in the 5.15 to 5.25 GHz frequency range. FCC requires this product to be used indoors for the frequency range 5.15 to 5.25 GHz to reduce the potential for harmful interference to cochannel Mobile Satellite systems. High power radars are allocated as primary users of the 5.25 to 5.35 GHz and 5.65 to 5.85 GHz bands. These radar stations can cause interference with and /or damage this device.

## **EN 55 022 Declaration of Conformance**

This is to certify that the Model HR314 802.11a Hi-Speed Wireless 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 HR314 802.11a Hi-Speed Wireless 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 HR314 802.11a Hi-Speed Wireless 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 HR314 802.11a Hi-Speed Wireless 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

## About This Guide

Technical Support .....	xv
Related Publications .....	xv
Typographical Conventions .....	xvi
Special Message Formats .....	xvi

## Chapter 1

### Introduction

About the Router .....	1-1
Key Features .....	1-2
802.11a Standards-based Wireless Networking .....	1-3
Content Filtering .....	1-4
Security .....	1-4
Autosensing 10/100 Ethernet .....	1-5
TCP/IP .....	1-5
Easy Installation and Management .....	1-5
Maintenance and Support .....	1-6

## Chapter 2

### Setting Up the Hardware

Package Contents .....	2-1
The Router's Front Panel .....	2-2
The Router's Rear Panel .....	2-3
Placement of the Router to Optimize Wireless Connectivity .....	2-3
Local Area Network (LAN) Hardware Requirements .....	2-4
PC Requirements .....	2-4
DSL or Cable Modem Requirements .....	2-4
Connecting the Router .....	2-4
Connecting to Your DSL or Cable Modem .....	2-5
Connecting to Your Ethernet LAN .....	2-5
Preparing Wireless Connections .....	2-5

Connecting the Power Adapter .....	2-6
Verifying Connections .....	2-6

### **Chapter 3**

#### **Preparing Your Network**

Preparing Your Computers for TCP/IP Networking .....	3-1
Configuring Windows 95, 98, and ME for TCP/IP Networking .....	3-2
Installing or Verifying Windows Networking Components .....	3-2
Enabling DHCP to Automatically Configure TCP/IP Settings .....	3-4
Selecting Windows' Internet Access Method .....	3-4
Verifying TCP/IP Properties .....	3-5
Configuring Windows NT, 2000 or XP for IP Networking .....	3-5
Install or Verify Windows Networking Components .....	3-5
Verifying TCP/IP Properties .....	3-6
Configuring A Macintosh for TCP/IP Networking .....	3-6
Configuring MacOS 8.6 or 9.x for TCP/IP Networking .....	3-6
Configuring MacOS X for TCP/IP Networking .....	3-7
Verifying Macintosh TCP/IP Properties .....	3-7
Verifying the Readiness of Your DSL or Cable Modem Internet Account .....	3-9
Are Login Protocols Used? .....	3-9
What is Your Configuration Information? .....	3-9
Obtaining ISP Configuration Information for Windows Computers .....	3-10
Obtaining ISP Configuration Information for Macintosh Computers .....	3-11
Restarting the Network .....	3-11
Ready for Configuration .....	3-12

### **Chapter 4**

#### **Basic Configuration of the Router**

Accessing the Web Configuration Manager .....	4-1
Configuration using the Setup Wizard .....	4-4
Configuring Dynamic IP Accounts .....	4-5
Configuring for Fixed IP Accounts .....	4-6
Configuring Login Accounts .....	4-7
Manual Configuration .....	4-8
Completing the Configuration .....	4-9

**Chapter 5**  
**Wireless**

Considerations For A Wireless Network ..... 5-1

    Security ..... 5-2

    Placement and Range ..... 5-2

Wireless LAN Setup ..... 5-3

Firmware Upgrade ..... 5-4

Security ..... 5-5

    Authentication Type ..... 5-5

    WEP and Encryption Keys ..... 5-6

Access Control ..... 5-7

Station List ..... 5-8

**Chapter 6**  
**Content Filtering**

Configuring for Content Filtering ..... 6-1

    E-Mail ..... 6-2

    Block Sites ..... 6-4

    Schedule ..... 6-5

    Logs ..... 6-6

**Chapter 7**  
**Maintenance**

System Status ..... 7-1

Attached Devices ..... 7-4

Router Software Upgrade ..... 7-4

Configuration File Settings Management ..... 7-5

    Restore and Backup the Configuration ..... 7-6

    Erase the Configuration ..... 7-6

Changing the Configuration Password ..... 7-7

**Chapter 8**  
**Advanced Configuration of the Router**

Configuring for Port Forwarding to Local Servers ..... 8-2

    Add a Custom Service ..... 8-3

    Edit or Delete a Port Forwarding Entry ..... 8-3

    Local Web and FTP Server Example ..... 8-3

    Tip: Multiple Computers for Half Life, KALI or Quake III ..... 8-4

Security ..... 8-4

DMZ Server .....	8-4
Respond to Ping on Internet WAN Port .....	8-5
Dynamic DNS .....	8-6
LAN IP Setup .....	8-7
DHCP .....	8-7
Use router as DHCP server .....	8-8
Static Routes .....	8-9
Static Route Example .....	8-10
Packet Filtering .....	8-12
Reserved IP addresses .....	8-13
Remote Management .....	8-15

## **Chapter 9**

### **Troubleshooting**

Basic Functioning .....	9-1
Power LED Not On .....	9-2
Test LED Never Turns On or Test LED Stays On .....	9-2
LAN or Internet Port LEDs Not On .....	9-3
Troubleshooting the Web Configuration Interface .....	9-3
Troubleshooting the ISP Connection .....	9-4
Troubleshooting a TCP/IP Network Using a Ping Utility .....	9-5
Testing the LAN Path to Your Firewall .....	9-6
Testing the Path from Your PC to a Remote Device .....	9-6
Using the Default Reset Button to Restore the Factory Configuration and Password ...	9-7
Problems with Date and Time .....	9-8

## **Appendix A**

### **Technical Specifications**

## **Appendix B**

### **Network and Routing Basics**

Basic Router Concepts .....	B-1
What is a Router? .....	B-1
Routing Information Protocol .....	B-2
IP Addresses and the Internet .....	B-2
Netmask .....	B-4
Subnet Addressing .....	B-5
Private IP Addresses .....	B-7



Single IP Address Operation Using NAT .....	B-8
MAC Addresses and Address Resolution Protocol .....	B-9
Domain Name Server .....	B-9
IP Configuration by DHCP .....	B-10
Wireless Networking .....	B-10
Wireless Network Configuration .....	B-10
Ad-hoc Mode (Peer-to-Peer Workgroup) .....	B-11
Infrastructure Mode .....	B-11
Extended Service Set Identification (ESSID) .....	B-11
Authentication and WEP Encryption .....	B-12
Wireless Channel Selection .....	B-13
Ethernet Cabling .....	B-15
Uplink Switches, Crossover Cables, and MDI/MDIX Switching .....	B-16
Cable Quality .....	B-16

**Glossary**

**Index**



Figure 2-1.	HR314 Front Panel .....	2-2
Figure 2-2.	HR314 Rear Panel .....	2-3
Figure 4-1.	Login window .....	4-2
Figure 4-2.	Browser-based configuration main menu .....	4-3
Figure 4-3.	Setup Wizard menu for Dynamic IP address .....	4-5
Figure 4-4.	Setup Wizard menu for Fixed IP address .....	4-6
Figure 4-5.	Setup Wizard menu for PPPoE login accounts .....	4-7
Figure 5-1.	Wireless LAN Setup menu .....	5-3
Figure 5-2.	Access Point Firmware Upgrade menu .....	5-4
Figure 5-3.	Access Point Security menu .....	5-5
Figure 5-4.	Access Control menu .....	5-7
Figure 5-5.	Station List window .....	5-8
Figure 7-1.	System Status screen .....	7-1
Figure 7-2.	Router Statistics screen .....	7-3
Figure 7-3.	Attached Devices menu .....	7-4
Figure 7-4.	Router Upgrade menu .....	7-5
Figure 7-5.	Backup Settings menu .....	7-6
Figure 7-6.	Set Password menu .....	7-7
Figure 8-1.	Port Forwarding Menu. ....	8-2
Figure 8-2.	Security menu. ....	8-5
Figure 8-3.	LAN IP Setup Menu .....	8-7
Figure 8-4.	Static Routes Summary Table .....	8-9
Figure 8-5.	Static Route Entry and Edit Menu .....	8-10
Figure 8-6.	Packet Filtering (IP Rule) menu .....	8-12
Figure 8-7.	Packet Filtering (Port Rule) menu .....	8-13
Figure 8-8.	Reserve IP menu .....	8-14
Figure 8-9.	Remote Management menu .....	8-15
Figure B-1.	Three Main Address Classes .....	B-3
Figure B-2.	Example of Subnetting a Class B Address .....	B-5
Figure B-3.	Single IP Address Operation Using NAT .....	B-8



Table 2-1.	LED Descriptions .....	2-2
Table 6-1.	Log entry descriptions .....	6-6
Table 6-2.	Log action buttons .....	6-7
Table 7-1.	Menu 3.2 - System Status Fields .....	7-2
Table 7-2.	Router Statistics Fields .....	7-3
Table B-1.	Netmask Notation Translation Table for One Octet .....	B-6
Table B-2.	Netmask Formats .....	B-6
Table B-3.	WEP Key Sizes and Content .....	B-12
Table B-4.	802.11a Wireless Channels .....	B-13
Table B-5.	UTP Ethernet cable wiring, straight-through .....	B-15



# About This Guide

Congratulations on your purchase of the NETGEAR™ Model HR314 802.11a Hi-Speed Wireless Router.

The HR314 connects your entire network of wired and 802.11a wireless PCs to share an Internet connection through a cable modem or DSL modem that otherwise is used by a single PC. The HR314 communicates at up to 54 Mbps. The HR314 is equipped with auto-sensing capability which automatically lowers the speed to 6Mbps for wireless communications across longer distances or for operating in an environment where there is electronic interference. .



**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](http://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 published by the Internet Engineering Task Force (IETF), an open organization that defines the architecture and operation of the Internet. RFC documents are listed on the World Wide Web at [www.ietf.org](http://www.ietf.org) and are mirrored and indexed at many other sites worldwide.

## Typographical Conventions

---





This guide uses the following typographical conventions:

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

## Special Message Formats

---

This guide uses the following formats to highlight special messages:

	<b>Note:</b> This format is used to highlight information of importance or special interest.
	<b>Caution:</b> This format is used to highlight information that will help you prevent equipment failure or loss of data.
	<b>Warning:</b> This format is used to highlight information about the possibility of injury or equipment damage.
	<b>Danger:</b> This format is used to alert you that 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 HR314 802.11a Hi-Speed Wireless Router.

### About the Router

---

The HR314 connects your entire network of wired and 802.11a wireless PCs to share an Internet connection through a cable modem or DSL modem that otherwise is used by a single PC. The HR314 communicates at up to 54 Mbps. The HR314 is equipped with auto-sensing capability which automatically lowers the speed to 6 Mbps for wireless communications across longer distances or for operating in an environment where there is a lot of electronic interference.

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

The HR314 lets you quickly network computers without laying any new cabling, and gives users the freedom to roam throughout the workplace while staying connected to corporate resources. It provides built-in capacity and flexibility for growing networks so it's easy to add new clients or move your entire network to a new office site. Equipped with auto-sensing capability, it allows packet transfer at up to 54 Mbps for maximum throughput, or speed reduction to the lower 6 Mbps speed for distance or for operating in a noisy environment.

The HR314 provides you with multiple Web content filtering options, plus browsing activity reporting and instant alerts -- both via e-mail. You 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.

## Key Features

---

The HR314 provides the following features:

- 802.11a Standards-based wireless networking
  - Blazing fast speeds – up to 54 Mbps, 72 Mbps in turbo mode
  - Free from interference, it coexists with IEEE 802.11b and Bluetooth™ devices
  - Built-in access point
  - Built-in dual antenna assembly to support antenna diversity on both transmit and receive
  - Highest level of data encryption using 152-bit Shared Key data encryption method. Lower level of data encryption or no data encryption is available to simplify your network setup or to improve data transfer rate.
  - WEP keys can be generated manually or by passphrase
  - Ability to restrict wireless access by adapter MAC address
- Easy, web-based setup for installation and management
  - Smart Wizard automatically senses Internet connection type
- Security
  - Allows control of web browsing 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
  - 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
  - Half-duplex or full-duplex operation
- Ethernet connection to a wide area network (WAN) device, such as a cable modem or DSL modem
  - Allows Ethernet connection at 10 megabits per second (Mbps)

- Protocol Support
  - IP routing
  - Network Address Translation (NAT) 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:
    - PPP over Ethernet (PPPoE) accounts
    - PPTP service (for European service providers)
    - BigPond service (for Telstra Australia)
- Front panel LEDs for easy monitoring of status and activity
- Flash memory for firmware upgrade

## 802.11a Standards-based Wireless Networking

The HR314 includes an 802.11a-compliant wireless access point, providing continuous, high-speed access between your wireless and Ethernet devices at up to 54 Mbps for maximum throughput, or speed reduction to the lower 6 Mbps speed for distance or for operating in a noisy environment. The access point provides:

- 802.11a Standards-based wireless networking at up to 54 Mbps, 72 Mbps in turbo mode
- Wired Equivalent Privacy (WEP) data encryption (64-bit/128-bit/152-bit) accomplished on the fly
- WEP keys can be generated manually or by passphrase
- Wireless access can be restricted by MAC address
- Distributed coordinated function (CSMA/CA, Back off procedure, ACK procedure, retransmission of unacknowledged frames)
- RTS/CTS handshake

- Duplicate detection and Recovery
- Beacon generation
- Fragmentation and reassembly
- Roaming among access points on the same subnet

## Content Filtering

With its content filtering features, the HR314 prevents objectionable content from reaching your PCs. Its content filtering features include:

- Content filtering by domain or keyword  
The HR314 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 Website names.
- Logging of inappropriate use  
You can configure the HR314 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 HR314 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.
- Encryption of the Wireless Link  
For security against eavesdropping of the wireless signal, the router supports Wired Equivalent Privacy (WEP) data encryption with Shared Key authentication. You can also restrict access to the wireless network by MAC address.

## Autosensing 10/100 Ethernet

With its internal, 4-port 10/100 switch, the HR314 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.

## TCP/IP

The HR314 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 Sharing by NAT**  
The HR314 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, known as Network Address Translation (NAT), allows the use of an inexpensive single-user ISP account.
- **Automatic Configuration of Attached PCs by DHCP**  
The HR314 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 PCs on your local network.
- **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 a DSL connection by simulating a dial-up connection. This feature eliminates the need to run a login program such as EnterNet or WinPOET on your PC.

## Easy Installation and Management

You can install, configure, and operate the Model HR314 802.11a Hi-Speed Wireless 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.
- **Smart Wizard**  
The HR314 automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- **Visual monitoring**  
The HR314'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 HR314:

- Flash memory for firmware upgrade

# Chapter 2

## Setting Up the Hardware

This chapter describes the Model HR314 802.11a Hi-Speed Wireless Router hardware and provides instructions for setting it up.

### Package Contents

---

The product package should contain the following items:

- Model HR314 802.11a Hi-Speed Wireless Router
- AC power adapter
- Category 5 (CAT5) Ethernet cable
- *Model HR314 Resource CD*, including:
  - This manual
  - Application Notes, Tools, and other helpful information
- *HR314 Hi-Speed Wireless Router Installation Guide*
- Warranty and registration card
- Support information card

Keep the carton, including the original packing materials, in case you need to return the product for repair.

## The Router's Front Panel

The front panel of the Model HR314 802.11a Hi-Speed Wireless Router ([Figure 2-1](#)) contains status LEDs.



**Figure 2-1.** HR314 Front Panel

You can use some of the LEDs to verify connections. [Table 2-1](#) describes each LED on the front panel of the router. These LEDs are green when lit, except for the TEST LED, which is amber.

**Table 2-1.** LED Descriptions

Label	Activity	Description
POWER	On	Power is supplied to the router.
TEST	On Off	The system is initializing. The system is ready and running.
INTERNET LINK ACT (Activity)	On Blinking	The Internet port has detected a link with an attached device. Data is being transmitted or received by the Internet port.
WIRELESS LINK/ACT (Link/Activity)	On Blinking	The Wireless port is ready. Data is being transmitted or received by the Wireless port.
LAN 100 (100 Mbps) LINK/ACT (Link/Activity)	On Off On Blinking	The Local port is operating at 100 Mbps. The Local port is operating at 10 Mbps. The Local port has detected a link with an attached device. Data is being transmitted or received by the Local port.



## The Router's Rear Panel

The rear panel of the HR314 (Figure 2-2) contains port connections.



**Figure 2-2.** HR314 Rear Panel

The rear panel contains the following features (right to left):

- AC power adapter outlet
- Four Local (LAN) Ethernet ports for connecting the router to the local PCs
- Factory Default Reset pushbutton
- Internet (WAN) Ethernet port for connecting the router to a cable or DSL modem
- Grounding terminal

## Placement of the Router to Optimize Wireless Connectivity

---

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the router. For best results, place your router:

- Near the center of the area in which your PCs will operate,
- In an elevated location such as a high shelf,
- Away from potential sources of interference, such as PCs, microwaves, and cordless phones,
- Away from large metal surfaces.



**Warning:** Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router.

## Local Area Network (LAN) Hardware Requirements

---

The HR314 is intended for use in a network of personal computers that are interconnected by 802.11a-compliant wireless adapters or twisted-pair Ethernet cables.

### PC Requirements

To install and run the HR314 over your network, each computer must have the following:

- An installed 802.11a-compliant wireless adapter

OR

- An Ethernet Network Interface Card (NIC).  
For interconnecting your wired Ethernet devices, the HR314 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.

### DSL or Cable Modem Requirements

The cable modem or DSL modem must provide a standard 10 Mbps (10BASE-T) Ethernet interface. The router does not support USB modems.

## Connecting the Router

---

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

- For wireless communications, identify a suitable location to place the router according to the guidelines in [“Placement of the Router to Optimize Wireless Connectivity”](#) on page 2-3. Then, prepare your wireless devices as described below.
- Connect your cable or DSL modem to the Internet port of the router (see [page 2-5](#)).
- Connect your local Ethernet network to the LAN port(s) of the router (see [page 2-5](#)).
- Connect the power adapter (see [page 2-6](#))

**Note:** The Resource CD included with your router contains an animated Installation Assistant to help you through this procedure.

## Connecting to Your DSL or Cable Modem

Using the Ethernet cable already attached to your cable modem or DSL modem, connect the router's Internet port to the Ethernet port on the modem. Turn the modem off for ten seconds, then on again.

## Connecting to Your Ethernet LAN

Your Ethernet network will attach to the four LAN ports on the router shown in [Figure 2-2](#). The LAN ports can operate at either 10 Mbps (10BASE-T) or 100 Mbps (100BASE-Tx), depending on the Ethernet adapters in the attached computers, hub, or switch. You must use a Category 5 (CAT5) rated Ethernet cable, such as the cable included with the router, for any connection which will operate at 100 Mbps.

The HR314 incorporates a four-port switch for connection to your local network. To connect the router to your LAN:

- Connect up to four computers directly to any of the four LAN ports of the router using standard Ethernet cables.
- To connect more than 4 computers on the Ethernet LAN, you will need to connect your router to another hub or switch. Connect any port of the other hub or switch to any LOCAL port of your router. The router's LOCAL port will automatically configure itself for the uplink connection.

**Note:** The HR314 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 switch or hub). That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables. Auto Uplink will accommodate either type of cable to make the right connection.

## Preparing Wireless Connections

Rotate the antennas to a vertical position.

Detailed instructions on configuring your wireless devices for TCP/IP networking are provided in the next chapter. However, if you already have a functioning wireless network and you wish to use a wireless PC to initially configure the router, you will need to change the settings of that PC to match the default settings of the router:

- The SSID should be **Wireless** (note the capitalization).
- WEP encryption is disabled.
- Your IP address must be in the range of 192.168.0.3 to 192.168.0.254, with a netmask of 255.255.255.0

See [Chapter 5, “Wireless”](#) for full details on setting up wireless connections.

## Connecting the Power Adapter

To connect the router to the power adapter:

1. Plug the connector of the power adapter into the power 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 Power LED on the router is lit.

## Verifying Connections

---

After applying power to the router, complete the following steps to verify the connections to it:

1. When power is first applied, verify that the POWER LED is on.
2. Verify that the TEST LED turns on within a few seconds.
3. After approximately 10 seconds, verify that:
  - a. The TEST LED has turned off.
  - b. The WIRELESS LINK/ACT LED is lit.
  - c. The LOCAL LINK/ACT LEDs are lit for any local ports that are connected.
  - d. The INTERNET LINK/ACT LED is lit.  
If a LINK/ACT LED is lit, a link has been established to the connected device.
4. If any LOCAL port is connected to a 100 Mbps device, verify that the 100 LED for that port is lit.

The router is now properly attached to the network. Next, you need to prepare your network to access the Internet through the router. See 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 HR314 802.11a Hi-Speed Wireless Router and how to verify the readiness of a broadband DSL or cable modem account from an Internet service provider (ISP).



**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. Write down this information before reconfiguring your PCs. Refer to [“Obtaining ISP Configuration Information for Windows Computers”](#) on page 3-10 or [“Obtaining ISP Configuration Information for Macintosh Computers”](#) on page 3-11 for further information.

### Preparing Your Computers for TCP/IP Networking

---

Computers access the Internet using a protocol called TCP/IP (Transmission Control Protocol/Internet Protocol). Each computer on your network must have TCP/IP installed and selected as its networking protocol. If a Network Interface Card (NIC) is already installed in your computer, then TCP/IP is probably already installed as well.

Most operating systems include the software components you need for networking with TCP/IP:

- Windows® 95 or later 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..

In your TCP/IP network, each computer and the router must be assigned a unique IP addresses. Each computer must also have other TCP/IP configuration information such as a subnet mask, a domain name server (DNS) address, and a default gateway address. In most cases, you should install TCP/IP so that the computer obtains its network configuration information automatically from a DHCP server during bootup. For a detailed explanation of the meaning and purpose of these configuration items, refer to “[Appendix B, “Networks, Routing, and Firewall Basics.”](#)”

The HR314 is shipped preconfigured as a DHCP server. The router assigns the following TCP/IP configuration information automatically when the computers are rebooted:

- PC, Macintosh, or workstation IP addresses—192.168.0.3 through 192.168.0.254
- 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, 98, and ME for TCP/IP Networking**

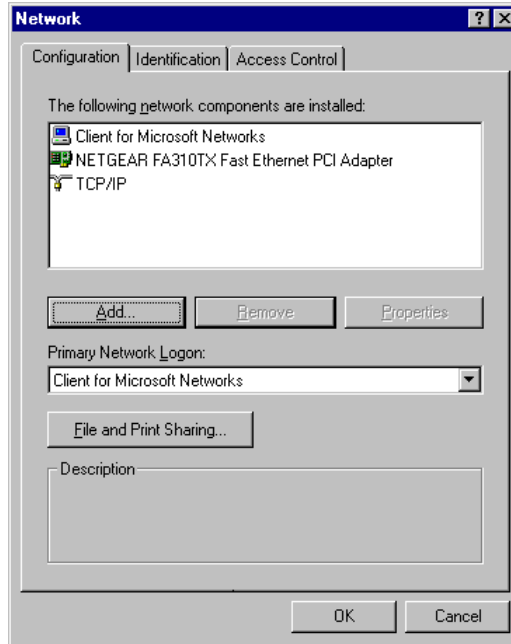
As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

### **Installing or Verifying Windows Networking Components**

To install or verify the necessary components 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:



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.

### **Enabling DHCP to Automatically Configure TCP/IP Settings**

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 HR314. To use DHCP with the recommended default addresses, follow these steps:

1. Connect all PCs to the router, then restart the router and allow it to boot.
2. On each attached PC, open the Network control panel (refer to the previous section) and select the Configuration tab.
3. From the components list, select TCP/IP->(your Ethernet adapter) and click Properties.
4. In the IP Address tab, select “Obtain an IP address automatically”.
5. Select the Gateway tab.
6. If any gateways are shown, remove them.
7. Click OK.
8. Restart the PC.

Repeat steps 2 through 8 for each PC on your network.

### **Selecting Windows' Internet Access Method**

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Internet Options icon.
3. Select “I want to set up my Internet connection manually” or “I want to connect through a Local Area Network” and click Next.
4. Select “I want to connect through a Local Area Network” and click Next.
5. Uncheck all boxes in the LAN Internet Configuration screen and click Next.
6. Proceed to the end of the Wizard.



## Verifying TCP/IP Properties

After your PC is configured and has rebooted, you can check the TCP/IP configuration using the utility *winiipcfg.exe*:

1. On the Windows taskbar, click the Start button, and then click Run.
2. Type `winiipcfg`, and then click OK.

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

3. From the drop-down box, 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 192.168.0.3 and 192.168.0.254
- The subnet mask is 255.255.255.0
- The default gateway is 192.168.0.1

## Configuring Windows NT, 2000 or XP 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.

### Install or Verify Windows Networking Components

To install or verify the necessary components 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 and Dialup Connections icon.
3. If an Ethernet adapter is present in your PC, you should see an entry for Local Area Connection. Double-click that entry.
4. Select Properties.
5. Verify that 'Client for Microsoft Networks' and 'Internet Protocol (TCP/IP)' are present. If not, select Install and add them.
6. Select 'Internet Protocol (TCP/IP)', click Properties, and verify that "Obtain an IP address automatically" is selected.

7. Click OK and close all Network and Dialup Connections windows.
8. Make sure your PC is connected to the router, then reboot your PC.

### **Verifying TCP/IP Properties**

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 `cmd` and then click OK.

A command window opens

3. Type `ipconfig /all`

Your IP Configuration information will be listed, and should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

- The IP address is between 192.168.0.3 and 192.168.0.254
- The subnet mask is 255.255.255.0
- The default gateway is 192.168.0.1

4. Type `exit`

## **Configuring A Macintosh for TCP/IP Networking**

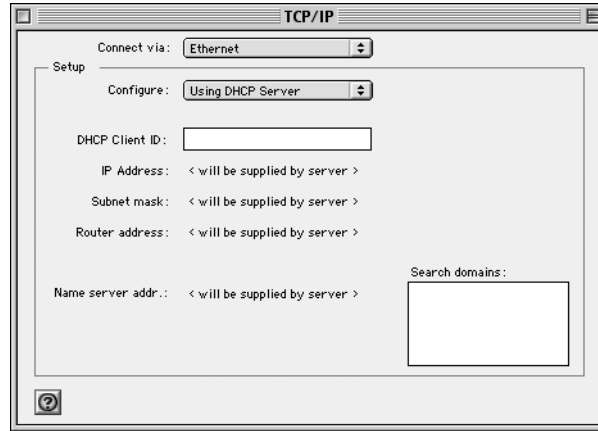
---

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.

### **Configuring MacOS 8.6 or 9.x for TCP/IP Networking**

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

The TCP/IP Control Panel opens::



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.

## Configuring MacOS X for TCP/IP Networking

1. From the Apple menu, choose System Preferences, then Network.
2. If not already selected, select Built-in Ethernet in the Configure list.
3. If not already selected, Select Using DHCP in the TCP/IP tab.
4. Click Save.

## Verifying Macintosh TCP/IP Properties

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.

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 192.168.0.3 and 192.168.0.254
- 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”.

## Verifying the Readiness of Your DSL or Cable Modem 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 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 computer. Your router does not support a USB-connected broadband modem.

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. You need to configure the router with the TCP/IP information that the single PC would normally use. When the router is connected to the broadband modem, the router appears to be a single PC to the ISP. The router then allows multiple computers on the local network to masquerade as the single PC to access the Internet through the broadband modem.

### Are Login Protocols Used?

Some ISPs require a special login protocol, in which you must enter a login name and password in order to access the Internet. If you normally log in to your Internet account by running a program such as WinPOET or EnterNet, then your account uses PPP over Ethernet (PPPoE). When you configure your router, you will need to enter your login name and password in the router's configuration menus.



**Note:** After your network and router are configured, the router will perform the login task when needed, and you will no longer need to run the login program from your PC. It is not necessary to uninstall the login program.

### What is Your Configuration Information?

More and more, ISPs are dynamically assigning configuration information. However, if your ISP does not dynamically assign configuration information but instead used fixed configurations, your ISP should have given 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 for Windows Computers**

As mentioned above, you may need to collect configuration information from your PC so that you can use this information when you configure the HR314. 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 for Macintosh Computers**

As mentioned above, you may need to collect configuration information from your Macintosh so that you can use this information when you configure the HR314. 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.

### **Restarting the Network**

---

Once you’ve set up your computers to work with the router, you must reset the network for the devices to be able to communicate correctly.

1. Turn off the DSL or cable modem, wait 15 seconds, and then turn it on again

2. Turn off the router, and then turn it on again and wait until the Test light turns off.
3. Restart any computer that is connected to the router.

**Note:** If the modem doesn't have an on/off switch, either pull the modem's power adapter out of the wall socket or power down the power strip.

## **Ready for Configuration**

---

After configuring all of your PCs for TCP/IP networking and connecting them to the local network of your HR314, 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 HR314 802.11a Hi-Speed Wireless Router using the Setup Wizard, which walks you through the configuration process for your Internet connection.

### Accessing the Web Configuration Manager

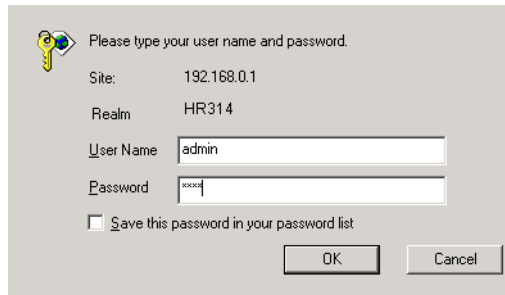
---

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 Microsoft Internet Explorer 5.0 or Netscape Navigator 4.7 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 ten seconds and verify that the Test LED is off.
2. Reboot your PC to obtain DHCP configuration from the router.
3. Launch your web browser.  
**Note:** If you normally use a login program (such as Enternet or WinPOET) to access the Internet, do not launch that program.
4. Click your browser's Stop button.
5. In the Address (or Location) box of your browser, type **http://192.168.0.1** and press ENTER.

A login window opens as shown in [Figure 4-1](#) below:.



**Figure 4-1. Login window**

This screen may have a different appearance in other browsers.

6. Type **admin** in the User Name box, **password** in the Password box, and then click OK.

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

If your router has not yet been configured, the Setup Wizard should launch automatically.

Otherwise, the main menu of the Web Configuration Manager will appear as shown in [Figure 4-2](#) below:

**NETGEAR Cable/DSL Wireless Router HR314**  
settings

**Basic Settings**

**Does Your Internet Connection Require A Login?**

Yes  
 No

**Account Name** (If Required)

**Domain Name** (If Required)

**Internet IP Address**

Get Dynamically From ISP  
 Use Static IP Address

IP Address:

IP Subnet Mask:

Gateway IP Address:

**Domain Name Server (DNS) Address**

Get Automatically From ISP  
 Use These DNS Servers

Primary DNS:

Secondary DNS:

**Router MAC Address**

Use Default MAC Address  
 Use Computer MAC Address  
 Use This MAC Address

Apply Cancel Test

**Help**

The HR314 *Settings* pages allow you to configure, upgrade and check the status of your NETGEAR Cable/DSL Web Safe Router.

Click an item in the leftmost column. The current settings or information for that area appear in the center column.

Helpful information related to the selected *Settings* page appears in this column. If you are using Internet Explorer, you may click an item in the center column to jump directly to the related help section; otherwise, scroll down until you reach it.

**Basic Settings Help**

**Note:** If you are setting up the router for the first time, the default settings may work for you with no changes.

**Does your Internet connection require a login?**

Select this option based on the type of account you have with your ISP. If you need to enter login information every time you connect to the Internet or you have a PPPoE account with your ISP, select **Yes**. Otherwise, select **No**.

**Figure 4-2. Browser-based configuration main menu**

You can manually configure your router using this menu as described in “Manual Configuration“ on page 4-8, or you can allow the Setup Wizard to determine your configuration as described in the following chapter.

## Configuration using the Setup Wizard

---

The Web Configuration Manager contains a Setup Wizard that can automatically determine your network connection type. If the Setup Wizard does not launch automatically, click on the Setup Wizard heading in the upper left of the opening screen, shown in [Figure 4-2](#).

When the Wizard launches, allow the router to automatically determine your connection type by selecting Yes in the menu below and clicking Next:

### Setup Wizard

---

**The Smart Setup Wizard Can Detect The Type Of Internet Connection That You Have.**

**Do You Want The Smart Setup Wizard To Try And Detect The Connection Type Now?**

- Yes.
- No. I Want To Configure The Router Myself.

---

Next

The Setup Wizard will now check for a connection on the Internet port. If the Setup Wizard determines that there is no connection to the Internet port, you will be prompted to check the physical connection between your router and cable or DSL modem. When the connection is properly made, the router's Internet LED should be on.

Next, the Setup Wizard will attempt to determine which of the following connection types your Internet service account uses:

- Dynamic IP assignment
- Fixed IP address assignment
- A login protocol such as PPPoE

The Setup Wizard will report which connection type it has discovered, and it will then use the appropriate configuration menu for that connection type.

## Configuring Dynamic IP Accounts

If the Setup Wizard determines that your Internet service account uses Dynamic IP assignment, you will be directed to the menu shown in [Figure 4-3](#) below:

**Dynamic IP**

---

**Account Name** (If Required)

**Domain Name** (If Required)

---

**Domain Name Server (DNS) Address**

Get Automatically From ISP

Use These DNS Servers

Primary DNS

Secondary DNS

---

**Router's MAC Address**

Use Default Address

Use This MAC Address

---

**Figure 4-3. Setup Wizard menu for Dynamic IP address**

1. Enter your Account Name (may also be called Host Name) and Domain Name. 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 may need to enter it manually.
2. Domain Name Server (DNS) Address: If you know that your ISP does not automatically transmit DNS addresses to the router during login, select "Use these DNS servers" and enter the IP address of your 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.

3. Router's MAC Address: This section determines the Ethernet MAC address that will be used by the router on the Internet port. If your ISP allows access by only one specific PC's Ethernet MAC address, select "Use this MAC address". The router will then capture and use the MAC address of the PC that you are now using. You must be using the one PC that is allowed by the ISP.

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.

4. Click on Apply, then proceed to ["Completing the Configuration"](#) on page 4-9.

## Configuring for Fixed IP Accounts

If the Setup Wizard determines that your Internet service account uses Fixed IP assignment, you will be directed to the menu shown in [Figure 4-4](#) below:

**Fixed IP**

---

**Internet IP Address**

IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
IP Subnet Mask	<input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="0"/>
Gateway IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>

---

**Domain Name Server (DNS) Address**

Primary DNS	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Secondary DNS	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>

---

**Figure 4-4. Setup Wizard menu for Fixed IP address**

1. Enter your assigned IP Address, Subnet Mask, and the IP Address of your ISP's gateway router. This information should have been provided to you by your ISP.
2. Domain Name Server (DNS) Address: If you know that your ISP does not automatically transmit DNS addresses to the router during login, select "Use these DNS servers" and enter the IP address of your 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.

- Click on Apply, then proceed to [“Completing the Configuration” on page 4-9](#).

## Configuring Login Accounts

If the Setup Wizard determines that your Internet service account uses a login protocol such as PPP over Ethernet (PPPoE), you will be directed to a menu like the PPPoE menu shown in [Figure 4-5](#) below:

**PPPoE**

Account Name

Domain Name

Login

Password

Idle Timeout

**Domain Name Server (DNS) Address**

Get automatically from ISP

Use these DNS servers

Primary DNS

Secondary DNS

Apply Cancel Test

**Figure 4-5. Setup Wizard menu for PPPoE login accounts**

- Enter your Account Name (may also be called Host Name) and Domain Name. 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.
- 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 minutes.

**Note:** You will no longer need to launch the ISP's login program on your PC in order to access the Internet. When you start an Internet application, your router will automatically log you in.

3. Domain Name Server (DNS) Address: If you know that your ISP does not automatically transmit DNS addresses to the router during login, select "Use these DNS servers" and enter the IP address of your 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.

4. Click on Apply, then proceed to ["Completing the Configuration" on page 4-9](#).

## Manual Configuration

---

You can manually configure the router in the Basic Settings menu shown in [Figure 4-2](#) using these steps:

1. Select whether your Internet connection requires a login.  
Select 'Yes' if you normally must launch a login program such as Enternet or WinPOET in order to access the Internet.
2. Enter your Account Name (may also be called Host Name) and Domain Name. These parameters may be necessary to access your ISP's services such as mail or news servers.
3. (If displayed) 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 minutes.  
**Note:** You will no longer need to launch the ISP's login program on your PC in order to access the Internet. When you start an Internet application, your router will automatically log you in.
4. Internet IP Address: If your ISP has assigned you a permanent, fixed (static) IP address for your PC or router, select "Use static IP address". Enter the IP address that your router has been assigned. Also enter the netmask and the Gateway IP address. The Gateway is the ISP's router to which your router will connect.



5. Domain Name Server (DNS) Address: If you know that your ISP does not automatically transmit DNS addresses to the router during login, select “Use these DNS servers” and enter the IP address of your 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.

6. Router’s MAC Address: This section determines the Ethernet MAC address that will be used by the router on the Internet port. 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 “cloning” its MAC address. You can specify the MAC address in one of two ways:
  - a. Select "Use this Computer’s MAC address". The router will then capture and use the MAC address of the PC that you are now using. You must be using the one PC that is allowed by the ISP.
  - b. Select "Use this MAC address" and manually enter the MAC address you wish to use.
7. Click on Apply, then proceed to [“Completing the Configuration” on page 4-9](#).

## Completing the Configuration

---

Click on the Test button to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to [Chapter 9, “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 or login application such as Dial-Up Networking or Internet 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.

The following chapters describe how to configure the Advanced features of your router, and how to troubleshoot problems that may occur.



# Chapter 5

## Wireless

This chapter describes how to configure the wireless features of your Model HR314 802.11a Hi-Speed Wireless Router.



**Note:** If you are configuring the router from a wireless PC and you change the router's SSID, channel, or WEP settings, you will lose your wireless connection when you click on Apply. You must then change the wireless settings of your PC to match the router's new settings.

From the menu bar on the left of the Main Menu of the browser interface, you can select the wireless configuration menus under the Access Point heading.

### Considerations For A Wireless Network

---

In planning your wireless network, you should consider the level of security required. You should also select the physical placement of your router in order to maximize the network speed. For further information on wireless networking, refer to [“Wireless Networking”](#) in [Appendix B](#), [“Network and Routing Basics.”](#)

## Security

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, NETGEAR strongly recommends that you make use of the security features of your wireless equipment. As a minimum security precaution, you should change the SSID setting of all devices on your network from the factory setting to a unique password. Restricting access by MAC address filtering adds another obstacle against unwanted hosts joining your network. To hinder a determined eavesdropper, you should enable Wired Equivalent Privacy (WEP) data encryption. However, there may be a significant degradation of the data throughput on the wireless link when WEP is enabled.

## Placement and Range

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless router. For best results, place your router:

- Near the center of the area in which your PCs will operate,
- In an elevated location such as a high shelf,
- Away from potential sources of interference, such as PCs, microwaves, and cordless phones,
- Away from large metal surfaces.



**Warning:** Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router.

## Wireless LAN Setup

To configure the Wireless LAN interface of your router, click on Wireless LAN Setup under the Access Point heading in the Main Menu of the browser interface. The Wireless LAN Setup menu will appear, as shown in [Figure 5-1](#):

**Wireless LAN setup**

---

SSID:	<input type="text" value="Wireless"/>
Channel / Frequency:	<input type="text" value="52 / 5.26GHz"/>
Turbo Mode:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Data Rate:	<input type="text" value="best"/>
Transmit Power:	<input type="text" value="full"/>
Beacon Interval: (20 - 1000)	<input type="text" value="100"/> ms
DTIM (1 - 16384):	<input type="text" value="1"/>

**Figure 5-1. Wireless LAN Setup menu**

The parameters for this menu are:

- **SSID (Service Set ID)**  
Enter a value of up to 32 alphanumeric characters. The same SSID must be assigned to all wireless devices in your network. The default SSID is **Wireless**, but NETGEAR strongly recommends that you change your network's SSID to a different value.
- **Channel/Frequency**  
Shows the current channel and frequency in use. The wireless channel in use will be between 36 and 64 or 42, 48, 54 with turbo mode enabled. Default: 52 (non-turbo), 42 (Turbo)
- **Turbo Mode**  
Enabling turbo mode allows the wireless node to transmit or receive at a higher rate, up to 72 Mbps. Default: Disable
- **Data Rate**  
Shows the available transmit data rate of the wireless network. The possible data rates supported are: 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps, and 6 Mbps. It can go up to 72 Mbps if the turbo mode is enabled. Default: Best

- **Transmit Power**  
Set the transmit signal strength of the access point. The options are “full”, ”half”, “quarter”, “eighth”, “and “min”. Decrease the transmit power if more than one AP is co-located using the same channel frequency. Default: Full
- **Beacon Interval**  
Specifies the Beacon Interval value. Enter a value in between 20 to 1000. Default: 100
- **DTIM**  
The Delivery Traffic Indication Message. Specifies the data beacon rate between 1 and 16384. Default: 1

## Firmware Upgrade

---

The firmware of the internal access point is separately upgradeable from the router’s firmware. To upgrade the access point firmware, click on Firmware Upgrade under the Access Point heading in the Main Menu of the browser interface. The Firmware Upgrade menu will appear, as shown in [Figure 5-2](#)

**Firmware Upgrade**

---

FTP server:  
IP address:     Parameters

Username:

Password:

File name:

**Figure 5-2. Access Point Firmware Upgrade menu**

The internal access point will contact an FTP server to download new firmware. To upgrade the access point, follow these steps:

1. Obtain the new access point firmware from NETGEAR’s website.
2. Install an FTP server on a computer on your local network.  
Simple FTP server software for personal computers can be found at many shareware sites.
3. Create a login account for the router on the FTP server.

4. Copy the new access point firmware file to the login directory of the FTP server.
5. In this router menu, enter the FTP server address, the login name and password, and the file name.
6. Click Apply.  
The router will log in to your FTP server, download the file, and install it.

**Note:** The installation will take a few minutes. Please do not interrupt the router during this period.

## Security

To configure the security features of the internal access point, click on Security under the Access Point heading in the Main Menu of the browser interface. The Security menu will appear, as shown in [Figure 5-3](#)

**Security**

---

**Authentication Type:**     Open System     Shared Key

---

**WEP:**     Disable     Enable

---

Encryption Key (Hex 0-9 A-F)	Key Size
<input type="radio"/> Auto <input type="radio"/> Manual	
Passphrase: <input style="width: 100px;" type="text"/>	<input type="button" value="Generate"/>
1 Shared Key 1: <input style="width: 150px;" type="text" value="1234567890123456789012"/>	<input style="width: 50px;" type="text" value="152 bits"/> ▼
2 Shared Key 2: <input style="width: 150px;" type="text"/>	<input style="width: 50px;" type="text" value="64 bits"/> ▼
3 Shared Key 3: <input style="width: 150px;" type="text"/>	<input style="width: 50px;" type="text" value="64 bits"/> ▼
4 Shared Key 4: <input style="width: 150px;" type="text"/>	<input style="width: 50px;" type="text" value="64 bits"/> ▼
Default Shared Key: <input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4	

---

**Figure 5-3. Access Point Security menu**

### Authentication Type

Select the Authentication type to be used:

- Open System  
Open System (no authentication or encryption)
- Shared Key (default)  
If “Shared Key” is selected, you need to enable the WEP and enter at least one shared key.

For easy installation, Open System is the default. However, NETGEAR strongly recommends that you change to Shared Key.

### **WEP and Encryption Keys**

Enable or Disable the Wired Equivalent Privacy. If WEP is enabled, you can manually or automatically program the four data encryption keys.

- Manual - Type the keys as hexadecimal digits (any combination of 0-9, a-f, or A-F)
- Automatic - Enter a word or group of printable characters in the Passphrase box and click the Generate Keys button.
- Shared Key (1-4)  
Specifies the shared key value in hexadecimal format based on the key size selected: 64 bits, 128 bits, or 152 bits. Default Key Size: 64 bits
- Default Shared Key  
Specifies the preferred share key entry from 1 to 4. Default: 1

**Note:** You must configure all PCs and Access Points in your network with the same KEY values to communicate.



## Access Control

For increased security, you can restrict access to the wireless network to only allow specific PCs, based on their MAC addresses. In this case, the router will authenticate each wireless PC by SSID and by MAC address, using the list of MAC addresses you have entered. To use this feature, click on Access Control under the Access Point heading in the Main Menu of the browser interface. The Access Control menu will appear, as shown in [Figure 5-4](#)

**Access Control**

Access Control  Disable  Enable

MAC Address:

	Index	Device Name	Mac Address
<input type="radio"/>	1	MAC1	00:B0:D0:7F:3A:0A
<input checked="" type="radio"/>	2	MAC2	11:22:33:44:55:66

**Figure 5-4. Access Control menu**

To specify the allowed MAC addresses, type or paste each MAC address into the box provided, then click Add. The MAC address will then appear in the list at the bottom of the menu.

You can modify or delete an entry by selecting it and then using the Edit or Delete buttons.

When you have entered all of the desired MAC addresses, enable Access Control and click Apply.

**Note:** If you apply this feature while connected wirelessly from a PC whose MAC is not on the list, you will lose communication with the router.

## Station List

---

The Station List window displays the assigned ID, MAC address and the current state of the access point and all the stations currently part of its Basic Service Set (BSS). To view the station list, click on Station List under the Access Point heading in the Main Menu of the browser interface. The Station List window will appear, as shown in [Figure 5-5](#)

### Station List

ID	MAC Address	State
AP	00:09:5B:01:23:45	up
STA1	00:09:5B:01:98:76	associated
STA2	00:09:5B:0A:BC:DE	associated

**Figure 5-5. Station List window**

# Chapter 6

## Content Filtering

This chapter describes how to use the Content Filtering features of your Model HR314 802.11a Hi-Speed Wireless Router. These features can be found by clicking on the Content Filtering heading in the Main Menu of the browser interface.

### Configuring for Content Filtering

---

The Model HR314 802.11a Hi-Speed Wireless 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 subheadings under the Content Filtering heading in the Main Menu of the browser interface. The subheadings are described below:

## E-Mail

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

**E-mail**

---

**Turn E-mail Notification On.**

---

**Send Alert And Logs Via E-mail**  
Your Outgoing Mail Server:  
  
Send To This E-mail Address:

---

**Send Alert Immediately**  
When Someone Attempts To Visit A Blocked Site.

---

Send Logs According To This Schedule  
When Log is Full ▾  
Sunday ▾  
12:00 ▾  A.M.  P.M.

---

**Time Zone**  
  
 Adjust for Daylight Savings Time

---

**Current Time : 22:37:22, Wednesday.**

---

- **Turn e-mail notification on**  
Check this box if you wish to receive e-mail logs and alerts from the router.
- **Your outgoing mail server**  
Enter the name of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You may be able to find this information in the configuration menu of your e-mail program. If you leave this box blank, log and alert messages will not be sent via e-mail.
- **Send to this e-mail address**  
Enter the e-mail address to which logs and alerts are sent. This e-mail address will also be used as the From address. If you leave this box blank, log and alert messages will not be sent via e-mail.

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

- Send alert immediately  
Check this box if you would like immediate notification of attempted access to a blocked site.
- Send logs according to this 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. Relevant when the log is sent daily or weekly.

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 HR314 uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet. In order to localize the time for your log entries, you must specify your Time Zone:

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

## Block Sites

The HR314 allows you to restrict access based on web addresses and web address keywords. Up to 255 entries are supported in the Keyword list. The Keyword Blocking menu is shown below:

**Block Sites**

---

Turn Keyword Blocking On

---

Type Keyword Or Domain Name Here:

---

Block Sites Containing These Keywords Or Domain Names:

badstuff

---

Allow Trusted IP Address To Visit Blocked Sites

Trusted IP address

---

To enable keyword blocking, check “Turn keyword blocking on”, then click Apply. Be sure that a time period for blocking is specified on the Schedule menu.

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.
- 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.

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

You may 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.

## Schedule

The HR314 allows you to specify when blocking will be enforced. The Schedule tab is shown below:

**Schedule**

---

**Days To Block:**

Every day  
 Sunday  
 Monday  
 Tuesday  
 Wednesday  
 Thursday  
 Friday  
 Saturday

---

**Time Of Day To Block:** (use 24-hour clock)

All Day

Start Blocking:       Hour  Min

End Blocking:         Hour  Min

---

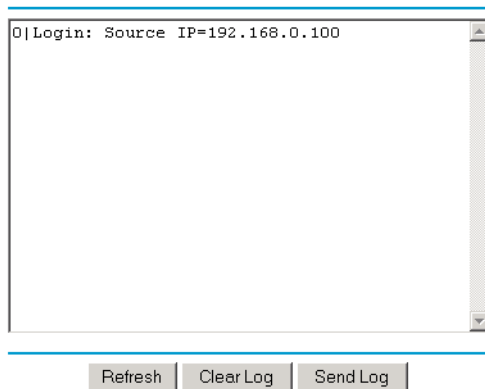
- Use this schedule for blocking content  
Check this box if you wish to enable a schedule for Content Filtering. Click Apply.
- Days to Block  
Select days to block by checking the appropriate boxes. Select Everyday to check the boxes for all days. Click Apply.
- Time of Day to Block  
Select a start and end time in 23:59 format. Select All day for 24 hour blocking. Click Apply.

Be sure to select your Time Zone in the E-Mail menu.

## 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. An example is shown below:

### Logs



Log entries are described in [Table 6-1](#)

**Table 6-1. Log entry descriptions**

Field	Description
Number	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.
Date and Time	The date and time the log entry was recorded.
Source IP	The IP address of the initiating device for this log entry.
Action	This field displays whether the access was blocked or allowed.
	The name or IP address of the website or newsgroup visited or attempted to access.



Log action buttons are described in [Table 6-2](#)

**Table 6-2. Log action buttons**

<b>Field</b>	<b>Description</b>
Refresh	Click this button to refresh the log screen.
Clear Log	Click this button to clear the log entries.
Send Log	Click this button to email the log immediately.



# Chapter 7

## Maintenance

This chapter describes how to use the maintenance features of your Model HR314 802.11a Hi-Speed Wireless 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 7-1](#).

**Router Status**

---

<b>System Name</b>	
<b>Firmware Version</b>	4.10 RC2 May 21 2002

---

**Internet Port**

<b>MAC Address</b>	00:40:33:00:00:8B
<b>IP Address</b>	0.0.0.0
<b>DHCP</b>	Client
<b>IP Subnet Mask</b>	None

---

**LAN Port**

<b>MAC Address</b>	00:40:33:00:00:8A
<b>IP Address</b>	192.168.0.1
<b>DHCP</b>	Server
<b>IP Subnet Mask</b>	255.255.255.0

---

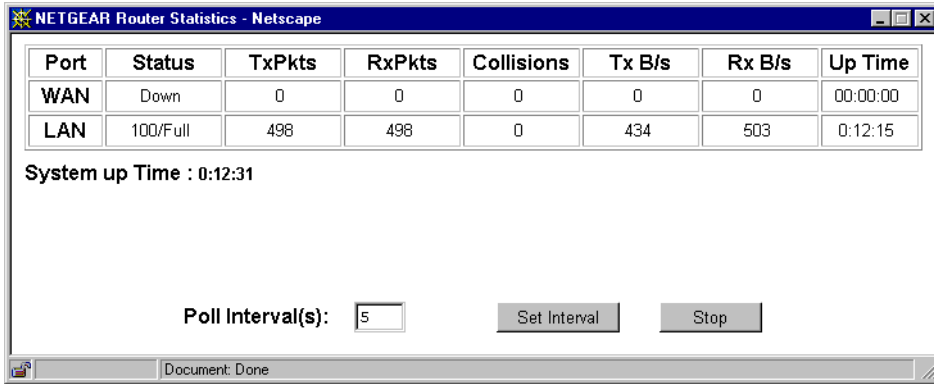
**Figure 7-1. System Status screen**

This screen shows the following parameters:

**Table 7-1. Menu 3.2 - System Status Fields**

<b>Field</b>	<b>Description</b>
System Name	This field displays the Host Name assigned to the router.
Firmware Version	This field displays the router firmware version.
WAN Port	These parameters apply to the Internet (WAN) port of the router.
MAC Address	This field displays the Ethernet MAC address being used by 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 (LAN) port of the router.
MAC Address	This field displays the Ethernet MAC address being used by the Local (LAN) 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 7-2](#) below:



**Figure 7-2. Router Statistics screen**

This screen shows the following statistics:.

**Table 7-2. 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.

Click on the “Show PPPoE Status” button to display the progress of the PPPoE connection.

## Attached Devices

---

The Attached Devices menu contains a table of all IP devices that the router has discovered on the local network. From the Main Menu of the browser interface, under the Maintenance heading, select Attached Devices to view the table, shown in [Figure 7-3](#)

### Attached Devices

#	IP Address	Device Name	MAC Address
1	192.168.0.2	emachine	00:48:54:8d:d7:d3

Refresh

**Figure 7-3.** Attached Devices menu

For each device, the table shows the IP address, NetBIOS Host Name (if available), and Ethernet MAC address. Note that if the router is rebooted, the table data is lost until the router rediscovers the devices. To force the router to look for attached devices, click the Refresh button.

## Router Software Upgrade

---

The routing software of the HR314 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 HR314 must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer 5.0 or Netscape Navigator 4.7 or above.

From the Main Menu of the browser interface, under the Maintenance heading, select the Router Upgrade heading to display the menu shown in [Figure 7-4](#).

Router Upgrade

---

Locate And Select The Upgrade File From Your Hard Disk:

---

**Figure 7-4. Router Upgrade menu**

To upload new firmware:

1. Download and unzip the new software file from NETGEAR.
2. In the Router 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 HR314, 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. The upgrade process will typically take about one minute.

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

## Configuration File Settings Management

---

The configuration settings of the HR314 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.

From the Main Menu of the browser interface, under the Maintenance heading, select the Backup Settings heading to bring up the menu shown in [Figure 7-5](#).

**Backup Settings**

---

Save A Copy Of Current Settings

---

Restore Saved Settings From a File

---

Revert To Factory Default Settings

---

**Figure 7-5. Backup Settings menu**

Three options are available, and are described in the following sections.

## Restore and Backup the Configuration

The Restore and Backup options in the Settings Backup 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 from the router and will prompt you for a location on your PC to store the file. You can give the file a meaningful name at this time, such as `pacbell.cfg`.

To restore your settings from a saved configuration file, enter the full path to the file on your PC or click the Browse button to browse to the file. When you have located it, click the Restore 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 **password**, 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 button.



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 to Restore the Factory Configuration and Password”](#) on page 9-7.

## Changing the Configuration Password

---

The default password for the router’s Web Configuration Manager is **password**. Netgear recommends that you change this password to a more secure password.

From the Main Menu of the browser interface, under the Maintenance heading, select Set Password to bring up the menu shown in [Figure 7-6](#).

**Set Password**

---

Old Password	<input type="text"/>
New Password	<input type="text"/>
Repeat New Password	<input type="text"/>

---

**Figure 7-6. Set Password menu**

To change the password, first enter the old password, and then enter the new password twice. Click Apply.



# Chapter 8

## Advanced Configuration of the Router

This chapter describes how to configure the advanced features of your Model HR314 802.11a Hi-Speed Wireless Router. These features can be found under the Advanced heading in the Main Menu of the browser interface.

## 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 a local server (for example, a web server or game server) visible and available to the Internet. This is done using the Port Forwarding menu. From the Main Menu of the browser interface, under Advanced, click on Port Forwarding to view the port forwarding menu, shown in Figure 8-1

**Port Forwarding**

Service Name: SERVICES Server IP Address: 192.168.0. Add

#	Service Name	Start Port	End Port	Server IP Address
1	foogame	1234	1235	192.168.0.119

Add Custom Service Edit Service Delete Service

**Figure 8-1. Port Forwarding Menu.**



**Note:** Some 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 Port Forwarding menu to configure the router to forward incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a Default DMZ Server to which all other incoming protocols are forwarded. The DMZ Server is configured in the Security Menu.

Before starting, you'll need to determine which type of service, application or game you'll provide and the IP address of the computer that will provide each service. Be sure the computer's IP address never changes.

To configure port forwarding to a local server:

1. From the Service & Game box, select the service or game that you will host on your network. If the service does not appear in the list, refer to the following section, "[Add a Custom Service](#)".

2. Enter the IP address of the local server in the corresponding Server IP Address box.
3. Click the Add button.

### **Add a Custom Service**

To define a service, game or application that does not appear in the Services & Games list, you must determine what port numbers are used by the service. For this information, you may need to contact the manufacturer of the program that you wish to use. When you have the port number information, follow these steps:

1. Click the Add Custom Service button.
2. Enter the first port number in an unused Start Port box.
3. 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.
4. Enter the IP address of the local server in the corresponding Server IP Address box.
5. Type a name for the service.
6. Click Apply at the bottom of the menu.

### **Edit or Delete a Port Forwarding Entry**

To edit or delete a Port Forwarding entry, follow these steps.

1. In the table, select the button next to the service name.
2. Click Edit or Delete.

### **Local Web and FTP Server Example**

If a local PC with a private IP address of 192.168.0.33 acts as a Web and FTP server, configure the Ports menu to forward HTTP (port 80) and FTP (port 21) to local address 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, you can manually configure the PC to use a fixed address or you can use the Reserved IP Address feature described in [“Reserved IP addresses“](#) on page 8-13.
- 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.

### **Tip: Multiple Computers for Half Life, KALI or Quake III**

To set up an additional computer to play Half Life, KALI or Quake III:

1. Click the button of an unused port in the table.
2. Select the game again from the Services/Games list.
3. Change the beginning port number in the Start Port box.  
For these games, use the supplied number in the default listing and add +1 for each additional computer. For example, if you've already configured one computer to play Hexen II (using port 26900), the second computer's port number would be 26901, and the third computer would be 26902.
4. Type the same port number in the End Port box that you typed in the Start Port box.
5. Type the IP address of the additional computer in the Server IP Address box.
6. Click Apply.

Some online games and videoconferencing applications are incompatible with NAT. The HR314 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.

## **Security**

---

### **DMZ Server**

Incoming traffic from the Internet is normally discarded by the router unless the traffic is a response to one of your local computers or a service that you have configured in the Port Forwarding menu. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the Default DMZ Server.

The Default DMZ Server feature is helpful when using some online games and videoconferencing applications that are incompatible with NAT. The 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 DMZ Server.

The Security menu, shown in [Figure 8-2](#), allows the configuration of a Default DMZ Server.

Security

---

Default DMZ Server      192 . 168 . 0 . 0

---

Respond To Ping On Internet WAN Port

---

Apply    Cancel

**Figure 8-2. Security menu.**



**Note:** For security, you should avoid using the Default DMZ Server feature. When a computer is designated as the Default DMZ Server, it loses much of the protection of the router, and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

To assign a computer or server to be a Default DMZ server:

1. Click Default DMZ Server.
2. Type the IP address for that server.
3. Click Apply.

### Respond to Ping on Internet WAN Port

If you want the router to respond to a 'ping' from the Internet, click the 'Respond to Ping on Internet WAN Port' check box. This should only be used as a diagnostic tool, since it allows your router to be discovered. Don't check this box unless you have a specific reason to do so.

## Dynamic DNS

---

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial dynamic DNS service, who will allow you to register your domain to their IP address, and will forward traffic directed at your domain to your frequently-changing IP address.

The router contains a client that can connect to many popular dynamic DNS services. You can select one of these services and obtain an account with them. Then, whenever your ISP-assigned IP address changes, your router will automatically contact your dynamic DNS service provider, log in to your account, and register your new IP address.

From the Main Menu of the browser interface, under Advanced, click on Dynamic DNS. To configure Dynamic DNS:

1. Access the website of one of the dynamic DNS service providers whose names appear in the 'Select Service Provider' box, and register for an account.  
For example, for dyndns.org, go to [www.dyndns.org](http://www.dyndns.org).
2. Select the Use a dynamic DNS service check box.
3. Select the name of your dynamic DNS Service Provider.
4. Type the Host Name that your dynamic DNS service provider gave you.  
The dynamic DNS service provider may call this the domain name.
5. Type the User Name for your dynamic DNS account.
6. Type the Password (or key) for your dynamic DNS account.
7. If your dynamic DNS provider allows the use of wildcards in resolving your URL, you may select the Use wildcards check box to activate this feature.  
For example, the wildcard feature will cause `*.yourhost.dyndns.org` to be aliased to the same IP address as `yourhost.dyndns.org`
8. Click Apply to save your configuration.



**Note:** If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the dynamic DNS service will not work because private addresses will not be routed on the Internet.



## LAN IP Setup

The second feature category under the Advanced heading is LAN IP 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 IP Setup to view the LAN IP Setup menu, shown in [Figure 8-3](#)

**LAN IP Setup**

---

**Use Router As DHCP Server**

Starting IP Address      192 . 168 . 0 . 2

Ending IP Address      192 . 168 . 0 . 50

---

**LAN TCP/IP Setup**

IP Address      192 . 168 . 0 . 1

IP Subnet Mask      255 . 255 . 255 . 0

RIP Direction      Both ▼

RIP Version      RIP-1 ▼

---

Apply      Cancel

**Figure 8-3. LAN IP Setup Menu**

The router is shipped preconfigured to use private IP addresses on the LAN side, and to act as a DHCP server. The router's default LAN IP configuration is:

- LAN IP addresses—192.168.0.1
- Subnet mask—255.255.255.0

These addresses are part of the IETF-designated private address range for use in private networks, and should be suitable in most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in this menu.

## DHCP

By default, the router will function as a DHCP (Dynamic Host Configuration Protocol) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the router's LAN. 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.

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

### **Use router as DHCP server**

If another device on your network will be the DHCP server, or if you will manually configure the network settings of all of your computers, clear the ‘Use router as DHCP server’ check box. Otherwise, leave it checked.

Specify the pool of IP addresses to be assigned by setting the Starting IP Address and Ending IP Address. These addresses should be part of the same IP address subnet as the router’s LAN IP address. Using the default addressing scheme, you should define a range between 192.168.0.2 and 192.168.0.253, although you may wish to save part of the range for devices with fixed addresses.

The router will deliver the following parameters to any LAN device that requests DHCP:

- An IP Address from the range you have defined
- Subnet Mask
- Gateway IP Address (the router’s LAN IP address)
- Primary DNS Server (if you entered a Primary DNS address in the Basic Settings menu; otherwise, the router’s LAN IP address)
- Secondary DNS Server (if you entered a Secondary DNS address in the Basic Settings menu)

### **LAN TCP/IP Setup**

The LAN IP parameters are:

- IP Address  
This is the LAN IP address of the router.
- IP Subnet Mask  
This is the LAN Subnet Mask of the router. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.
- RIP Direction  
RIP (Router Information Protocol) allows a router to exchange routing information with other routers. The RIP Direction selection controls how the router sends and receives RIP packets. Both is the default.
  - When set to Both or Out Only, the router will broadcast its routing table periodically.

- When set to Both or In Only, it will incorporate the RIP information that it receives.
- When set to None, it will not send any RIP packets and will ignore any RIP packets received.
- **RIP Version**  
This controls the format and the broadcasting method of the RIP packets that the router sends. (It recognizes both formats when receiving.) By default, this is set for RIP-1.
  - RIP-1 is universally supported. RIP-1 is probably adequate for most networks, unless you have an unusual network setup.
  - RIP-2 carries more information. RIP-2B uses subnet broadcasting..



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

## Static Routes

Static Routes provide additional routing information to your router. 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 Routes to view the Static Routes menu, shown in [Figure 8-4](#).

### Static Routes

#	Active	Name	Destination	Gateway
1	YES	idsn_rtr	134.177.0.0	192.168.0.99

**Figure 8-4. Static Routes Summary Table**

To add or edit a Static Route:

1. Select a number and click the Edit button to open the Edit Menu, shown in [Figure 8-5](#).

Route Name	<input type="text" value="isdn_rtr"/>
<input checked="" type="checkbox"/> Private	
<input checked="" type="checkbox"/> Active	
Destination IP Address	<input type="text" value="134"/> <input type="text" value="177"/> <input type="text" value="0"/> <input type="text" value="0"/>
IP Subnet Mask	<input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="0"/> <input type="text" value="0"/>
Gateway IP Address	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="0"/> <input type="text" value="99"/>
Metric	<input type="text" value="1"/>

---

**Figure 8-5. Static Route Entry and Edit Menu**

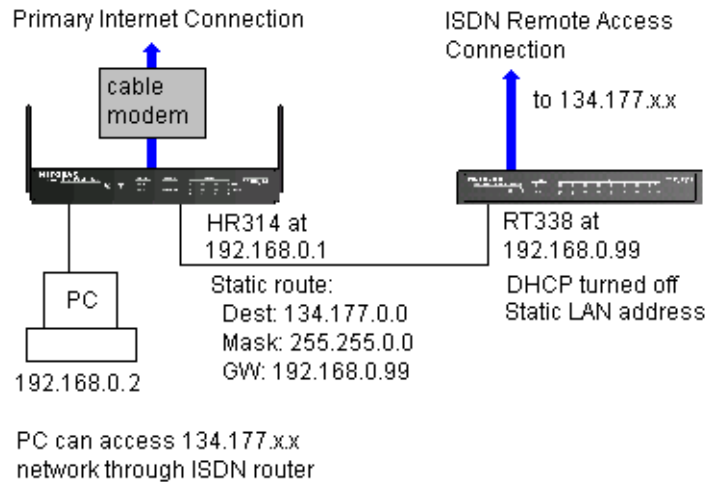
2. Type a route name for this static route in the Route Name box under the table. (This is for identification purpose only.)
3. Select Private if you want to limit access to the LAN only. The static route will not be reported in RIP.
4. Select Active to make this route effective.
5. Type the Destination IP Address of the final destination.
6. Type the IP Subnet Mask for this destination.  
If the destination is a single host, type 255.255.255.255.
7. Type the Gateway IP Address, which must be a router on the same LAN segment as the router.
8. Type a number between 1 and 15 as the Metric value.  
This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.
9. Click Apply to have the static route entered into the table.

## 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 192.168.0.99.
- Your company's network is 134.177.0.0.

This example is illustrated below:



When you first configured your router, a default route was created with your ISP as the gateway. 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 192.168.0.99. The static route would look like [Figure 8-5](#).

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 192.168.0.99.
- A Metric value of 1 will work since the ISDN router is on the LAN.
- Private is selected only as a precautionary security measure in case RIP is activated.

## Packet Filtering

---

The Model HR314 802.11a Hi-Speed Wireless Router allows you to block Internet access by specific users on your local network based on their IP addresses. In addition, you can prevent the use of certain Internet services. These functions are performed by packet filtering.

From the Main Menu of the browser interface, under Advanced, click on Packet Filtering to view the Packet Filtering menu, shown in [Figure 8-6](#).

The screenshot shows the 'Packet Filtering' configuration page. At the top, the title 'Packet Filtering' is displayed in blue. Below it, the checkbox 'Enable Packet Filtering' is checked. Underneath, the 'Packet Rule:' section has two radio buttons: 'IP Rule' (selected) and 'Port Rule'. Below this is a table with two columns: '#' and 'Destination IP'. The table contains one row with the value '1' in the '#' column and '192.168.0.33' in the 'Destination IP' column. At the bottom of the table are four buttons: 'Apply', 'Add', 'Edit', and 'Delete'.

#	Destination IP
1	192.168.0.33

**Figure 8-6. Packet Filtering (IP Rule) menu**

To block Internet access by a PC on your network:

1. Make sure the Enable Packet Filtering checkbox is checked.
2. Select IP Rule.
3. Click Add.
4. In the next screen, enter the IP address to be blocked.
5. Click OK  
The address should now appear in the table.
6. Click Apply.

By selecting Port Rule, you can block access to a specific Internet service from your network. For example, you can prevent your users from using chat or games. The Port Rule menu is shown in Figure 8-7.

**Packet Filtering**

Enable Packet Filtering

---

Packet Rule:  IP Rule  Port Rule

---

#	Service Type	Protocol	Port
1	TCP	FTP	21

Apply Add Edit Delete

**Figure 8-7. Packet Filtering (Port Rule) menu**

To block a service:

1. Make sure the Enable Packet Filtering checkbox is checked.
2. Select Port Rule.
3. Click Add.
4. From the Protocol list in the next screen, select the service to be blocked.  
If it does not exist, select “User defined” and specify the port number(s), protocol, and name.
5. Click OK  
The entry should now appear in the table.
6. Click Apply.

To delete or edit an entry in the table, click its button and then click Edit or Delete.

## Reserved IP addresses

Reserved IP addresses should be assigned to servers or PCs on your network that require non-changing IP addresses. When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time it accesses the router’s DHCP server, in addition to receiving other DHCP-assigned configuration information.

From the Main Menu of the browser interface, under Advanced, click on Reserve IP to view the Reserve IP menu, shown in [Figure 8-8](#).

Reserve IP

#	IP Address	MAC Address	Device Name
1	192.168.0.111	66-22-33-44-55-11	test

**Figure 8-8. Reserve IP menu**

To reserve an IP address:

1. Click the Add button.
2. In the IP Address box, type the IP address to assign to the PC or server.  
(choose an IP address from the router's LAN subnet, such as 192.168.0.X)
3. Type the MAC Address of the PC or server.  
(Tip: If the PC is already present on your network, you can copy its MAC address from the Attached Devices menu and paste it here.)
4. Click Apply to enter the reserved address into the table.

Note: The reserved address will not be assigned until the next time the PC contacts the router's DHCP server. Reboot the PC or access its IP configuration and force a DHCP release and renew.

To edit or delete a reserved address entry:

1. Click the button next to the reserved address you want to edit or delete.
2. Click Edit or Delete.



## Remote Management

Using the Remote Management menu, you can allow a user or users on the Internet to configure, upgrade and check the status of your router.



**Note:** Be sure to change the router's default password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper and lower case), numbers, and symbols. Your password can be up to 30 characters.

From the Main Menu of the browser interface, under Advanced, click on Remote Management to view the Remote Management menu, shown in [Figure 8-9](#).

**Remote Management**

---

**Allow Remote Management**

Start IP address     .  .  .

End IP address      .  .  .

Port                

---

**Figure 8-9. Remote Management menu**

To configure your router for Remote Management:

1. Select the Allow Remote Management check box.
2. Specify what external addresses will be allowed to access the router's remote management by entering a beginning and ending IP address to define the allowed range.

*For security, NETGEAR recommends that you restrict access to as few external IP addresses as practical.*

3. Specify the Port Number that will be used for accessing the management interface.

Web browser access normally uses the standard HTTP service port 80. For greater security, you can change the remote management web interface to a custom port by entering that number in the box provided. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

4. Click Apply to have your changes take effect.

When accessing your router from the Internet, you will type your router's WAN IP address into your browser's Address (in IE) or Location (in Netscape) box, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, enter in your browser:

```
http://134.177.0.123:8080
```

---

# Chapter 9

## Troubleshooting

This chapter gives information about troubleshooting your Model HR314 802.11a Hi-Speed Wireless Router. For the common problems listed, go to the section indicated.

Is the router on?

Have I connected the router correctly?

Go to [“Basic Functioning“](#) on page 9-1.

I can't access the router's configuration with my browser.

Go to [“Troubleshooting the Web Configuration Interface“](#) on page 9-3.

I've configured the router but I can't access the Internet.

Go to [“Troubleshooting the ISP Connection“](#) on page 9-4.

I can't remember the router's configuration password.

I want to clear the configuration and start over again.

Go to [“Using the Default Reset Button to Restore the Factory Configuration and Password“](#) on page 9-7.

### Basic Functioning

---

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

1. When power is first applied, verify that the Power LED is on.
2. Verify that the Test LED lights within a few seconds, indicating that the self-test procedure is running.
3. After approximately 10 seconds, verify that:

- a. The Test LED is not lit.
- b. The Local port LEDs are lit for any local ports that are connected.
- c. The Internet port LED is lit.

If a port's LED is lit, a link has been established to the connected device. If a Local port is connected to a 100 Mbps device, verify that the port's LED is green. If the port is 10 Mbps, the LED will be amber.

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

## Power LED Not On

If the Power 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 12VDC 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 Turns On or Test LED Stays On

When the router is turned on, the Test LED turns on for about 10 seconds and then turns off. If the Test LED does not turn on, or if it 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 all LEDs including the Test LED are still on one minute after power up:

- Cycle the power to see if the router recovers.
- Clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.0.1. This procedure is explained in [“Using the Default Reset Button to Restore the Factory Configuration and Password” on page 9-7.](#)

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

## LAN or Internet Port LEDs Not On

If either the LAN LEDs or Internet LED do 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 Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could 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 the 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 192.168.0.254. Refer to [“Verifying TCP/IP Properties“ on page 3-5](#) or [“Verifying Macintosh TCP/IP Properties“ on page 3-7](#) to find your PC's IP address. Follow the instructions in [Chapter 3](#) to configure your PC.

**Note:** If your PC's IP address is shown as 169.254.x.x:

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 connection from the PC to the router and reboot your PC.

- 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. This procedure is explained in [“Using the Default Reset Button to Restore the Factory Configuration and Password“ on page 9-7](#).
- 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.

- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

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. You may need to clear the browser's temporary or cached files.

## 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 the Web Configuration Manager.

To check the WAN IP address:

1. Launch your browser and select an external site such as [www.netgear.com](http://www.netgear.com)
2. Access the Main Menu of the router's configuration at <http://192.168.0.1>
3. Under the Maintenance heading, select Router Status
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.

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 some other type of login.
- If your ISP requires a login, 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 as the Account Name in the Basic Settings menu.
- Your ISP only allows one Ethernet MAC address to connect to Internet, and may check for your PC's MAC address. In this case:  
  
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 the Basic Settings menu. Refer to [“Manual Configuration” on page 4-8](#).

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” on page 3-5](#). 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” on page 3-5](#).

## 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 in your PC or workstation.

## Testing the LAN Path to Your Firewall

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 port LED is on. If the LED is off, follow the instructions in [“LAN or Internet Port LEDs Not On”](#) on [page 9-3](#).
  - 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 <IP address>
```



where *<IP address>* is 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 your PC's Network Control Panel. Verify that the IP address of the router is listed as the default gateway as described in [“Verifying TCP/IP Properties“ on page 3-5](#).
- 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 that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your PC, enter that host name as the Account Name in the Basic Settings menu.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many 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 your router to “clone” or “spoof” the MAC address from the authorized PC. Refer to [“Manual Configuration“ on page 4-8](#).

## Using the Default Reset Button to Restore the Factory Configuration and Password

---

This section explains how to restore the factory default configuration settings, changing the router's administration password to **password** and the IP address to 192.168.0.1. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the Web Configuration Manager (see [“Erase the Configuration“ on page 6-5](#)).
- Use the Default Reset button on the rear panel of the router. Use this method for cases when the administration password or IP address is not known.

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

1. Press and hold the Default Reset button until the Test LED turns on (about 10 seconds).
2. Release the Default Reset button and wait for the router to reboot.

## Problems with Date and Time

---

The E-Mail menu in the Content Filtering section displays the current date and time of day. The HR314 uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000  
Cause: The router has not yet successfully reached a Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the router, wait at least five minutes and check the date and time again.
- Time is off by one hour  
Cause: The router does not automatically sense Daylight Savings Time. In the E-Mail menu, check or uncheck the box marked “Adjust for Daylight Savings Time”.

# Appendix A

## Technical Specifications

This appendix provides technical specifications for the Model HR314 802.11a Hi-Speed Wireless Router.

### Network Protocol and Standards Compatibility

Data and Routing Protocols: TCP/IP, RIP-1, RIP-2, DHCP  
PPP over Ethernet (PPPoE)

### Wireless Protocol and Standards Compatibility

Wireless Standard	IEEE 802.11a
Radio Data Rate	Normal Mode: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel Turbo Mode: 12, 18, 24, 36, 48, 72 Mbps per channel
Frequency	5.15 ~ 5.25 GHz (lower band) for US/Canada, Japan 5.25 ~ 5.35 GHz (middle band) for US/Canada
Encryption	40-bit (also called 64-bit), 128-bit or 152-bit WEP data encryption
Maximum Clients	Limited by the amount of wireless network traffic generated by each node; typically 30 to 70 nodes

### 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 @ 1.5A output, 35W maximum

### **Physical Specifications**

Dimensions:	253 by 181 by 35 mm 9.95 by 7.1 by 1.4 in.
Weight:	1.2 kg 2.6 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, routing, and firewalls.

### 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 HR314 802.11a Hi-Speed Wireless 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 HR314 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](http://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
```

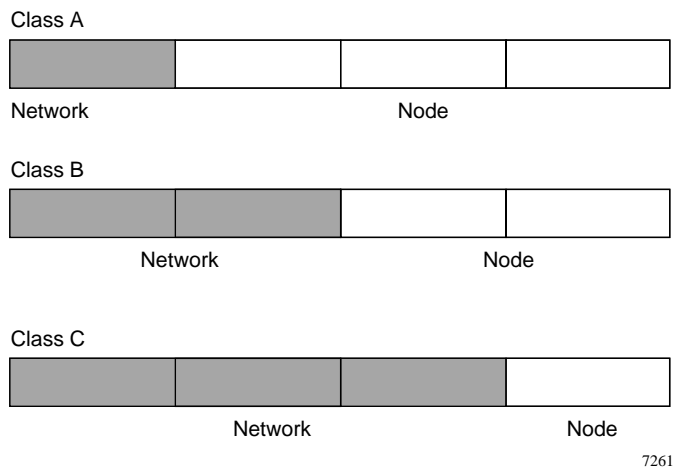
is normally written as:

```
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 192.68.135.126, 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 HR314 is preconfigured to automatically assign private addresses.

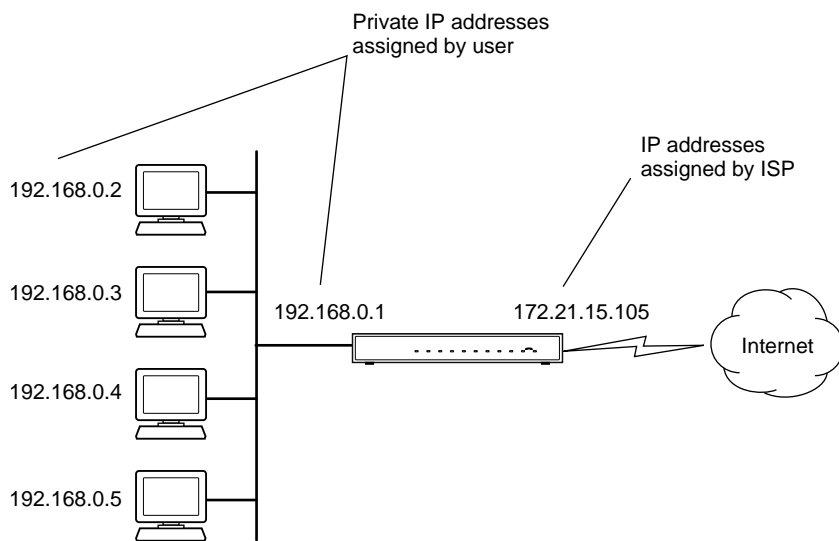
Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines explained here. For more information about address assignment, refer to RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*. The Internet Engineering Task Force (IETF) publishes RFCs on its Web site at [www.ietf.org](http://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 HR314 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.



7786EA

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

This scheme offers the additional benefit of simple 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.

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)*.

## 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 HR314 has the capacity to act as a DHCP server.

The HR314 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.

## Wireless Networking

---

The Model HR314 802.11a Hi-Speed Wireless Router conforms to the Institute of Electrical and Electronics Engineers (IEEE) 802.11a standard for wireless LANs (WLANs). On an 802.11a wireless link, data is encoded using direct-sequence spread-spectrum (DSSS) technology and is transmitted in the unlicensed radio spectrum at 5GHz. The maximum data rate for the wireless link is 72 Mbps, but it will automatically back down to 6 Mbps when the radio signal is weak or when interference is detected.

The 802.11a standard is also called Wireless Ethernet or Wi-Fi5 by the Wireless Ethernet Compatibility Alliance (WECA, see <http://www.wi-fi.net>), an industry standard group promoting interoperability among 802.11 devices.

## Wireless Network Configuration

The 802.11a standard offers two methods for configuring a wireless network - ad hoc and infrastructure.

## **Ad-hoc Mode (Peer-to-Peer Workgroup)**

In an ad hoc network, computers are brought together as needed; thus, there is no structure or fixed points to the network - each node can generally communicate with any other node. There is no Access Point involved in this configuration. This mode enables you to quickly set up a small wireless workgroup and allows workgroup members to exchange data or share printers as supported by Microsoft Networking in the various Windows operating systems. Some vendors also refer to ad hoc networking as Peer-to-Peer group networking.

In this configuration, network packets are directly sent and received by the intended transmitting and receiving stations. As long as the stations are within range of one another, this is the easiest and least expensive way to set up a wireless network.

## **Infrastructure Mode**

With a wireless Access Point, you can operate the wireless LAN in the infrastructure mode. This mode provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage, interacting with wireless nodes via an antenna.

In the infrastructure mode, the wireless access point converts airwave data into wired Ethernet data, acting as a bridge between the wired LAN and wireless clients. Connecting multiple Access Points via a wired Ethernet backbone can further extend the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one Access Point domain to another and still maintain seamless network connection.

## **Extended Service Set Identification (ESSID)**

The Extended Service Set Identification (ESSID) is one of two types of Service Set Identification (SSID). In an ad-hoc wireless network with no access points, the Basic Service Set Identification (BSSID) is used. In an infrastructure wireless network that includes an access point, the Extended Service Set Identification (ESSID) is used, but may still be referred to as SSID.

An SSID is a thirty-two character (maximum) alphanumeric key identifying the wireless local area network. Some vendors refer to the SSID as network name. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.

## Authentication and WEP Encryption

The absence of a physical connection between nodes makes the wireless links vulnerable to eavesdropping and information theft. To provide a certain level of security, the IEEE 802.11 standard has defined two types of authentication methods, Open System and Shared Key. With Open System authentication, a wireless PC can join any network and receive any messages that are not encrypted. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network. By default, IEEE 802.11 wireless devices operate in an Open System network.

Wired Equivalent Privacy (WEP) data encryption is utilized when the wireless nodes or access points are configured to operate in Shared Key authentication mode. There are three shared key methods implemented in NETGEAR's 802.11a solutions: the standard based 40-bit WEP data encryption and 128-bit WEP data encryption plus the extended 152-bit WEP data encryption.

The 64-bit WEP data encryption method, allows for a five-character (40-bit) input. Additionally, 24 factory-set bits are added to the forty-bit input to generate a 64-bit encryption key. (The 24 factory-set bits are not user-configurable). This encryption key will be used to encrypt/decrypt all data transmitted via the wireless interface. Some vendors refer to the 64-bit WEP data encryption as 40-bit WEP data encryption since the user-configurable portion of the encryption key is 40 bits wide.

The 128-bit WEP data encryption method consists of 104 configurable bits and the 152-bit WEP data encryption method consists of 128 configurable bits. Similar to the forty-bit WEP data encryption method, the remaining 24 bits are factory set and not user configurable. Some vendors allow passphrases to be entered instead of the cryptic hexadecimal characters to ease encryption key entry.

Figure B-3 shows examples of key sizes and content for the different WEP methods:

**Table B-3. WEP Key Sizes and Content**

Encryption Key Size	# of Hexadecimal Digits	Example of Hexadecimal Key Content
64-bit (24+40)	10	4C72F08AE1
128-bit (24+104)	26	4C72F08AE19D57A3FF6B260037
152-bit (24+128)	32	4C72F08AE19D57A3FF6B26003715DAC2



## Wireless Channel Selection

IEEE 802.11a utilizes 300 MHz of bandwidth in the 5 GHz Unlicensed National Information Infrastructure (U-NII) band. Though the lower 200 MHz is physically contiguous, the FCC has divided the total 300 MHz into three distinct domains, each with a different legal maximum power output.

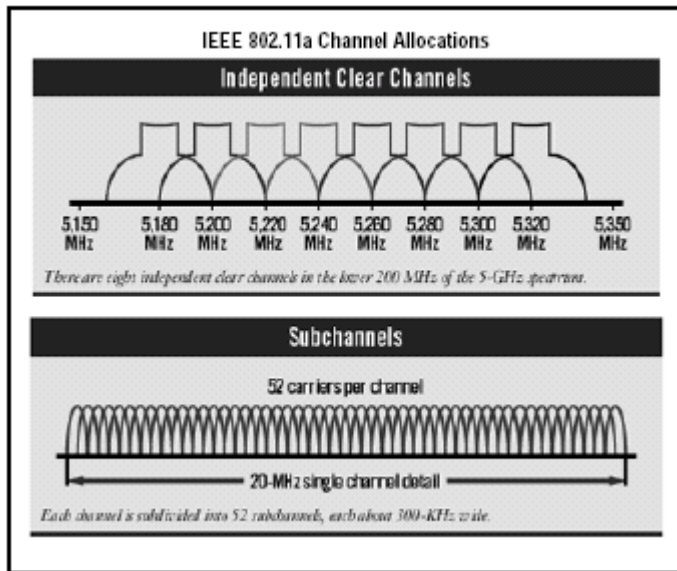
The radio frequency channels used are listed in [Table B-4](#):

**Table B-4. 802.11a Wireless Channels**

U-NII Band	Low	Middle	High
Frequency (GHz)	5.15 – 5.25	5.25 – 5.35	5.725 – 5.825
Max. Power Output	50 mW	250 mW	1W

**Note:** The high band is not supported in the Model HR314 802.11a Hi-Speed Wireless Router.

IEEE 802.11a uses Orthogonal Frequency Division Multiplexing (OFDM), a new encoding scheme that offers certain benefits over a spread spectrum in channel availability and data rate. The 802.11a uses OFDM to define a total of 8 non-overlapping 200 MHz channels across the 2 lower bands; each of these is divided into 52 subcarriers and each carrier is approximately 300 KHz wide. By comparison, 802.11b uses only 3 non-overlapping channels.



The Model HR314 user can use eight channels in non-turbo mode.

TURBO MODE: OFF	
Channel	Frequency
36	5.18 GHz
40	5.20 GHz
44	5.22 GHz
48	5.24 GHz
52	5.26 GHz
56	5.28 GHz
60	5.30 GHz
64	5.32 GHz

The Model HR314 user can use three channels in turbo mode:

TURBO MODE: ON	
Channel	Frequency
42	5.21 GHz
50	5.25 GHz
58	5.29 GHz

**Note:** The available channels supported by the wireless products in various countries are different.

## 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-5](#).

**Table B-5. 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 two 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.

## 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" or "Cat V", 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

<b>10BASE-T</b>	IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.
<b>100BASE-Tx</b>	IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.
<b>802.11a</b>	IEEE specification for wireless networking at 54 Mbps and higher using Orthogonal Frequency Division Multiplexing (OFDM), a new encoding scheme that offers benefits over spread spectrum compared with 802.11b. 802.11a operates in the 5 GHz Unlicensed National Information Infrastructure (U-NII) band.
<b>Denial of Service attack</b>	DoS. A hacker attack designed to prevent your computer or network from operating or communicating.
<b>DHCP</b>	<i>See</i> Dynamic Host Configuration Protocol.
<b>DNS</b>	<i>See</i> Domain Name Server.
<b>domain name</b>	A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, etc. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.
<b>Domain Name Server</b>	A Domain Name Server (DNS) resolves descriptive names of network resources (such as www.NETGEAR.com) to numeric IP addresses.
<b>Dynamic Host Configuration Protocol</b>	DHCP. An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.
<b>ESSID</b>	The Extended Service Set Identification (ESS ID) is a thirty-two character (maximum) alphanumeric key identifying the wireless local area network.

<b>Gateway</b>	A local device, usually a router, that connects hosts on a local network to other networks.
<b>IP</b>	<i>See</i> Internet Protocol.
<b>IP Address</b>	A four-byte number uniquely defining each host on the Internet. Ranges of addresses are assigned by Internic, an organization formed for this purpose. Usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57).
<b>IPSec</b>	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.
<b>ISP</b>	Internet service provider.
<b>Internet Protocol</b>	The main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.
<b>LAN</b>	<i>See</i> local area network.
<b>local area network</b>	LAN. A communications network serving users within a limited area, such as one floor of a building. A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers.
<b>MAC address</b>	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.
<b>Mbps</b>	Megabits per second.
<b>MSB</b>	<i>See</i> Most Significant Bit or Most Significant Byte.
<b>MRU</b>	<i>See</i> Maximum Receive Unit.
<b>Maximum Receive Unit</b>	The size in bytes of the largest packet that can be sent or received.
<b>Most Significant Bit or Most Significant Byte</b>	The portion of a number, address, or field that is farthest left when written as a single number in conventional hexadecimal ordinary notation. The part of the number having the most value.
<b>NAT</b>	<i>See</i> Network Address Translation.

<b>netmask</b>	A number that explains which part of an IP address comprises the network address and which part is the host address on that network. It can be expressed in dotted-decimal notation or as a number appended to the IP address. For example, a 28-bit mask starting from the MSB can be shown as 255.255.255.192 or as /28 appended to the IP address.
<b>Network Address Translation</b>	A technique by which several hosts share a single IP address for access to the Internet.
<b>packet</b>	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.
<b>PPP</b>	<i>See</i> Point-to-Point Protocol.
<b>PPP over Ethernet</b>	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.
<b>PPTP</b>	Point-to-Point Tunneling Protocol. A method for establishing a virtual private network (VPN) by embedding Microsoft's network protocol into Internet packets.
<b>PSTN</b>	Public Switched Telephone Network.
<b>Point-to-Point Protocol</b>	PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.
<b>RFC</b>	Request For Comment. Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFCs can be found at <a href="http://www.ietf.org">www.ietf.org</a> .
<b>RIP</b>	<i>See</i> Routing Information Protocol.
<b>router</b>	A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.
<b>Routing Information Protocol</b>	A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.
<b>SSID</b>	Service Set Identification. A thirty-two character (maximum) alphanumeric key identifying the wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.
<b>subnet mask</b>	<i>See</i> netmask.

<b>UTP</b>	Unshielded twisted pair. The cable used by 10BASE-T and 100BASE-Tx Ethernet networks.
<b>VPN</b>	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.
<b>WAN</b>	<i>See</i> wide area network.
<b>WEP</b>	Wired Equivalent Privacy. WEP is a data encryption protocol for 802.11b wireless networks. All wireless nodes and access points on the network are configured with a 64-bit or 128-bit Shared Key for data encryption.
<b>wide area network</b>	WAN. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.
<b>Wi-Fi</b>	<i>See</i> 802.11b. A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see <a href="http://www.wi-fi.net">http://www.wi-fi.net</a> ), an industry standard group promoting interoperability among 802.11b devices.
<b>Windows Internet Naming Service</b>	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.
<b>WINS</b>	<i>See</i> Windows Internet Naming Service.



## Numerics

802.11a B-10

## A

Account Name 4-5, 4-7, 4-8

Address Resolution Protocol B-9

ad-hoc mode B-11

antenna orientation 2-5

## B

backup configuration 7-6

Beacon Interval 5-4

BSSID B-11

## C

cables, pinout B-15

Cabling B-15

Cat5 cable 2-4, 2-5, B-16

Channel B-13

Channel/Frequency 5-3

configuration

    automatic by DHCP 1-5

    backup 7-6

    erasing 7-6

    restore 7-5

    router, initial 4-1

connections

    verifying 2-6

content filtering 1-4, 6-1

conventions

    typography xvi

crossover cable 9-3, B-16

customer support iv

## D

Data Rate 5-3

date and time 9-8

Daylight Savings Time 9-8

daylight savings time 6-3

DHCP 1-5, 8-7, B-10

DHCP Client ID 3-7

DHCP Setup field, Ethernet Setup menu 7-2

DMZ 1-4, 8-2, 8-5

DNS Proxy 1-5

DNS server 3-11, 4-5, 4-6, 4-8, 4-9

DNS, dynamic 8-6

domain 3-11

Domain Name 4-5, 4-7, 4-8

domain name server (DNS) B-9

DTIM 5-4

Dynamic DNS 8-6

## E

End Port 8-3

EnterNet 3-9

erase configuration 7-6

ESSID B-11

Ethernet cable B-15

## F

factory settings, restoring 7-6

features 1-2

Flash memory, for firmware upgrade 1-3

front panel 2-2

## G

gateway address 3-10, 3-11

## H

Half Life 8-4

host name 4-5, 4-7, 4-8

## I

IANA

contacting B-2

IETF xv

Web site address B-7

infrastructure mode B-11

installation 1-5

Internet account

address information 3-9

establishing 3-9

IP addresses 3-10, 3-11

and NAT B-8

and the Internet B-2

assigning B-2, B-9

auto-generated 9-3

private B-7

translating B-9

IP configuration by DHCP B-10

IP networking

for Macintosh 3-6

for Windows 3-2, 3-5

## K

KALI 8-4

## L

LAN IP Setup Menu 8-7

LEDs

description 2-2

troubleshooting 9-3

log

sending 6-2

log entries 6-6

## M

MAC address 9-7, B-9

spoofing 4-6, 4-9, 9-5

Macintosh 3-10

DHCP Client ID 3-7

Obtaining ISP Configuration Information 3-11

MDI/MDI-X wiring B-16

metric 8-10

## N

NAT. *See* Network Address Translation

NETGEAR

contacting xv

netmask

translation table B-6

Network Address Translation 1-5, B-8

Network Time Protocol 6-3, 9-8

NTP 6-3, 9-8

## O

OFDM B-13

Open System authentication B-12

## P

package contents 2-1

Passphrase 5-6

passphrase 1-3

password

restoring 9-7

PC, using to configure 3-11

ping 8-5

pinout, Ethernet cable B-15

placement 5-2

Port Forwarding 8-2

port forwarding behind NAT B-9

- Port Forwarding Menu 8-2
- PPP over Ethernet 1-3, 1-5, 3-9
- PPPoE 1-3, 1-5, 3-9, 4-7
- Primary DNS Server 4-5, 4-6, 4-8, 4-9
- protocols
  - Address Resolution B-9
  - DHCP 1-5, B-10
  - Routing Information 1-5, B-2
  - support 1-3
- publications, related xv

## Q

- Quake 8-4

## R

- range 2-3, 5-2
- range, port forwarding 8-3
- rear panel 2-3
- requirements
  - access device 2-4
  - hardware 2-4
- restore configuration 7-5
- restore factory settings 7-6
- RFC
  - 1466 B-7, B-9
  - 1597 B-7, B-9
  - 1631 B-8, B-9
  - finding B-7
- RIP (Router Information Protocol) 8-8
- router concepts B-1
- Routing Information Protocol 1-5, B-2

## S

- Secondary DNS Server 4-5, 4-6, 4-8, 4-9
- security 1-2, 1-4
- Setup Wizard 4-1
- Shared Key authentication 1-4, B-12
- SMTP 6-2
- spoof MAC address 9-5

- SSID 2-6, 5-1, 5-3, B-11
- Start Port 8-3
- Static Routes 8-9
- subnet addressing B-5
- subnet mask 3-10, 3-11, B-5

## T

- TCP/IP
  - configuring 3-1
  - network, troubleshooting 9-5
- TCP/IP properties
  - verifying for Macintosh 3-7
  - verifying for Windows 3-5, 3-6
- technical support xv
- time of day 9-8
- time zone 6-3
- time-stamping 6-3
- Transmit Power 5-4
- troubleshooting 9-1
- Trusted Host 6-5
- Turbo Mode 5-3
- typographical conventions xvi

## U

- uplink switch B-16
- USB 3-9

## W

- WEP 1-3, B-12
- Wi-Fi5 B-10
- Windows, configuring for IP routing 3-2, 3-5
- winiptcfg utility 3-5
- WinPOET 3-9
- Wired Equivalent Privacy. *See* WEP
- Wireless Ethernet B-10
- World Wide Web iv