

# Reference Manual for the Wireless Cable Modem Gateway CG814WG v2



## **NETGEAR**

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

202-10074-01  
January 2005

© 2005 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.

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

This is to certify that the CG814WG v2 Wireless Cable Modem Gateway 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 CG814WG v2 Wireless Cable Modem Gateway 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 CG814WG v2 Wireless Cable Modem Gateway 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.

## Technical Support

Thank you for choosing Netgear product(s). Please register online and take advantage of the technical support resources such as Netgear online knowledge base. Technical support is available twenty-four hours a day, seven days a week; please call your Cable Internet Service Provider.

## Product and Publication Details

<b>Model Number:</b>	CG814WG v2
<b>Publication Date:</b>	January 2005
<b>Product Family:</b>	firewall
<b>Product Name:</b>	CG814WG v2 Wireless Cable Modem Gateway
<b>Home or Business Product:</b>	Insert value by editing user variable Target Market
<b>Language:</b>	English



# Contents

<b>Chapter 1</b>	
<b>About This Manual</b> .....	<b>1-1</b>
Audience, Conventions, Publication Date .....	1-1
<b>Chapter 2</b>	
<b>Introduction</b> .....	<b>2-1</b>
About the CG814WG v2 .....	2-1
Key Features .....	2-1
Built-in Cable Modem .....	2-1
A Powerful, True Firewall .....	2-1
Content Filtering .....	2-2
802.11b and 802.11g Standards-based Wireless Networking .....	2-2
Configurable Auto Uplink™ Ethernet Connection .....	2-2
USB Port .....	2-3
Protocol Support .....	2-3
Easy Installation and Management .....	2-3
What's in the Box? .....	2-4
The Gateway's Front Panel .....	2-4
The Gateway's Rear Panel .....	2-6
<b>Chapter 3</b>	
<b>Connecting the Gateway to the Internet</b> .....	<b>3-1</b>
What You Will Need Before You Begin .....	3-1
Hardware Requirements .....	3-1
LAN Configuration Requirements .....	3-1
Internet Configuration Requirements .....	3-2
Connecting the CG814WG v2 Gateway .....	3-2
<b>Chapter 4</b>	
<b>Wireless Configuration</b> .....	<b>4-1</b>
Considerations For A Wireless Network .....	4-1
Implement Appropriate Security .....	4-1

Observe Placement and Range Guidelines .....	4-2
Configuring Wireless Settings .....	4-3
Wireless Network Settings .....	4-4
Wireless Access Point .....	4-4
Restricting Wireless Access by MAC Address .....	4-4
Configuring Wired Equivalent Privacy (WEP) .....	4-6
<b>Chapter 5</b>	
<b>Protecting Your Network .....</b>	<b>5-1</b>
Protecting Access to Your CG814WG v2 Gateway .....	5-1
Blocking Keywords, Sites, and Services .....	5-2
Blocking Keywords and Domains .....	5-3
Using MAC Filtering .....	5-4
Blocking Access by Time of Day .....	5-6
Using Port Blocking .....	5-6
Port Forwarding .....	5-7
Using Port Triggering .....	5-9
Setting Up A Default DMZ Host .....	5-10
Respond to Ping on Internet WAN Port .....	5-11
Enabling or Disabling Content Filtering Services .....	5-11
<b>Chapter 6</b>	
<b>Managing Your Network .....</b>	<b>6-1</b>
Network Status Information .....	6-1
Viewing Gateway Status .....	6-1
Connection Status .....	6-3
Configuring LAN IP Settings .....	6-4
LAN IP Setup .....	6-4
Using the Gateway as a DHCP Server .....	6-5
Viewing and Emailing Logged Information .....	6-6
Enabling Logs Event E-mail Notification .....	6-6
Erasing Configuration .....	6-7
Running Diagnostic Utilities .....	6-8
Enabling Remote Management Access .....	6-9
Enabling Remote Management Access After a Reset .....	6-9

<b>Chapter 7</b>	
<b>Troubleshooting</b>	<b>7-1</b>
Basic Functions	7-1
Power LED Not On	7-2
All LEDs Stay On	7-2
Local Link LEDs Not On	7-2
Cable Link LED Not On	7-2
Troubleshooting the Web Configuration Interface	7-3
Troubleshooting the ISP Connection	7-4
Troubleshooting a TCP/IP Network Using a Ping Utility	7-4
Testing the LAN Path to Your Gateway	7-4
Testing the Path from Your PC to a Remote Device	7-5
<b>Appendix A</b>	
<b>Technical Specifications</b>	<b>A-1</b>
<b>Appendix B</b>	
<b>Networks, Routing, and Firewall Basics</b>	<b>B-1</b>
Related Publications	B-1
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-4
Private IP Addresses	B-7
Single IP Address Operation Using NAT	B-7
MAC Addresses and Address Resolution Protocol	B-8
Related Documents	B-9
Domain Name Server	B-9
IP Configuration by DHCP	B-10
Internet Security and Firewalls	B-10
What is a Firewall?	B-10
Stateful Packet Inspection	B-11
Denial of Service Attack	B-11
Wireless Networking Overview	B-11
Infrastructure Mode	B-11

Ad Hoc Mode (Peer-to-Peer Workgroup) .....	B-12
Network Name: Extended Service Set Identification (ESSID) .....	B-12
Authentication and WEP .....	B-13
802.11b Authentication .....	B-13
Open System Authentication .....	B-14
Shared Key Authentication .....	B-14
Overview of WEP Parameters .....	B-15
Key Size .....	B-16
WEP Configuration Options .....	B-16
Wireless Channels .....	B-17
Ethernet Cabling .....	B-18
Uplink Switches and Crossover Cables .....	B-19
Cable Quality .....	B-19

## **Appendix C**

<b>Preparing Your Network to Work with a Router .....</b>	<b>C-1</b>
What You Need To Use a Router with a Broadband Modem .....	C-1
Cabling and Computer Hardware .....	C-1
Computer Network Configuration Requirements .....	C-1
Internet Configuration Requirements .....	C-2
Where Do I Get the Internet Configuration Parameters? .....	C-2
Record Your Internet Connection Information .....	C-3
Preparing Your Computers for TCP/IP Networking .....	C-4
Configuring Windows 95, 98, and Me for TCP/IP Networking .....	C-5
Installing or Verifying Windows Networking Components .....	C-5
Enabling DHCP to Automatically Configure TCP/IP Settings in Windows 95B, 98, and Me .....	C-6
Selecting the Windows' Internet Access Method .....	C-8
Verifying TCP/IP Properties .....	C-8
Configuring Windows NT4, 2000 or XP for IP Networking .....	C-9
Installing or Verifying Windows Networking Components .....	C-9
Configuring DHCP of TCP/IP in Windows XP, 2000, or NT4 .....	C-10
DHCP Configuration of TCP/IP in Windows XP .....	C-10
DHCP Configuration of TCP/IP in Windows 2000 .....	C-12
DHCP Configuration of TCP/IP in Windows NT4 .....	C-14
Verifying TCP/IP Properties for Windows XP, 2000, and NT4 .....	C-15
Configuring the Macintosh for TCP/IP Networking .....	C-16

MacOS 8.6 or 9.x .....	C-16
MacOS X .....	C-16
Verifying TCP/IP Properties for Macintosh Computers .....	C-17
Verifying the Readiness of Your Internet Account .....	C-17
Are Login Protocols Used? .....	C-18
What Is Your Configuration Information? .....	C-18
Obtaining ISP Configuration Information for Windows Computers .....	C-19
Obtaining ISP Configuration Information for Macintosh Computers .....	C-20
Restarting the Network .....	C-20
<b>Appendix D</b>	
<b>Wireless Networking Basics .....</b>	<b>D-1</b>
Wireless Networking Overview .....	D-1
Infrastructure Mode .....	D-1
Ad Hoc Mode (Peer-to-Peer Workgroup) .....	D-2
Network Name: Extended Service Set Identification (ESSID) .....	D-2
Wireless Channels .....	D-2
WEP Wireless Security .....	D-4
WEP Authentication .....	D-4
WEP Open System Authentication .....	D-5
WEP Shared Key Authentication .....	D-6
How to Use WEP Parameters .....	D-8
WPA Wireless Security .....	D-8
How Does WPA Compare to WEP? .....	D-9
How Does WPA Compare to IEEE 802.11i? .....	D-10
What are the Key Features of WPA Security? .....	D-10
Is WPA Perfect? .....	D-16
Product Support for WPA .....	D-16
<b>Glossary.....</b>	<b>G-1</b>



# Chapter 1

## About This Manual

Congratulations on your purchase of the CG814WG v2 Wireless Cable Modem Gateway. The CG814WG v2 provides connection for multiple personal computers to the Internet. It connects directly to your cable line using an embedded DOCSIS 2.0 cable modem.

### Audience, Conventions, Publication Date

This reference manual assumes that the reader has basic-to-intermediate computer and Internet skills. However, basic computer network, Internet, firewall, and networking technology tutorial information is provided in the Appendices.

This guide uses the following typographical conventions:

**Table 1-1. Typographical conventions**

<i>italics</i>	Emphasis, books, CDs, URL names
<b>bold time</b>	User input
<code>courier font</code>	Screen text, file and server names, extensions, commands, IP addresses

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.
---	--

This manual is written f according to these specifications.:

**Table 1-2. Firmware Version and Manual Publication Date**

<i>Firmware Version</i>	2.95r09
Manual Publication Date	January 2005

## How to Print this Manual

---

To print this manual you can choose one of the following several options, according to your needs.

- **Printing a Chapter.** Use the [PDF of This Chapter](#) link at the top right of any page.
  - Click “PDF of This Chapter” link at the top right of any page in the chapter you want to print. A new browser window opens showing the PDF version of the chapter you were viewing.
  - Click the print icon in the upper left of the window.
  - **Tip:** If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.
- **Printing the Full Manual.** Use the PDF button in the toolbar at the top right of the browser window.
  - Click PDF button. A new browser window opens showing the PDF version of the chapter you were viewing.
  - Click the print icon in the upper left of the window.
  - **Tip:** If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

## Chapter 2 Introduction

This chapter describes the features of the NETGEAR CG814WG v2 Wireless Cable Modem Gateway.

### About the CG814WG v2

---

The NETGEAR CG814WG v2 Wireless Cable Modem Gateway connects directly to the wide area network (WAN) using its built-in cable modem. It has multiple options to connect to your local area network (LAN), including a 4-port 10/100 Mbps Ethernet switch, a USB port and an 802.11b wireless Access Point.

The CG814WG v2 Gateway is a complete security solution that protects your network from attacks and intrusions. Unlike simple Internet sharing routers that rely on Network Address Translation (NAT) for security, the CG814WG v2 uses Stateful Packet Inspection for Denial of Service (DoS) attack protection and intrusion detection. The CG814WG v2 provides highly reliable Internet access for up to 253 users.

### Key Features

---

The CG814WG v2 offers the following features.

#### Built-in Cable Modem

The CG814WG v2 Gateway connects directly the WAN using an integrated cable modem. The modem is DOCSIS 2.0, guaranteeing that it will work with your local cable service provider.

#### A Powerful, True Firewall

Unlike simple Internet sharing NAT routers, the CG814WG v2 is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- Denial of Service (DoS) protection  
Automatically detects and thwarts Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND Attack and IP Spoofing.
- Configurable Port Forwarding, Port Blocking, Port Triggering and DMZ provide enough flexibility for most applications.
- Blocks access from your LAN to Internet locations or services that you specify as off-limits.
- Logs security incidents  
The CG814WG v2 will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the gateway to email the log to you whenever a significant event occurs.

## Content Filtering

With its content filtering feature, the CG814WG v2 prevents objectionable content from reaching your PCs. The gateway allows you to control access to Internet content by screening for keywords within Web addresses.

Dual login allows an adult to configure content filtering, while still allowing a child to configure other features of the gateway.

## 802.11b and 802.11g Standards-based Wireless Networking

The CG814WG v2 Gateway includes an 802.11g- and 802.11b-compliant wireless access point, providing continuous, high-speed 54 Mbps access between your wireless and Ethernet devices. The access point provides:

- 802.11g Standards-based wireless networking at up to 54Mbps
- 64-bit and 128-bit WEP encryption security
- WEP keys can be generated manually or by passphrase
- Wireless access can be restricted by MAC address.

## Configurable Auto Uplink™ Ethernet Connection

With its internal 4-port 10/100 switch, the CG814WG v2 can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. Both the local LAN and the Internet WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

The gateway incorporates Auto Uplink™ technology. Each LOCAL Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a ‘normal’ connection such as to a PC or an ‘uplink’ connection such as 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, as Auto Uplink will accommodate either type of cable to make the right connection.

## USB Port

A USB connection for your computer eliminates the need for installing an Ethernet card.

## Protocol Support

The CG814WG v2 supports the Transmission Control Protocol/Internet Protocol (TCP/IP). [Appendix B, "Networks, Routing, and Firewall Basics"](#) provides further information on TCP/IP.

- **IP Address Sharing by NAT**  
The CG814WG v2 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 CG814WG v2 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.

## Easy Installation and Management

You can install, configure, and operate the CG814WG v2 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 gateway 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.

- Diagnostic functions  
The gateway incorporates built-in diagnostic functions such as Ping, DNS lookup, and remote reboot. These functions allow you to test Internet connectivity and reboot the gateway. You can use these diagnostic functions directly from the CG814WG v2 when you are connect on the LAN or when you are connected over the Internet via the remote management function.
- Visual monitoring  
The gateway's front panel LEDs provide an easy way to monitor its status and activity.

## What's in the Box?

---

The product package should contain the following items:

- CG814WG v2 Wireless Cable Modem Gateway
- AC power adapter
- Category 5 (CAT5) Ethernet cable
- USB cable
- *Resource CD*, including:
  - This manual
  - Application Notes, Tools, and other helpful information

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

## The Gateway's Front Panel

The front panel of the CG814WG v2 ([Figure 2-1](#)) contains status LEDs.



**Figure 2-1: CG814WG v2 Front Panel**

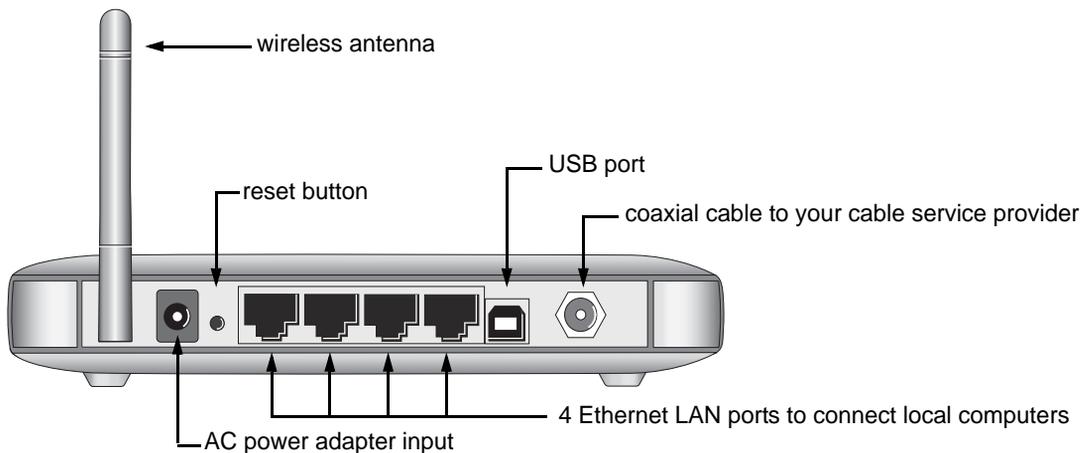
You can use some of the LEDs to verify connections. [Table 2-1](#) lists and describes each LED on the front panel of the CG814WG v2 Gateway. These LEDs are green when lit.

**Table 2-1. LED Descriptions**

Label	Activity	Description
Power 	On Off	Power is supplied to the gateway. Power is not supplied to the gateway.
Cable Link 	On (Green) Off	Configuration of the cable interface by your cable service provider is complete. Configuration of the cable interface is still in progress.
Upload Traffic 	Blink Off	Data is being transmitted to the cable interface. The cable interface is idle.
Download Traffic 	Blink Off	Data is being received from the cable interface. The cable interface is idle.
Wireless 	On Blink	Indicates that the wireless Access Point is operating normally. Data is being transmitted or received on the wireless interface.
Local (Local Area Network) 	On (Green) Blink (Green) On (Yellow) Blink (Yellow) Off	The Local port has detected link with a 100 Mbps device. Data is being transmitted or received at 100 Mbps. The Local port has detected link with a 10 Mbps device. Data is being transmitted or received at 10 Mbps. No link is detected on this port.

## The Gateway's Rear Panel

The rear panel of the CG814WG v2 (Figure 2-2) contains the connections identified below.



**Figure 2-2: CG814WG v2 Rear Panel**

## Chapter 3

# Connecting the Gateway to the Internet

This chapter describes how to set up the CG814WG v2 Gateway on your Local Area Network (LAN), connect to the Internet and perform basic configuration.

### What You Will Need Before You Begin

---

You need to prepare these three things before you can connect your gateway to the Internet:

1. A computer properly connected to the gateway as explained below.
2. Active Data Over Cable Internet service provided by cable modem account.
3. The Internet Service Provider (ISP) configuration information for your cable modem account.

### Hardware Requirements

The CG814WG v2 Gateway connects to your LAN using either its twisted-pair Ethernet, USB or 802.11b or 802.11g wireless port.

To use the CG814WG v2 Gateway on your network, each computer must have either an installed Ethernet Network Interface Card (NIC), USB Host port or 802.11b or 802.11g wireless adapter. If the computer will connect to your network at 100 Mbps, you must use a Category 5 (CAT5) cable such as the one provided with your gateway.

### LAN Configuration Requirements

For the initial connection to the Internet and configuration of your gateway, you will need to connect a computer to the gateway which is set to automatically get its TCP/IP configuration from the gateway via DHCP.

**Note:** Please refer to [Appendix C, “Preparing Your Network”](#) for assistance with DHCP configuration.

## Internet Configuration Requirements

Depending on how your ISP set up your Internet account, you will need one or more of these configuration parameters to connect your gateway to the Internet:

- Host and Domain Names
- ISP Domain Name Server (DNS) Addresses
- Fixed or Static IP Address

## Connecting the CG814WG v2 Gateway

---

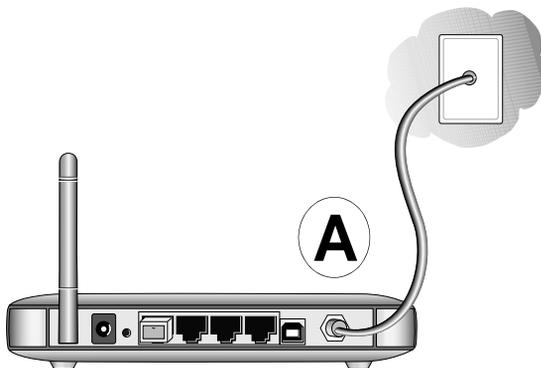
Before using your gateway, you need to do the following:

- Connect to your computer, using either Ethernet, USB or wireless.
- Connect the line from your cable service provider to the cable connector of the gateway.
- Connect the power adapter.

Your computer will attach to either the Ethernet, USB or wireless ports on the CG814WG v2 Gateway.

### 1. Connect the Gateway.

- a. Turn off your computer.
- b. Using the coaxial cable provided by your cable company, connect the CG814WG v2 cable port (A) to your cable line splitter or outlet.



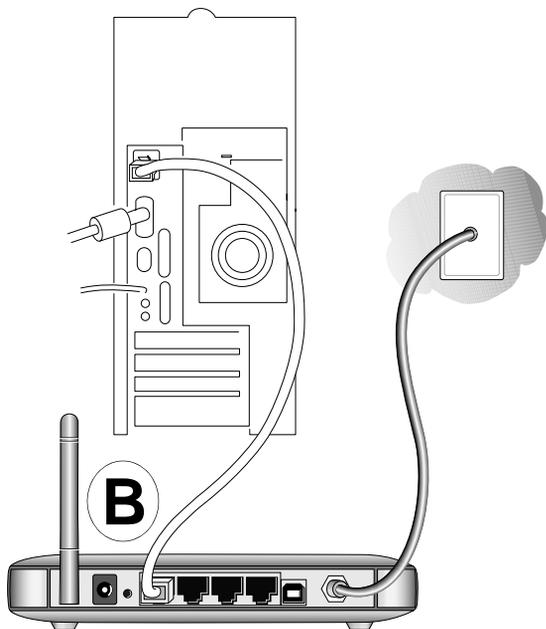
**Figure 3-1: Connect the gateway to the cable network.**

- c. Connect the gateway to you computer.
  - If you will connect with the Ethernet cable, follow the instructions below.
  - If you will connect with the USB cable, skip to step d below.



**Note:** Set up the CG814WG v2 Gateway using either an Ethernet or USB connection to your computer first, then configure the wireless settings. Detailed instructions on configuring your wireless devices for TCP/IP networking are provided in the next chapter.

Connect the gateway to you computer using the Ethernet cable included in the box from your CG814WG v2's LAN port (B) to the Ethernet adapter in your computer.



**Figure 3-2: Connect a PC to the gateway**

The CG814WG v2 Gateway incorporates Auto Uplink™ technology. Each LOCAL Ethernet port will automatically sense whether the 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, as Auto Uplink will accommodate either type of cable to make the right connection.

- d. To connect your computer to the modem via USB you must install the USB driver. Insert the *Resource CD* that came with your gateway into the CD drive of your computer.



**Note:** The USB connection option is only available for Windows PCs. Also, Windows 95 does not support USB without special operating system upgrades and patches.

Install the USB driver.

- Connect the USB cable to your modem and plug in the AC power for the gateway.
- Use the USB cable to connect your computer to the gateway.
- The found new hardware Windows installation wizard will prompt you for the drivers.



**Figure 3-3: Found New Hardware Wizard window**

Browse to the *Resource CD* and install the USB driver by clicking through the Windows wizard prompts.

- e. Plug in your CG814WG v2 and wait about 30 seconds for the lights to stop blinking.
- f. Now, turn on your computer. If software usually logs you in to your Internet connection, do not run that software or cancel it if it starts automatically.
- g. Verify the following:
  - ① The power light is lit after turning on the gateway.
  - ② The cable link light is solid green, indicating a link has been established to the cable network.
  - ④ The local lights are lit for any connected computers.

## 2. Log in to the Gateway.

**Note:** To connect to the gateway, your computer needs to be configured to obtain an IP address automatically via DHCP. For instructions on how to do this, please see [Appendix C, “Preparing Your Network”](#).

- a. Using the computer that you first used to access your cable modem Internet service, connect to the gateway by typing <http://192.168.0.1> in the address field of your Internet browser.



A login window opens as shown below:



**Figure 3-4: Login window**

- b. For security reasons, the gateway has two sets of user names and passwords: one for a parent and one for children. Only the parent's login can be used to set up Parental Control and MAC Filtering. The child's login can configure all other features of the gateway.

When prompted to log in as the parent, enter **superuser** for the user name and **password** for the password, both in lower case letters.

When prompted to log in as the child, enter **admin** for the user name and **password** for the password, both in lower case letters.

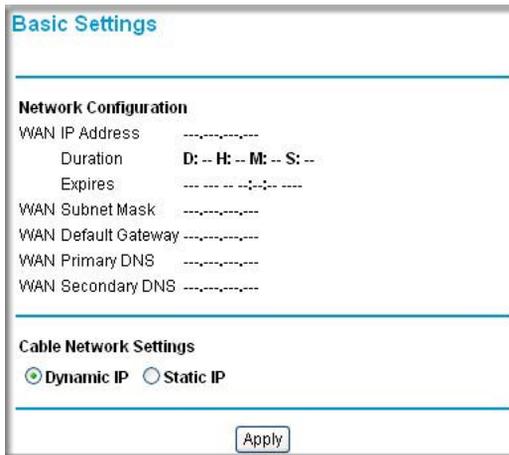
- c. After logging in, you will see the Basic Settings shown in [Figure 3-5](#) below.



**Note:** If you were unable to connect to the gateway, please refer to [“Basic Functions” on page 7-1](#).

### 3. Connect to the Internet.

- a. You are now connected to the gateway. Click the Basic Settings link on the upper left of the main menu. You are now connected to the gateway's *Basic Settings* page, shown below.



The screenshot shows the 'Basic Settings' page with two main sections: 'Network Configuration' and 'Cable Network Settings'. The 'Network Configuration' section includes fields for WAN IP Address, Duration (with sub-fields D, H, M, S), Expires, WAN Subnet Mask, WAN Default Gateway, WAN Primary DNS, and WAN Secondary DNS. The 'Cable Network Settings' section has radio buttons for 'Dynamic IP' (selected) and 'Static IP'. An 'Apply' button is located at the bottom of the page.

**Figure 3-5: Basic Settings page**

You are ready to configure your gateway to connect to the Internet.

- b. Select Dynamic or Static IP Address:

If your service provider assigns your IP address automatically through DHCP, select “Dynamic IP”. If your service provider has assigned you a permanent, fixed (static) IP address for your PC, select “Static IP”.

If you select Static IP, enter the IP address that your ISP assigned. Also enter the Static IP Mask (also known as netmask), Gateway IP address and Domain Name Server (DNS) Address.

- The Gateway is the ISP’s router to which your gateway will connect.
  - A DNS server is a host on the Internet that translates Internet names (such as `www.netgear.com`) to numeric IP addresses. Typically your ISP transfers the IP address of one or two DNS servers to your gateway 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 gateway.
- c. Click **Apply** to accept these settings.

## Chapter 4

# Wireless Configuration

This chapter describes how to configure the wireless features of your CG814WG v2 Wireless Cable Modem Gateway.



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

## 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 gateway in order to maximize the network speed. For further information on wireless networking, refer to [“Wireless Networking Overview”](#) in [Appendix B, “Networks, Routing, and Firewall Basics”](#).

### Implement Appropriate 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, use the security features of your wireless equipment. Restricting access by MAC address filtering adds an obstacle to unwanted users joining your network. To hinder a determined eavesdropper, you should use one of Wired Equivalent Privacy (WEP) data encryption options.

## Observe Placement and Range Guidelines

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless gateway.



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

For best results, place your gateway:

- 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 2.4 GHz cordless phones.
- Away from large metal surfaces.

## Configuring Wireless Settings

To configure the Wireless interface of your gateway, click on the Wireless Settings heading in the Setup section of the browser interface. The Wireless Settings menu will appear, as shown below:

The screenshot shows a web-based configuration interface for wireless settings. It is titled "Basic" and contains several sections:

- Wireless Network:** Includes a text field for "Name(SSID)" containing "Customer ID" and a dropdown menu for "Channel" set to "6".
- Wireless Access Point:** Contains two checked checkboxes: "Enable Wireless Access Point" and "Allow Broadcast of Name (SSID)".
- Wireless Card Access List:** Features an unchecked checkbox "Turn Access Control On" and a "Setup Access List" button.
- Security Encryption(WEP):** Includes a dropdown for "Encryption Mode" set to "WEP (128-bit)" and another dropdown for "Authentication" set to "Open System or Shared Key". Below this is a "WEP PassPhrase" field with a "Generate" button.
- WEP Keys:** Four radio buttons labeled "Key 1" through "Key 4" are shown, each with a corresponding text field containing 24 zeros. "Key 1" is selected.
- Apply:** A button at the bottom of the form.

Figure 4-1: Wireless Settings menu

## Wireless Network Settings

In the Wireless Settings section are the following parameters:

- **Name (SSID)**  
Enter a Service Set ID (SSID) 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**  
This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby access point.

## Wireless Access Point

In the Wireless Access Point Settings section are the following parameters:

- **Enable Wireless Access Point**  
Use this checkbox to turn on or turn off the wireless network. The default is to enable the wireless network.
- **Allow Broadcast of Name (SSID)**  
Use this checkbox to turn on or turn off broadcast of the wireless network Name (SSID). The default is to broadcast the wireless network Name (SSID). If you uncheck this item, only wireless devices with the correct SSID will be connect. Turning off the SSID broadcast prevents some wireless devices from discovering and reporting the SSID of your wireless network.

## Restricting Wireless Access by MAC Address

By default, any wireless PC that is configured with the correct SSID will be allowed access to your wireless network. For increased security, you can restrict access to the wireless network to only allow specific PCs based on their MAC addresses.

Check the Turn Access Control On box to restrict access to you network to computers in the Access Control List.

To access the Access List, click the Setup Access List button.



**Note:** If the **Turn Access Control On** is enabled and the Access Control List is blank; then all wireless PCs will be unable to connect to your wireless network.

**Wireless Card Access List**

---

**Access List**

#	Device Name	MAC Address
<input type="radio"/> 1	cowens-ibm	00:30:ab:14:14:16

---

**Connected Wireless Devices**

	Device Name	IP Address	MAC Address	Interface
<input type="radio"/>	cowens-ibm	192.168.0.12	00:30:ab:14:14:16	802.11
<input type="radio"/>	djames-IBM	192.168.0.13	00:30:ab:11:e9:f4	802.11

**Add Access Filter**

Device Name	MAC Address
<input type="text"/>	<input type="text"/>

**Figure 4-2: Wireless Access List menu**

The Access List displays a list of MAC addresses that will be allowed to connect to the gateway. These PCs must also have the correct SSID and WEP settings. You can add MAC addresses to the Access List by either selecting from the list of Connected Wireless Devices, or by manually entering MAC addresses.

To restrict access based on MAC addresses:

1. For your convenience, this menu displays a list of currently Connected Wireless Devices and their MAC addresses. Select a device from the list that you want to allow to access your network.
2. If the desired PC does not appear in the list, you can manually enter the MAC address of the authorized PC.  
The MAC address is usually printed on the wireless card.
3. If no Device Name appears, you can type a descriptive name for the PC that you are adding.

4. Click Add.
5. When you have finished entering MAC addresses, click Apply to save the Access List and return to the Wireless Settings menu.

To delete a MAC address from the table, click on it to select it, then click the Delete button.

## Configuring Wired Equivalent Privacy (WEP)

In the Wireless Settings menu you can configure WEP data encryption using the following parameters:

- Encryption Mode  
Select the WEP Encryption level:
  - Off - no data encryption (Open System)
  - 64-bit (sometimes called 40-bit) encryption
  - 128-bit encryption
- Authentication Type  
Select the appropriate value - "Open System" or "Shared Key." Check your wireless card's documentation to see what method to use.
- Encryption (WEP) Key  
If WEP is enabled, you can manually or automatically program the four data encryption keys. These values must be identical on all PCs and Access Points in your network.
  - Automatic - Enter a word or group of printable characters in the WEP PassPhrase box and click the Generate button. The four key boxes will be automatically populated with key values.
  - Manual - Enter ten hexadecimal digits (any combination of 0-9, a-f, or A-F)  
Select which of the four keys will be active.

Be sure to click **Apply** to save your settings in this menu.

## Chapter 5

# Protecting Your Network

This chapter describes how to use the firewall features of the CG814WG v2 Wireless Cable Modem Gateway to protect your network.

### Protecting Access to Your CG814WG v2 Gateway

---

For security reasons, the gateway has its own user name and password. Also, after a period of inactivity for a set length of time, the administrator login will automatically disconnect. When prompted, enter **admin** for the gateway User Name and **password** for the gateway Password. You can use procedures below to change the gateway's password and the amount of time for the administrator's login timeout.

**Note:** The user name and password are not the same as any user name or password you may use to log in to your Internet connection.

NETGEAR recommends that you change this password to a more secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of both upper and lower case letters, numbers, and symbols. Your password can be up to 30 characters.

#### Procedure 5-1: Changing the Built-In Password

1. Log in to the gateway at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the gateway.

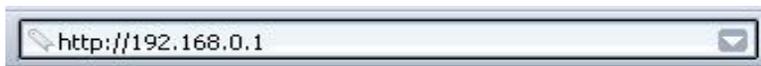
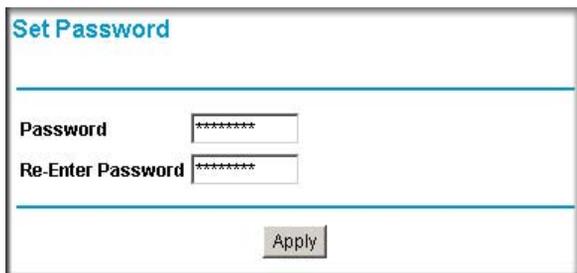


Figure 5-1: Log in to the gateway

2. From the main menu of the browser interface, under the Maintenance heading, select Set Password to bring up the dialog box shown below.

The image shows a web browser dialog box titled "Set Password" in blue text. Below the title is a horizontal line. There are two input fields: the first is labeled "Password" and the second is labeled "Re-Enter Password". Both fields contain a series of asterisks (\*\*\*\*\*). Below the input fields is another horizontal line, and at the bottom center is a button labeled "Apply".

**Figure 5-2: Set Password dialog box**

3. To change the password, first enter the old password, and then enter the new password twice.
4. Click **Apply** to save your changes.

**Note:** After changing the password, you will be required to log in again to continue the configuration. If you have backed up the gateway settings previously, you should do a new backup so that the saved settings file includes the new password.

## **Blocking Keywords, Sites, and Services**

---

The gateway provides a variety of options for blocking Internet based content and communications services. With its content filtering feature, the CG814WG v2 Gateway prevents objectionable content from reaching your PCs. The CG814WG v2 allows you to control access to Internet content by screening for keywords within Web addresses. It also has the capability to block access to all sites except those that are explicitly allowed. Key content filtering options include:

- Blocking access from your LAN to Internet locations that contain keywords that you specify.
- Blocking access to Web sites that you specify as off-limits.
- Allowing access to only Web sites that you specify as allowed.

The section below explains how to configure your gateway to perform these functions.

## Blocking Keywords and Domains



**Note:** The Block Sites feature must be configured while logged in as a parent.

The CG814WG v2 Gateway allows you to restrict access to Internet content based on functions such as Web address keywords and Web domains.

A domain name is the name of a particular Web site. For example, for the address [www.NETGEAR.com](http://www.NETGEAR.com), the domain name is NETGEAR.com.

1. Log in to the gateway at its default LAN address of <http://192.168.0.1> with its parent default User Name of **superuser**, default password of **password**, or using whatever Password and LAN address you have chosen for the gateway in parent mode.
2. Click on the Block Sites link of the Content Filtering menu.

**Block Sites**

---

**Keyword Blocking**  *Enable*

**Keyword List**

yahoo

---

**Domain Blocking**  *Enable*

**Domain List**

**Figure 5-3: Block Sites menu**

3. To enable keyword blocking or Domain Blocking, check the appropriate Enable box.
4. Enter Keywords into the Keyword List by typing then in the Add Keyword box, then, click Add Keyword.

Some examples of Keyword applications follow:

- If the keyword “XXX” is specified, the URL <http://www.badstuff.com/xxx.html> is blocked.
- If the keyword “.com” is specified, only Web sites with other domain suffixes (such as .edu or .gov) can be viewed.
- Enter the keyword “.” to block all Internet browsing access.

Up to eight entries are supported in the Keyword list.

5. Enter Domains into the Domain List by typing then in the Add Domain box, then, click Add Domain.

If the domain “badstuff.com” is specified, the URL <http://www.badstuff.com/xxx.html> is blocked, along with all other urls in the badstuff.com site.

Up to eight entries are supported in the Keyword list.

6. To block access to the domains in the Domain List, select Deny Domains.  
To allow access to only the domains in the Domain List, select Allow Domains. If the domain “goodstuff.com” is specified, you will be able to access only sites on the goodstuff site.
7. To delete a keyword or domain, select it from the list, click Remove Keyword or Remove Domain.
8. Click **Apply** to save your settings.

## Using MAC Filtering

---



**Note:** The MAC Filtering feature must be configured while logged in as a parent.

By default, any PC will be allowed access to the Internet through your Gateway. MAC Filtering allows you to block access to the Internet to any PC on your LAN based on the hardware address of its ethernet or wireless adapter: the MAC address.

1. Log in to the gateway at its default LAN address of <http://192.168.0.1> with its parent default User Name of **superuser**, default password of **password**, or using whatever Password and LAN address you have chosen for the gateway in parent mode.
2. Click the MAC Filtering link on the Advanced menu. At the top of the page is a list of *Trusted Devices* that are currently connected to the Gateway.

### To add a device to the MAC Filtering list:

1. Enter the MAC address:
  - If the desired device is in the *Trusted Devices* table, click the radio button of that PC to capture its MAC address.
  - If the desired device is not in the *Trusted Devices* table, you can manually enter the MAC address of the PC you wish to block.
  - If no Device Name automatically appears, you can type a descriptive name for the PC that you are adding.
2. When you have finished entering the MAC address, click **Add**, and click **Apply**.

### To delete a device from the MAC Filtering list:

1. Select the MAC address of the PC you want to delete from the list.
2. Click **Delete** to delete the entry.
3. Click **Apply** to activate the settings.

**MAC Filtering**

---

**Trusted Devices**

	Device Name	IP Address	MAC Address	Interface
<input type="radio"/>	PC12345	192.168.0.10	00:0d:60:5d:3c:35	Ethernet3

---

**Add MAC Filter**

Device Name	MAC Address
<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>

**MAC Filter List**

Enable

**Day(s) to Block**

Everyday  Sunday  Monday  Tuesday  
 Wednesday  Thursday  Friday  Saturday

**Time of Day to Block**

All day

Start:  (hour)  (min)

End:  (hour)  (min)

---

**Figure 5-4: MAC Filtering menu**

## Blocking Access by Time of Day

The default blocking schedule is to block access all day. However, you can also block access according to a daily schedule for each PC individually.

1. In the *MAC Filter List*, select the PC for which the schedule will be modified.
2. In the *Day(s) to Block* section, click the boxes next to the days when you want access blocked.
3. In the *Time of Day to Block* section, select either **All Day**, or set the hours for internet blocking.
4. Click **Apply** to activate the settings.

## Using Port Blocking

---

Firewall rules are used to block or allow specific traffic passing through from one side to the other. Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Instructions for setting up inbound rules can be found in [“Port Forwarding“ on page -7](#). Outbound rules (LAN to WAN) determine what outside resources local users can have access to. This section describes how to set up outbound rules.

A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the CG814WG v2 are:

- **Inbound:** Block all access from outside except responses to requests from the LAN side.
- **Outbound:** Allow all access from the LAN side to the outside.

You may define additional rules that will specify exceptions to the default rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day.

To configure outbound rules on the CG814WG v2, click the Port Blocking link on the Advanced section of the main menu.

**Port Blocking**

Active Filters				
	Name	Start Port	End Port	Protocol
<input type="radio"/>	FTP	21	21	TCP
<input type="radio"/>	AIM	5190	5190	TCP

**Add Predefined Service**

Service:

**Add Custom Service**

Name	Start Port	End Port	Protocol
<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="Both"/>

**Figure 5-5: Port Blocking menu**

- To block outbound traffic, select the service you would like to block from the drop-down list of predefined services. Click Add.
- If the service you would like to block is not in the predefined list, you can add a custom service. Enter the range of ports you would like to block and select whether the ports are TCP, UDP or Both. Click Add.
- To delete an existing rule, select its button on the left side of the table and click Delete.

## Port Forwarding

Because the CG814WG v2 uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a Web server or game server) visible and available to the Internet. The rule tells the gateway to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as Port Forwarding.



**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.

### Considerations for Port Forwarding

- If the IP address of the local server PC is assigned by DHCP, it may change when the PC is rebooted. To avoid this, you can assign a static IP address to your server outside the range that is assigned by DHCP, but in the same subnet as the rest of your LAN. By default, the IP addresses in the range of 192.168.0.2 through 192.168.0.9 are reserved for this.
- Local PCs must access the local server using the PCs' local LAN address (192.168.0.XXX, by default). Attempts by local PCs to access the server using the external WAN IP address will fail.

Remember that allowing inbound services opens holes in your firewall. Only enable those ports that are necessary for your network.

The following are two application examples of inbound rules.

- To forward inbound traffic:
  1. Select the service you would like to forward from the drop-down list of predefined services.

**Port Forwarding**

**Active Forwarding Rules**

	Name	Start Port	End Port	Protocol	Local IP Address
<input type="radio"/>	TELNET	23	23	TCP	192.168.0.10
<input type="radio"/>	HTTP	80	80	TCP	192.168.0.15

**Choose Predefined Service**

Service:

**Add Custom Rules**

Name	Start Port	End Port	Protocol	Local IP Address
<input type="text"/>	0	0	Both	192.168.0.0

**Figure 5-6: Port Forwarding menu**

If the service you would like to forward is not in the predefined list, you can add a custom service. Enter the range of ports you would like to forward and select whether the ports are TCP, UDP or Both.

2. Enter the IP address of the computer on your network to which you would like to direct the inbound traffic
  3. Click Add.
  4. To access the local computer from the Internet, you must use the WAN address of your gateway, which can be found on the Basic Settings page.
- To delete an existing rule, select its button on the left side of the table and click Delete.

## Using Port Triggering

---

Port Triggering is an advanced feature that allows you to dynamically open inbound ports based on outbound traffic on different ports. This is an advanced feature that can be used for gaming and other internet applications.

Port Forwarding can typically be used to enable similar functionality, but it is static and has some limitations. Ports will be open to traffic from the internet until the port forwarding rule is removed. Additionally, port forwarding does not work well for some applications when your WAN IP address is assigned by DHCP, and is changed frequently. Port Triggering opens in incoming port temporarily and can does not require the server on the internet to track your IP address if it is changed.

Port Triggering monitors outbound traffic. When the gateway detects traffic on the specified outbound port, it remembers the IP address of the computer that sent the data and “triggers” the incoming port. Incoming traffic on the triggered port is then forwarded to the triggering computer.

An example of Port Triggering for Internet Relay Chat (IRC) is shown in [Figure 5-7](#). When you connect to an IRC server, the server tries to connect back on port 113 to do an Ident lookup. Unless you have configured Port Forwarding to open port 113, the traffic will be blocked. In this example, the initial login to the server in the range of ports 6660 to 6670 will be detected. This will trigger the gateway to temporarily forward port 113 to the PC that initiated the login.

To configure Port Triggering:

1. In the Trigger Range, enter the outbound ports that will be monitored for activity. This will be the “trigger”.
2. In the Target Range, enter the inbound ports that should be forwarded when the trigger occurs.
3. Select the appropriate protocol: TCP, UDP or Both.
4. Check the Enable box
5. Click **Apply**.

To clear a Port Triggering rule, you can either remove the check from the Enable box, to temporarily disable the rule, or you can select the rule and click Delete.

Port Triggering						
	Trigger Range		Target Range		Protocol	Enable
	Start Port	End Port	Start Port	End Port		
<input checked="" type="radio"/>	6660	6670	113	113	TCP	<input checked="" type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>

**Figure 5-7: Port Triggering menu, with IRC example.**

## Setting Up A Default DMZ Host

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



**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 firewall, and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

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

To assign a computer or server to be a DMZ Host, from the main menu, under Advanced, select DMZ Host. Enter the IP address of the computer you would like to assign as a DMZ Host and click Apply. To disable the DMZ Host, enter “0” and click Apply.

## Respond to Ping on Internet WAN Port

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

## Enabling or Disabling Content Filtering Services

---



**Note:** The Services page is only accessible while logged in as a parent.

You can use the Services page to disable certain gateway features. To disable a feature, remove the check box from its Enable check box.

When Firewall Features are enabled, the gateway will perform Stateful Packet Inspection (SPI) and protect against Denial of Service (DoS) attacks.

When VPN Pass-Through is enabled, IPSec and PPTP traffic will be forwarded. When it is disabled, this traffic will be blocked.



# Chapter 6

## Managing Your Network

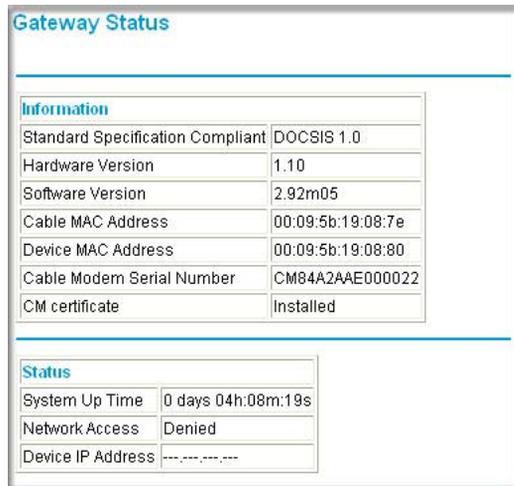
This chapter describes how to perform network management tasks with your CG814WG v2 Wireless Cable Modem Gateway.

### Network Status Information

The CG814W provides a variety of status and usage information which is discussed below.

### Viewing Gateway Status

From the main menu, under Maintenance, select Gateway Status to view the screen in [Figure 6-1](#).



The screenshot shows the 'Gateway Status' screen with two main sections: 'Information' and 'Status'. The 'Information' section contains a table with the following data:

Information	
Standard Specification Compliant	DOCSIS 1.0
Hardware Version	1.10
Software Version	2.92m05
Cable MAC Address	00:09:5b:19:08:7e
Device MAC Address	00:09:5b:19:08:80
Cable Modem Serial Number	CM84A2AAE000022
CM certificate	Installed

The 'Status' section contains a table with the following data:

Status	
System Up Time	0 days 04h:08m:19s
Network Access	Denied
Device IP Address	.....

**Figure 6-1: Gateway Status screen**

This screen shows the following parameters:

**Table 6-1. 3.2 - Router Status Fields**

<b>Field</b>	<b>Description</b>
Information	
Standard Specification Compliant	The specification to which the gateway's cable interface is compatible.
Hardware Version	The hardware version of the gateway.
Software Version	The software version of the gateway.
Cable Modem MAC Address	The MAC address being used by the Cable Modem port of the gateway. This MAC address may need to be registered with your Cable Service Provider.
Device MAC Address	The MAC address of the router side of the gateway. This is the equivalent of your PC when connected to a cable modem. You can use the MAC Cloning feature to replace this MAC address with another address when sending packets to the WAN.
Cable Modem Serial Number	The serial number of the gateway hardware.
CM Certificate	If the Cable Modem certificate is Installed, it is possible for the service provider to upgrade your Data Over Cable service securely.
Status	
System Up Time	This is the time since the gateway has registered with your cable service provider.
Network Access	This field will change to Allowed when the registration with your cable service provider is complete.
Cable Modem IP Address	The IP address of you gateway, as seen from the Internet.

## Connection Status

From the main menu, under Maintenance, select Connection to view the screen in [Figure 6-2](#).

Connection			
<b>Startup Procedure</b>			
Procedure	Status	Comment	
Acquire Downstream Channel		Locked	
Connectivity State	OK	Operational	
Boot State	OK	Operational	
Configuration File			
Security	Disabled	Disabled	
<b>Downstream Channel</b>			
Lock Status	Locked	Modulation	QAM64
Channel ID	1	Symbol rate	5056941
Downstream Frequency		Downstream Power	15.9 dBmV
SNR	37.9 dB		
<b>Upstream Channel</b>			
Lock Status	Locked	Modulation	QPSK
Channel ID	1	Symbol rate	1280 Ksym/sec
Upstream Frequency		Upstream Power	11.0 dBmV
<b>Current System Time:</b> THU APR 19 22:36:09 2001			

**Figure 6-2: Connection screen**

This screen shows detailed information about the status of the connection to your cable service provider that can be used for troubleshooting. The gateway goes through the following steps to be provisioned

1. Acquire and lock Downstream Channel
2. Acquire upstream parameters and range.
3. Lock Upstream Channel
4. Acquire IP Address through DHCP

### Current System Time

The date and time is acquired from your cable service provider as part of the registration procedure.

## Configuring LAN IP Settings

The LAN IP Setup menu allows configuration of LAN IP services such as the IP address of the gateway and DHCP. These features can be found under the Advanced heading in the main menu in the LAN IP menu.

### LAN IP Setup

The gateway is shipped preconfigured to use private IP addresses on the LAN side, and to act as a DHCP server. The gateway'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 the LAN IP Setup menu as shown to the right.

The LAN TCP/IP Setup parameters are:

- LAN IP Address  
This is the IP address of the gateway.
- Subnet Mask  
This is the LAN Subnet Mask of the gateway. Combined with the IP address, the Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.

The screenshot shows the LAN IP configuration interface. At the top, the title is "LAN IP". Below it are several configuration fields:

- LAN IP Address:** 192, 168, 0, 1
- Subnet Mask:** 255, 255, 255, 0
- DHCP Server:** Yes (selected), No
- Starting IP Address:** 192, 168, 0, 10
- Ending IP Address:** 192, 168, 0, 14

An "Apply" button is located below these fields. Below the configuration fields is a table titled "DHCP Client Lease Info":

MAC Address	IP Address	Expires
0030ab141416	192.168.000.012	APR 19 23:30:49
0030ab11e9f4	192.168.000.013	APR 19 23:34:01

At the bottom of the interface, it shows the "Current System Time: THU APR 19 22:37:07 2001" and a "Clear DHCP Leases" button.

Figure 6-3: LAN IP Setup menu.



**Note:** If you change the LAN IP address of the gateway 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.

## Using the Gateway as a DHCP Server

By default, the gateway 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 gateway. 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 gateway are satisfactory. See [“IP Configuration by DHCP” on page A-10](#) for an explanation of DHCP and information about how to assign IP addresses for your network.

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, select NO for the DHCP Server, otherwise leave Yes selected.

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 gateway's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.0.10 and 192.168.0.253. The range of IP addresses between 192.168.0.2 and 192.168.0.9 can be used for devices with fixed addresses.

The gateway 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 is the gateway's LAN IP address
- Primary DNS Server, if you entered a Primary DNS address in the Basic Settings menu; otherwise, the gateway's LAN IP address
- Secondary DNS Server, if you entered a Secondary DNS address in the Basic Settings menu.



**Note:** The gateway implements a DNS Relay function. When it receives a DNS request on the LAN, it passes it to the DNS server specified on the WAN. It then relays the response back to the original requesting PC.

### DHCP Client Lease Info

The DHCP Client Lease Info table lists information about each PC that has been assigned a DHCP lease by the gateway. The MAC address of the PC, IP address assigned and the expiration time of the DHCP lease are listed.

You can manually revoke the DHCP leases by clicking Clear DHCP Leases.

## Viewing and Emailing Logged Information

---

The gateway will log security-related events such as denied incoming service requests and hacker probes. You can enable e-mail notification to receive these logs in an e-mail message. Log entries are described in [Table 6-4](#)

**Table 6-4: Security Log entry descriptions**

Field	Description
Description	The type of event and what action was taken if any.
Count	This is a reference number for each event.
Last Occurrence	The date and time the log entry was recorded.
Target	The name or IP address of the destination device or Web site.
Source	The IP address of the initiating device for this log entry.

### Enabling Logs Event E-mail Notification

In order to receive logs and alerts by e-mail, you must provide your e-mail information in the E-Mail section of the Logs menu:

- In the Contact Email Address, type the e-mail address to which the logs will be sent. Use a full e-mail address (for example, ChrisXY@myISP.com).
- In the SMTP Server Name box, type the outgoing SMTP mail server of your ISP (for example, 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, no alerts or logs will be sent.
- Check the E-mail Alerts Enable box.
- Click E-mail Log to send the log immediately.
- Click **Apply**.

## Erasing Configuration

---

The configuration settings of the CG814WG v2 Gateway are stored in a configuration file in the gateway. This file can be reverted to factory default settings. The procedures below explain how to do these tasks.

It is sometimes desirable to restore the gateway to the factory default settings. This can be done by using the Erase function.

1. To erase the configuration, from the main menu, under Maintenance select Set Password. Select Yes for Restore Factory Defaults and click Apply.
2. The gateway will then reboot automatically.

After an erase, the gateway's password will be **password**, the LAN IP address will be 192.168.0.1, and the router's DHCP client will be enabled.

**Note:** 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 gateway.

1. Using a paper clip, depress and hold the Default Reset Button. All the numbered Ethernet LEDs will illuminate green.
2. Continue to depress the button for at least 5 seconds.
3. The gateway will reboot and clear its configuration information.

## Running Diagnostic Utilities

---

The CG814WG v2 Gateway has a diagnostics feature. You can use the diagnostics menu to test connectivity to PC using the Ping command:

From the main menu of the browser interface, under the Maintenance heading, select the Diagnostics menu, shown below.

The screenshot shows a web interface titled "Diagnostics". Under the heading "Ping Test Parameters", there are four input fields: "Ping Target" (192.168.0.10), "Ping Size" (64 bytes), "No. of Pings" (3), and "Ping Interval" (1000 ms). Below these fields are three buttons: "Start Test", "Abort Test", and "Clear Results". A "Results" section contains a text box with the following output: "Pinging 192.168.0.10 with 64 bytes of data:[Complete] Reply from 192.168.0.10: bytes = 64, time = 0 ms Reply from 192.168.0.10: bytes = 64, time = 0 ms Reply from 192.168.0.10: bytes = 64, time = 0 ms 3/3 replies received. min time=10 ms, max time=10 ms, avg time=0 ms". At the bottom of the results section, there is a red text prompt: "To get an update of the results you must REFRESH the page." with a "REFRESH" button.

**Figure 6-5: Diagnostics menu**

To perform a Ping test

1. In the Ping Target section, enter the IP address of the PC you would like to ping.
2. If you would like to specify additional details, you can set the Ping Size, No. of Ping and Ping Interval.
3. Click Start Test.
4. Click REFRESH to see the results of the Ping test.

## Enabling Remote Management Access

---

Using the Remote Management page, you can allow a user or users on the Internet to configure, upgrade and check the status of your CG814WG v2 Gateway.

To configure your gateway for Remote Management:

1. Select the Allow Remote Management check box.
2. Specify what the Remote User Name and Remote Password that will be required to remotely access your CG814WG v2.
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.
5. When accessing your router from the Internet, type your router's WAN IP address into your browser, followed by a colon (:) and the port number. For example, if your WAN IP address is 134.177.0.123 and you use port number 8080, type the following in your browser:

**http://134.177.0.123:8080**

## Enabling Remote Management Access After a Reset

---

Using the Remote Management page, you can allow the Remote Management feature to be active after a Factory Default Reset. If you do not select this checkbox and use the Erase button to revert to the Factory Default settings, you will not be able to remotely access your CG814WG v2.



## Chapter 7

# Troubleshooting

This chapter gives information about troubleshooting your CG814WG v2 Wireless Cable Modem Gateway. For the common problems listed, go to the section indicated.

- Is the gateway on?
- Have I connected the gateway correctly?  
Go to [“Basic Functions” on page 7-1](#).
- I can’t access the gateway’s configuration with my browser.  
Go to [“Troubleshooting the Web Configuration Interface” on page 7-3](#).
- I’ve configured the gateway but I can’t access the Internet.  
Go to [“Troubleshooting the ISP Connection” on page 7-4](#).
- I can’t remember the gateway’s configuration password.
- I want to clear the configuration and start over again.  
Go to [“Erasing Configuration” on page 6-7](#).

## Basic Functions

---

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

1. When power is first applied, verify that the Power LED is on.
2. Verify that the numbered Ethernet LEDs come on momentarily.
3. After approximately 30 seconds, verify that:
  - a. The Local port Link LEDs are lit for any local ports that are connected.
  - b. The Internet Link port LED is lit.

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 gateway is turned on:

- Make sure that the power cord is properly connected to your gateway 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.

## All LEDs Stay On

If All LEDs stay on when your gateway is turned on:

- Clear the gateway's configuration to factory defaults. This will set the gateway's IP address to 192.168.0.1. This procedure is explained in [“Erasing Configuration” on page 6-7](#).

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

## Local Link LEDs Not On

If the Local Port Link LEDs do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the gateway and at the hub or PC.
- Make sure that power is turned on to the connected hub or PC.
- Be sure you are using the correct cable:
  - When connecting the gateway'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.

## Cable Link LED Not On

If the Cable Link LED does not light when connected to your cable television cable, check the following:

- Make sure that the coaxial cable connections are secure at the gateway and at the wall jack.
- Make sure that your cable internet service has been provisioned by your cable service provider. Your provider should verify that the signal quality is good enough for cable modem service.

- Remove any excessive splitters you may have on your cable line. It may be necessary to run a “home run” back to the point where the cable enters your home.

## Troubleshooting the Web Configuration Interface

---

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

- Check the Ethernet connection between the PC and the gateway as described in the previous section.
- Make sure your PC’s IP address is on the same subnet as the gateway. If you are using the recommended addressing scheme, your PC’s address should be in the range of 192.168.0.10 to 192.168.0.254. Refer to [“Verifying TCP/IP Properties” on page C-6](#) or [“Configuring the Macintosh for TCP/IP Networking” on page C-17](#) to find your PC’s IP address. Follow the instructions in [Appendix C](#) 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 gateway and reboot your PC.

- If your gateway’s IP address has been changed and you don’t know the current IP address, clear the gateway’s configuration to factory defaults. This will set the gateway’s IP address to 192.168.0.1. This procedure is explained in [“Erasing Configuration” on page 6-7](#).
- 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 gateway does not save changes you have made in the Web Configuration Interface, check the following:

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

## Troubleshooting the ISP Connection

---

If your gateway is unable to access the Internet and your Cable Link LED is on, you may need to register the Cable MAC Address and/or Device MAC Address of your gateway with your cable service provider. This is described in [“Connecting the CG814WG v2 Gateway” on page 3-2](#).

Additionally, your PC may not have the gateway configured as its TCP/IP gateway. If your PC obtains its information from the gateway by DHCP, reboot the PC and verify the gateway address as described in [“DHCP Configuration of TCP/IP in Windows 2000 ” on page C-11](#).

## 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 easier by using the ping utility in your PC or workstation.

### Testing the LAN Path to Your Gateway

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

To ping the gateway 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 gateway, as in this example:

```
ping 192.168.0.1
```

3. Click 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 [“Local Link LEDs Not On”](#) on [page 7-2](#).
- Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and gateway.
- 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 gateway 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 gateway 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 gateway is listed as the default gateway as described in [“DHCP Configuration of TCP/IP in Windows 2000”](#) on [page C-11](#).
- 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 Link LED is on.
- 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 Device MAC Address of your gateway because it does not match the MAC Address of the PC you previously used to connect to a cable modem. In this case you will need to clone your PC’s MAC Address. Refer to [“Connecting the CG814WG v2 Gateway”](#) on [page 3-2](#).



# Appendix A

## Technical Specifications

This appendix provides technical specifications for the CG814WG v2 Wireless Cable Modem Gateway.

### Network Protocol and Standards Compatibility

Data and Routing Protocols: TCP/IP  
DHCP server and client  
DNS relay  
NAT (many-to-one)  
TFTP client  
VPN pass through (IPSec, PPTP)

### Power Adapter

North America (input): 120V, 60 Hz, input  
All regions (output): 12 V DC @ 1.25A output, 15W maximum

### Physical Specifications

Dimensions: 175 by 114 by 30 mm  
6.9 by 4.5 by 1.2 in.  
Weight: 0.31 kg  
0.68 lb

### Environmental Specifications

Operating temperature: 32°-140° F (0° to 40° C)  
Operating humidity: 90% maximum relative humidity, noncondensing

### Electromagnetic Emissions

Meets requirements of: FCC Part 15 Class B

### Interface Specifications

Local: 10BASE-T or 100BASE-Tx, RJ-45  
USB 1.1 Function  
802.11b Wireless Access Point  
Internet: DOCSIS 2.0. Downward compatible with DOCSIS 1.0 and DOCSIS 1.1.

---



## Appendix B

# Networks, Routing, and Firewall Basics

This chapter provides an overview of IP networks, routing, and firewalls.

### Related Publications

---

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

### 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 CG814WG v2 Wireless Cable Modem Gateway 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 CG814WG v2 Gateway 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
```

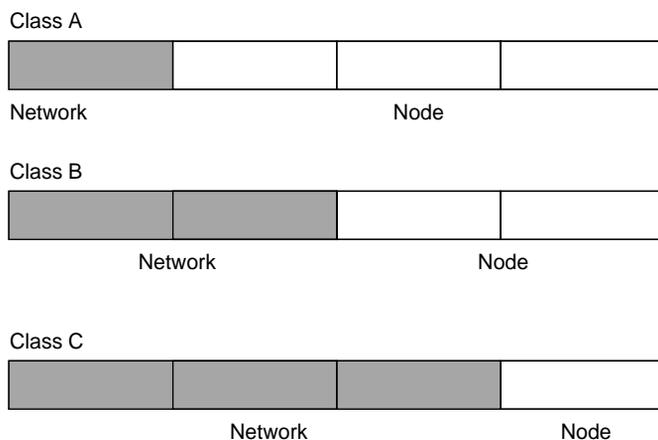
is normally written as:

```
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 7-1. 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 mask length formats.

**Table 7-2. Netmask Formats**

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/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 CG814WG v2 Gateway is preconfigured to automatically assign private addresses.

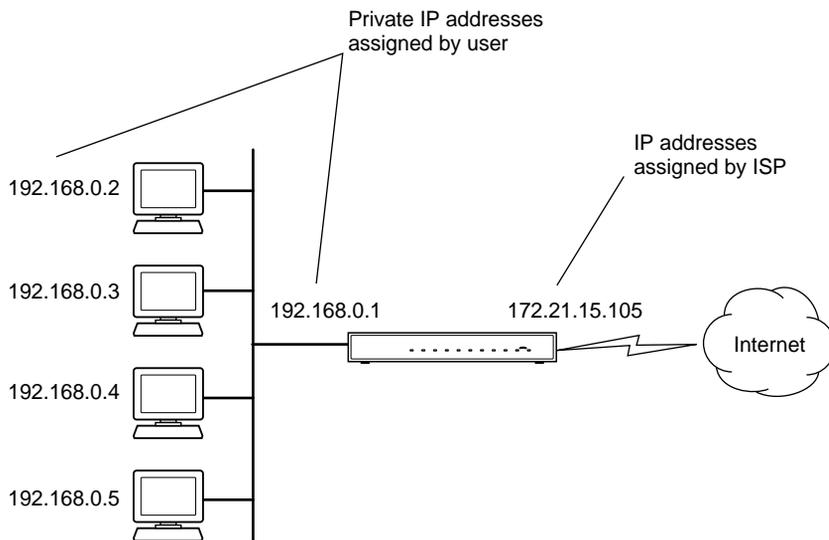
Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines explained here. For more information about address assignment, refer to RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*. The 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 CG814WG v2 Gateway employs an address-sharing method called Network Address Translation (NAT). This method allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your ISP.

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

The following figure illustrates a single IP address operation.



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

This scheme offers the additional benefit of firewall-like protection because the internal LAN addresses are not available to the Internet through the translated connection. All incoming inquiries are filtered out by the router. This filtering can prevent intruders from probing your system. However, using port forwarding, you can allow one PC (for example, a Web server) on your local network to be accessible to outside users.

## MAC Addresses and Address Resolution Protocol

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

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

## Related Documents

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.

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)*.

## 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 CG814WG v2 Gateway has the capacity to act as a DHCP server.

The CG814WG v2 Gateway also functions as a DHCP client when connecting to the ISP. The gateway can automatically obtain an IP address, subnet mask, DNS server addresses, and a gateway address if the ISP provides this information by DHCP.

## Internet Security and Firewalls

---

When your LAN connects to the Internet through a router, an opportunity is created for outsiders to access or disrupt your network. A NAT router provides some protection because by the very nature of the Network Address Translation (NAT) process, the network behind the NAT router is shielded from access by outsiders on the Internet. However, there are methods by which a determined hacker can possibly obtain information about your network or at the least can disrupt your Internet access. A greater degree of protection is provided by a firewall router.

### What is a Firewall?

A firewall is a device that protects one network from another, while allowing communication between the two. A firewall incorporates the functions of the NAT router, while adding features for dealing with a hacker intrusion or attack. Several known types of intrusion or attack can be recognized when they occur. When an incident is detected, the firewall can log details of the attempt, and can optionally send email to an administrator notifying them of the incident. Using information from the log, the administrator can take action with the ISP of the hacker. In some types of intrusions, the firewall can fend off the hacker by discarding all further packets from the hacker's IP address for a period of time.

## Stateful Packet Inspection

Unlike simple Internet sharing routers, a firewall uses a process called stateful packet inspection to ensure secure firewall filtering to protect your network from attacks and intrusions. Since user-level applications such as FTP and Web browsers can create complex patterns of network traffic, it is necessary for the firewall to analyze groups of network connection “states.” Using Stateful Packet Inspection, an incoming packet is intercepted at the network layer and then analyzed for state-related information associated with all network connections. A central cache within the firewall keeps track of the state information associated with all network connections. All traffic passing through the firewall is analyzed against the state of these connections in order to determine whether or not it will be allowed to pass through or rejected.

## Denial of Service Attack

A hacker may be able to prevent your network from operating or communicating by launching a Denial of Service (DoS) attack. The method used for such an attack can be as simple as merely flooding your site with more requests than it can handle. A more sophisticated attack may attempt to exploit some weakness in the operating system used by your router or gateway. Some operating systems can be disrupted by simply sending a packet with incorrect length information.

## Wireless Networking Overview

---

The CG814WG v2 Gateway conforms to the Institute of Electrical and Electronics Engineers (IEEE) 802.11b standard for wireless LANs (WLANs). On an 802.11b wireless link, data is encoded using direct-sequence spread-spectrum (DSSS) technology and is transmitted in the unlicensed radio spectrum at 2.5GHz. The maximum data rate for the wireless link is 11 Mbps, but it will automatically back down from 11 Mbps to 5.5, 2, and 1 Mbps when the radio signal is weak or when interference is detected.

The 802.11b standard is also called Wireless Ethernet or Wi-Fi by the Wireless Ethernet Compatibility Alliance (WECA, see <http://www.wi-fi.net>), an industry standard group promoting interoperability among 802.11b devices. The 802.11b standard offers two methods for configuring a wireless network - ad hoc and infrastructure.

## 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.

## 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.

## Network Name: 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 ESSID is used, but may still be referred to as SSID.

An SSID is a thirty-two character (maximum) alphanumeric key identifying the name of 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

---

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 used when the wireless devices are configured to operate in Shared Key authentication mode. There are two shared key methods implemented in most commercially available products, 64-bit and 128-bit WEP data encryption.

### 802.11b Authentication

The 802.11b standard defines several services that govern how two 802.11b devices communicate. The following events must occur before an 802.11b Station can communicate with an Ethernet network through an access point such as the one built in to the CG814WG v2:

1. Turn on the wireless station.
2. The station listens for messages from any access points that are in range.
3. The station finds a message from an access point that has a matching SSID.
4. The station sends an authentication request to the access point.
5. The access point authenticates the station.
6. The station sends an association request to the access point.
7. The access point associates with the station.
8. The station can now communicate with the Ethernet network through the access point.

An access point must authenticate a station before the station can associate with the access point or communicate with the network. The IEEE 802.11b standard defines two types of authentication: Open System and Shared Key.

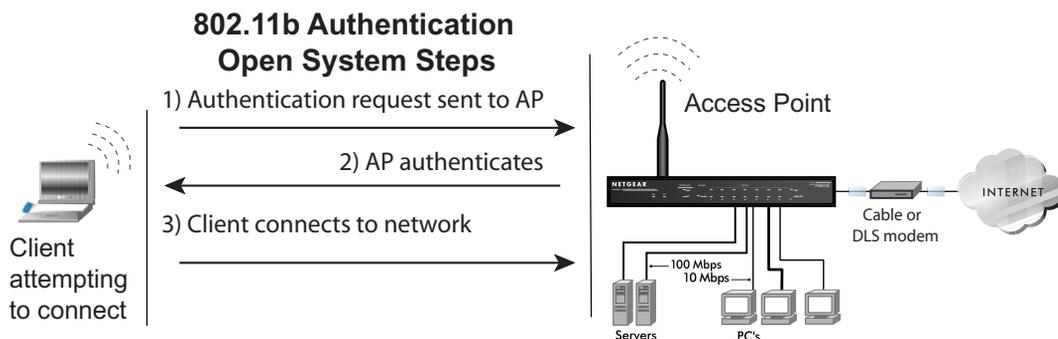
- Open System Authentication allows any device to join the network, assuming that the device SSID matches the access point SSID. Alternatively, the device can use the “ANY” SSID option to associate with any available Access Point within range, regardless of its SSID.
- Shared Key Authentication requires that the station and the access point have the same WEP Key to authenticate. These two authentication procedures are described below.

## Open System Authentication

The following steps occur when two devices use Open System Authentication:

1. The station sends an authentication request to the access point.
2. The access point authenticates the station.
3. The station associates with the access point and joins the network.

This process is illustrated in below.



**Figure B-4: 802.11b open system authentication**

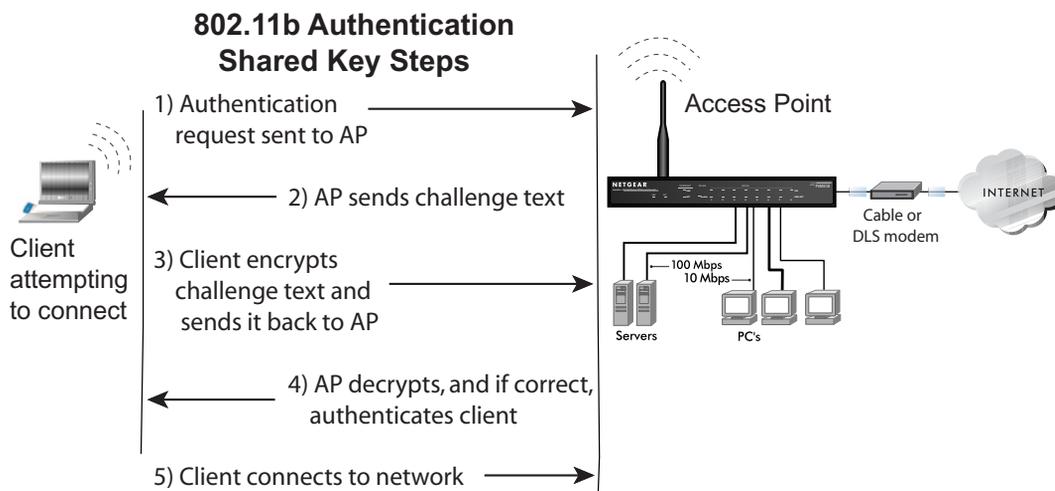
## Shared Key Authentication

The following steps occur when two devices use Shared Key Authentication:

1. The station sends an authentication request to the access point.
2. The access point sends challenge text to the station.
3. The station uses its configured 64-bit or 128-bit default key to encrypt the challenge text, and sends the encrypted text to the access point.
4. The access point decrypts the encrypted text using its configured WEP Key that corresponds to the station's default key. The access point compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, then the access point and the station share the same WEP Key and the access point authenticates the station.
5. The station connects to the network.

If the decrypted text does not match the original challenge text (i.e., the access point and station do not share the same WEP Key), then the access point will refuse to authenticate the station and the station will be unable to communicate with either the 802.11b network or Ethernet network.

This process is illustrated in below.



**Figure B-5: 802.11b shared key authentication**

## Overview of WEP Parameters

Before enabling WEP on an 802.11b network, you must first consider what type of encryption you require and the key size you want to use. Typically, there are three WEP Encryption options available for 802.11b products:

1. **Do Not Use WEP:** The 802.11b network does not encrypt data. For authentication purposes, the network uses Open System Authentication.
2. **Use WEP for Encryption:** A transmitting 802.11b device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving 802.11b device decrypts the data using the same WEP Key. For authentication purposes, the 802.11b network uses Open System Authentication.
3. **Use WEP for Authentication and Encryption:** A transmitting 802.11b device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving 802.11b device decrypts the data using the same WEP Key. For authentication purposes, the 802.11b network uses Shared Key Authentication.

**Note:** Some 802.11b access points also support **Use WEP for Authentication Only** (Shared Key Authentication without data encryption).

## Key Size

The IEEE 802.11b standard supports two types of WEP encryption: 40-bit and 128-bit.

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 user-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.

128-bit encryption is stronger than 40-bit encryption, but 128-bit encryption may not be available outside of the United States due to U.S. export regulations.

When configured for 40-bit encryption, 802.11b products typically support up to four WEP Keys. Each 40-bit WEP Key is expressed as 5 sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90” is a 40-bit WEP Key.

When configured for 128-bit encryption, 802.11b products typically support four WEP Keys but some manufacturers support only one 128-bit key. The 128-bit WEP Key is expressed as 13 sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90 AB CD EF 12 34 56 78 90” is a 128-bit WEP Key.

**Note:** Typically, 802.11b access points can store up to four 128-bit WEP Keys but some 802.11b client adapters can only store one. Therefore, make sure that your 802.11b access and client adapters configurations match.

## WEP Configuration Options

The WEP settings must match on all 802.11b devices that are within the same wireless network as identified by the SSID. In general, if your mobile clients will roam between access points, then all of the 802.11b access points and all of the 802.11b client adapters on the network must have the same WEP settings.

**Note:** Whatever keys you enter for an AP, you must also enter the same keys for the client adapter in the same order. In other words, WEP key 1 on the AP must match WEP key 1 on the client adapter, WEP key 2 on the AP must match WEP key 2 on the client adapter, etc.

**Note:** The AP and the client adapters can have different default WEP Keys as long as the keys are in the same order. In other words, the AP can use WEP key 2 as its default key to transmit while a client adapter can use WEP key 3 as its default key to transmit. The two devices will communicate as long as the AP's WEP key 2 is the same as the client's WEP key 2 and the AP's WEP key 3 is the same as the client's WEP key 3.

## Wireless Channels

---

IEEE 802.11 wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4 GHz and 2.5 GHz. Neighboring channels are 5 MHz apart. However, due to spread spectrum effect of the signals, a node sending signals using a particular channel will utilize frequency spectrum 12.5 MHz above and below the center channel frequency. As a result, two separate wireless networks using neighboring channels (for example, channel 1 and channel 2) in the same general vicinity will interfere with each other. Applying two channels that allow the maximum channel separation will decrease the amount of channel cross-talk, and provide a noticeable performance increase over networks with minimal channel separation.

The radio frequency channels used are listed in [Table 7-3](#):

**Table 7-3. 802.11 Radio Frequency Channels**

Channel	Center Frequency	Frequency Spread
1	2412 MHz	2399.5 MHz - 2424.5 MHz
2	2417 MHz	2404.5 MHz - 2429.5 MHz
3	2422 MHz	2409.5 MHz - 2434.5 MHz
4	2427 MHz	2414.5 MHz - 2439.5 MHz
5	2432 MHz	2419.5 MHz - 2444.5 MHz
6	2437 MHz	2424.5 MHz - 2449.5 MHz
7	2442 MHz	2429.5 MHz - 2454.5 MHz
8	2447 MHz	2434.5 MHz - 2459.5 MHz
9	2452 MHz	2439.5 MHz - 2464.5 MHz
10	2457 MHz	2444.5 MHz - 2469.5 MHz

**Table 7-3. 802.11 Radio Frequency Channels**

Channel	Center Frequency	Frequency Spread
11	2462 MHz	2449.5 MHz - 2474.5 MHz
12	2467 MHz	2454.5 MHz - 2479.5 MHz
13	2472 MHz	2459.5 MHz - 2484.5 MHz

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

The preferred channel separation between the channels in neighboring wireless networks is 25 MHz (5 channels). This means that you can apply up to three different channels within your wireless network. There are only 11 usable wireless channels in the United States. It is recommended that you start using channel 1 and grow to use channel 6, and 11 when necessary, as these three channels do not overlap.

## 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 as described in [Table 7-4](#).

**Table 7-4. 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 and Crossover Cables

In the wiring table, the concept of transmit and receive are from the perspective of the PC. For example, the PC transmits on pins 1 and 2. At the hub, the perspective is reversed, and the hub receives on pins 1 and 2. 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. 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. The second method is to use a crossover cable, which 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", 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.



# Appendix C

## Preparing Your Network to Work with a Router

This appendix describes how to prepare your network to connect to the Internet through a router and how to verify the readiness of your broadband Internet service from an Internet service provider (ISP).



**Note:** If your computer was configured during the installation of a broadband modem, or using instructions provided by your ISP, you may need to copy the ISP configuration information for use in the configuration of your router. Write down this information before reconfiguring your computers. Refer to [“Obtaining ISP Configuration Information for Windows Computers”](#) on page C-19 or [“Obtaining ISP Configuration Information for Macintosh Computers”](#) on page C-20 for further information.

### What You Need To Use a Router with a Broadband Modem

---

You need to prepare these three things before you begin:

#### Cabling and Computer Hardware

To use the router on your network, each computer must have an 802.11g or 802.11b wireless adapter or an installed Ethernet Network Interface Card (NIC) and an Ethernet cable. If the computer will connect to your network using an Ethernet NIC at 100 Mbps, you must use a Category 5 (Cat 5) cable such as the one provided with your router. The cable or DSL broadband modem must provide a standard 10 Mbps (10BASE-T) or 100 Mbps (100BASE-Tx) Ethernet interface.

#### Computer Network Configuration Requirements

The router includes a built-in Web Configuration Manager. To access the configuration menus on the router, you must use a Java-enabled Web browser program that supports HTTP uploads such as Microsoft Internet Explorer or Netscape Navigator. Use Internet Explorer or Netscape Navigator 4.0 or above.

For the initial setup of your router, you will need to connect a computer to the router. This computer has to be set to automatically get its TCP/IP configuration from the router via DHCP.

**Note:** For help with DHCP configuration, please use the *Windows TCP/IP Configuration Tutorials* on the Resource CD.

## Internet Configuration Requirements

Depending on how your Internet service set up your account, you may need one or more of these configuration parameters to connect your router to the Internet:

- Host and Domain Names
- ISP Login Name and Password
- ISP Domain Name Server (DNS) Addresses
- Fixed IP Address, which is also known as the Static IP Address

## Where Do I Get the Internet Configuration Parameters?

There are several ways you can gather the required Internet connection information:

- Your Internet service provides all the information needed to connect to the Internet. If you cannot locate this information, you can ask your Internet service provider to provide it or you can try one of the options below.
- If you have a computer already connected to the Internet, you can gather the configuration information from that computer.
  - For Windows 95/98/ME, open the Network control panel, select the TCP/IP entry for the Ethernet adapter, and click Properties. Record all the settings for each tab page.
  - For Windows 2000/XP, open the Local Area Network Connection, select the TCP/IP entry for the Ethernet adapter, and click Properties. Record all the settings for each tab page.
  - For Macintosh computers, record the settings in the TCP/IP or Network control panel.
- You may also refer to the Resource CD or the *NETGEAR Router ISP Guide*, which provides Internet connection information for many ISPs.

Once you locate your Internet configuration parameters, you may want to record them on the page below.

## Record Your Internet Connection Information

Print this page. Fill in the configuration parameters from your Internet Service Provider (ISP).

**ISP Login Name:** The login name and password are case sensitive and must be entered exactly as given by your ISP. Some ISPs use your full e-mail address as the login name. The Service Name is not required by all ISPs. If you connect using a login name and password, enter the following:

Login Name: \_\_\_\_\_

Password: \_\_\_\_\_

Service Name: \_\_\_\_\_

**Fixed or Static IP Address:** If you have a static IP address, record the following information. For example, 169.254.141.148 could be a valid IP address.

Fixed or Static Internet IP Address: \_\_\_\_\_

Gateway IP Address: \_\_\_\_\_

Subnet Mask: \_\_\_\_\_

**ISP DNS Server Addresses:** If you were given DNS server addresses, fill in the following:

Primary DNS Server IP Address: \_\_\_\_\_

Secondary DNS Server IP Address: \_\_\_\_\_

**Host and Domain Names:** Some ISPs use a specific host or domain name like CCA7324-A or home. If you have not been given host or domain names, you can use the following examples as a guide:

- If your main e-mail account with your ISP is aaa@xxx.yyy.com, then use aaa as your host name. Your ISP might call this your account, user, host, or system name.
- If your ISP's mail server is mail.xxx.yyy.com, then use xxx.yyy.com as the domain name.

ISP Host Name: \_\_\_\_\_ ISP Domain Name: \_\_\_\_\_

**For Wireless Access:** See the configuration worksheet in the *Resource Manual* for your NETGEAR wireless equipment.

## 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 IP network, each computer and the router must be assigned unique IP addresses. Each computer must also have certain other IP configuration information such as a subnet mask (netmask), a domain name server (DNS) address, and a default gateway address. In most cases, you should install TCP/IP so that the computer obtains its specific network configuration information automatically from a DHCP server during bootup.

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

TCP/IP Configuration	Current NETGEAR Standard	Previous NETGEAR Standard
Computer or workstation IP Address	192.168.1.2 through 192.168.1.254	192.168.0.2 through 192.168.0.254
Subnet mask	255.255.255.0	255.255.255.0
Gateway address for router	192.168.1.1 default address	192.168.0.1 default address

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

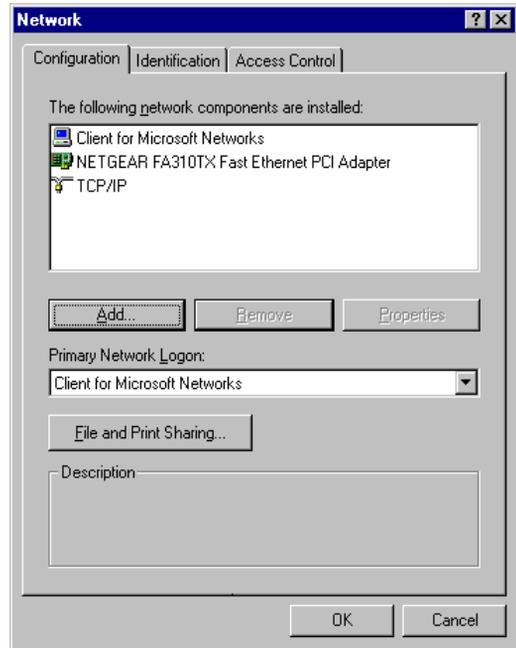
## Configuring Windows 95, 98, and Me for TCP/IP Networking

As part of the computer preparation process, you need to manually install and configure TCP/IP on each networked computer. 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 and displays a list of installed components.
3. Make sure that the following components are installed:
  - Client for Microsoft Networks
  - Ethernet Adapter
  - TCP/IP
4. The Primary Network Logon should be set to Client for Microsoft Networks.
5. If any of these items needs to be installed, follow the steps below.



**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 the Client for Microsoft Networks.

#### Installing a New Adapter

If you need to install a new adapter, follow these steps:

- 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.

### **Installing TCP/IP**

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.

### **Installing the Client for Microsoft Networks**

If you need the 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.
6. Restart your computer for the changes to take effect.

## **Enabling DHCP to Automatically Configure TCP/IP Settings in Windows 95B, 98, and Me**

After the TCP/IP protocol components are installed, each computer 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 computer to obtain the information from a DHCP server in the network.

There are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP. The following steps walk you through the configuration process for each of these versions of Windows.

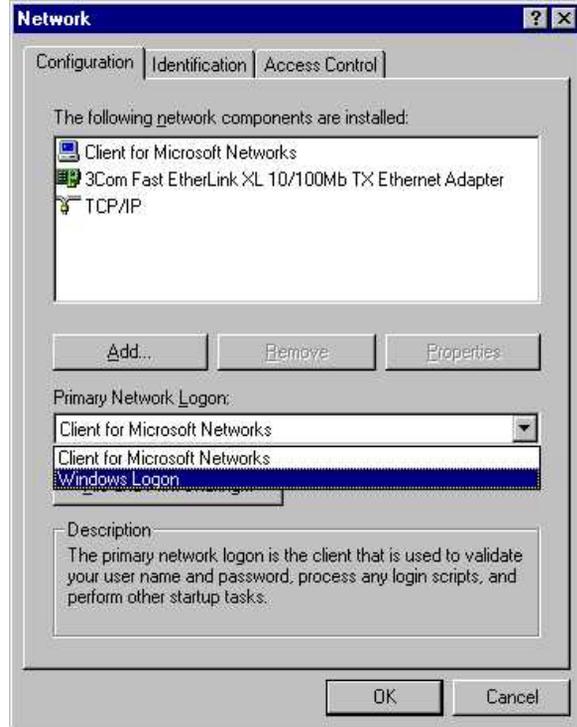
## 1. Open the Network Panel

- If the Network Neighborhood icon is on the Windows desktop, position your mouse pointer over it and right-click your mouse button.
- If the icon is not on the desktop:
  - On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
  - Locate the Network Neighborhood icon and click on it.

The Network panel opens as shown to the right.

## 2. Verify the Configuration Settings

- a. On the Configuration tab, make sure that the following components are installed:
  - Client for Microsoft Networks
  - Ethernet Adapter
  - TCP/IP
- b. The Primary Network Logon should be set to Windows Logon.



### 3. Verify the Properties IP Address Setting

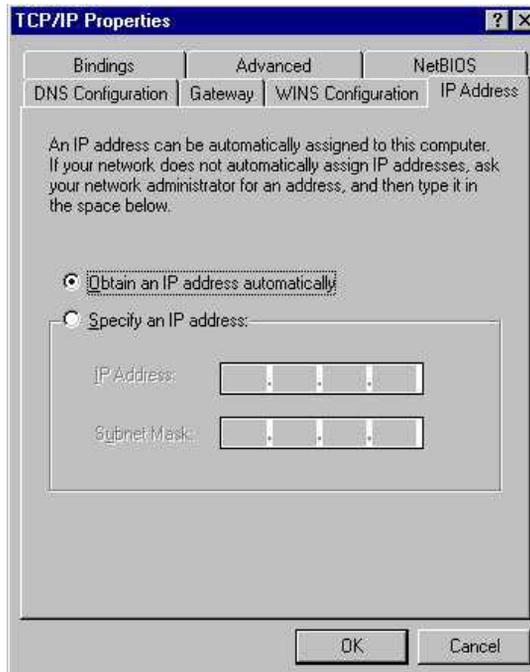
- a. Click the Properties button.

The TCP/IP Properties window displays as shown to the right. By default, the IP Address tab is open.

- b. Verify that “Obtain an IP address automatically” is selected.

If it is not selected, click the radio button to the left of it to select it. This setting is required to enable the DHCP server to automatically assign an IP address.

- c. Click OK to continue.
- d. Restart the computer.
- e. Repeat these steps for each computer with this version of Windows on your network.



## Selecting the 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. Clear all the check boxes in the LAN Internet Configuration screen and click Next.
5. Proceed to the end of the Wizard.

## Verifying TCP/IP Properties

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

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

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

- From the drop-down box, select your Ethernet adapter.

The window is updated to show your settings. They should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway:

TCP/IP Configuration	Current NETGEAR Standard	Previous NETGEAR Standard
Computer or workstation IP Address	192.168.1.2 through 192.168.1.254	192.168.0.2 through 192.168.0.254
Subnet mask	255.255.255.0	255.255.255.0
Gateway address for router	192.168.1.1 default address	192.168.0.1 default address

---

## Configuring Windows NT4, 2000 or XP for IP Networking

---

As part of the computer preparation process, you may need to install and configure TCP/IP on each networked computer. 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:

- On the Windows taskbar, click the Start button, then click Control Panel.
- Double-click the Network Connections icon.
- If an Ethernet adapter is present in your computer, you should see an entry for Local Area Connection. Double-click that entry.
- Select Properties.
- Verify that *Client for Microsoft Networks* and *Internet Protocol (TCP/IP)* are present. If not, select Install and add them.
- Select “Internet Protocol (TCP/IP)”, click Properties, and verify that “Obtain an IP address automatically” is selected.
- Click OK and close all Network and Dialup Connections windows.
- Then, restart your computer.

## Configuring DHCP of TCP/IP in Windows XP, 2000, or NT4

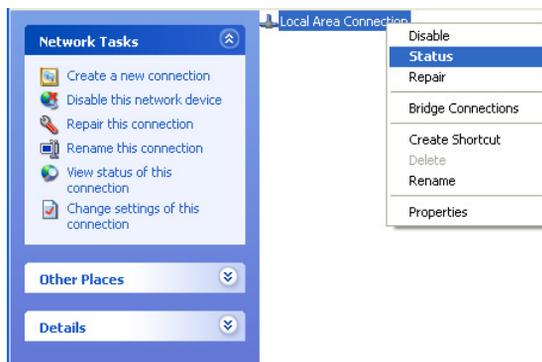
There are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP. The following steps walk you through the configuration process for each of these versions of Windows.

### DHCP Configuration of TCP/IP in Windows XP

#### 1. Open the Network Connection Window.

- a. Select Control Panel from the Windows XP Start menu.
- b. Select the Network Connections icon on the Control Panel.

The Network Connection window displays as shown here. The Connections List is located to the right of that window.

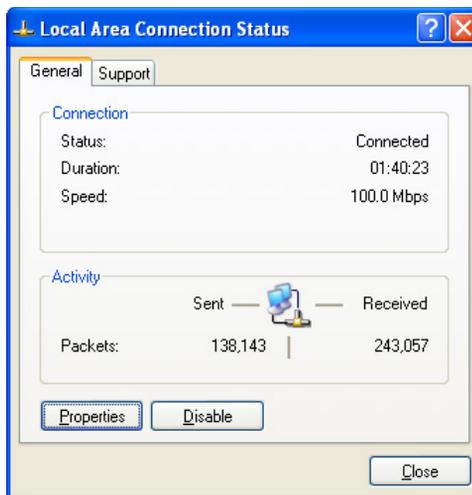


#### 2. Go to the Network Connection Status window.

**Note:** Administrator logon access rights are needed to use this window.

Double-click the Connection you will use.

The Local Area Network Connection Status window opens, as shown here. This box displays the connection status, duration, speed, and activity statistics.

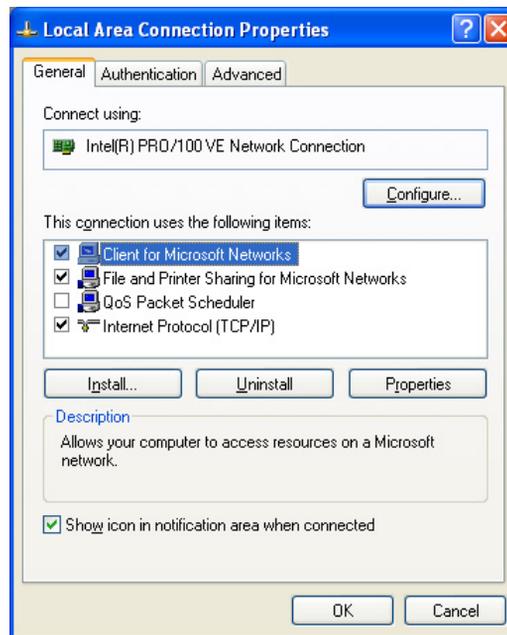


### 3. Go to Properties.

- a. Click the Properties button to view details about the connection.

The TCP/IP details are shown on the Support tab page.

- b. Select “Internet Protocol”, and click Properties to view the configuration information.



### 4. Set DHCP for TCP/IP.

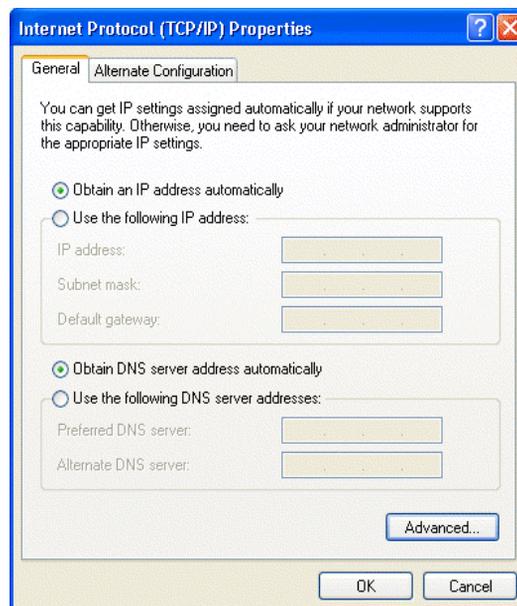
- a. Verify that the following two radio buttons are selected:

- Obtain an IP address automatically
- Obtain DNS server address automatically

- b. Click the OK button.

This completes the DHCP configuration of TCP/IP in Windows XP for this computer.

- c. Repeat these steps for each computer with this version of Windows on your network.



## DHCP Configuration of TCP/IP in Windows 2000

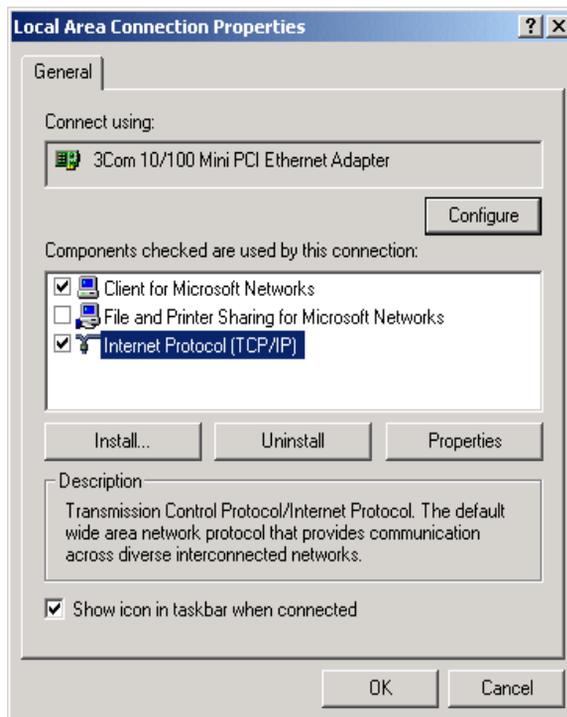
After you have installed the network card, TCP/IP for Windows 2000 is configured. TCP/IP should be added by default and set to DHCP without your having to configure it. However, if there are problems, follow these steps to configure TCP/IP with DHCP for Windows 2000.

### 1. Check the Local Area Connection Properties Settings.

- a. Click the My Network Places icon on the Windows desktop. The Network and Dial-up Connections window opens.
- b. Right click on “Local Area Connection” and select Properties.

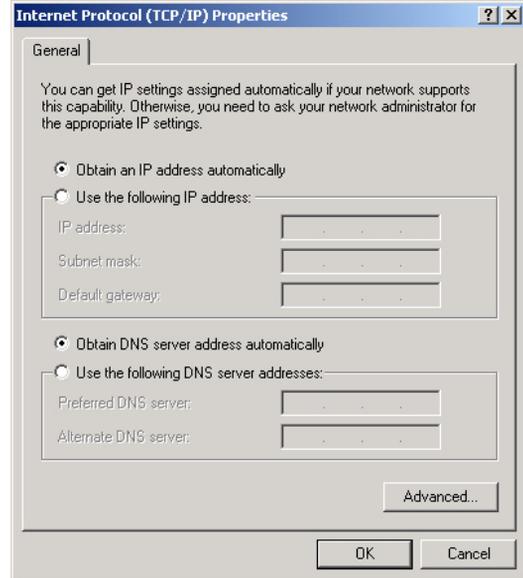
The Local Area Connection Properties dialog box appears, as shown to the right.

- c. Verify that you have the correct Ethernet card selected in the “Connect using:” box.
- d. Verify that at least the following two items are displayed and selected in the “Components checked are used by this connection:” box:
  - Client for Microsoft Networks
  - Internet Protocol (TCP/IP)
- e. Click OK.



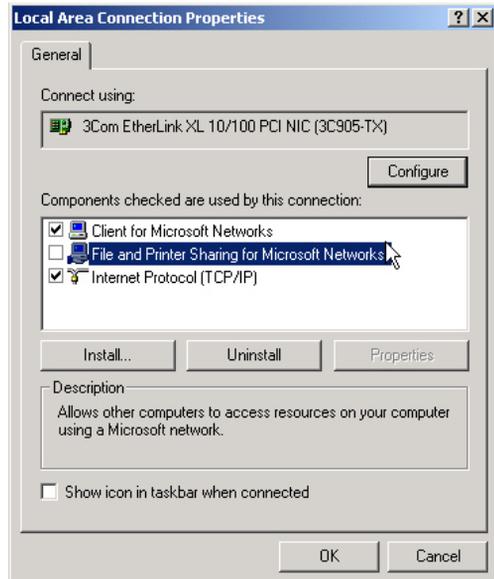
## 2. Check the Internet Protocol Properties.

- a. With “Internet Protocol (TCP/IP)” selected, click Properties to open the Internet Protocol (TCP/IP) Properties dialog box.
- b. Verify that the following items are selected:
  - Obtain an IP address automatically
  - Obtain DNS server address automatically
- c. Click OK to return to Local Area Connection Properties.



## 3. Complete the configuration.

- a. Click OK again to complete the configuration process for Windows 2000.
- b. Restart the computer.
- c. Repeat these steps for each computer with this version of Windows on your network.

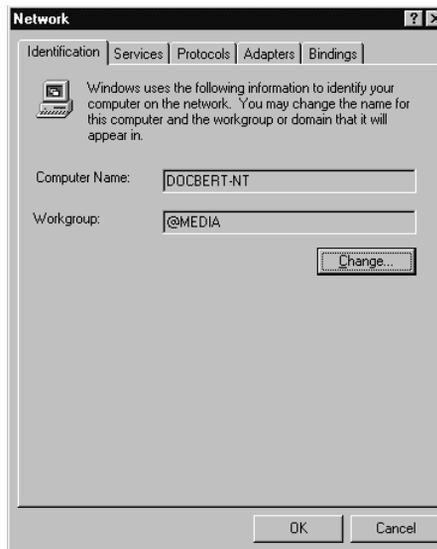


## DHCP Configuration of TCP/IP in Windows NT4

Once you have installed the network card, you need to configure the TCP/IP environment for Windows NT 4.0. Follow this procedure to configure TCP/IP with DHCP in Windows NT 4.0.

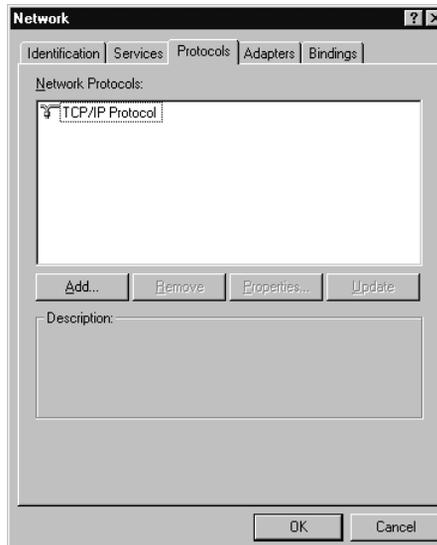
### 1. Open the Network panel.

- a. Choose Settings from the Start menu.
- b. Select Control Panel to display Control Panel window.
- c. Double-click the Network icon to display the Network panel, as shown to the right.



### 2. Go to TCP/IP Properties.

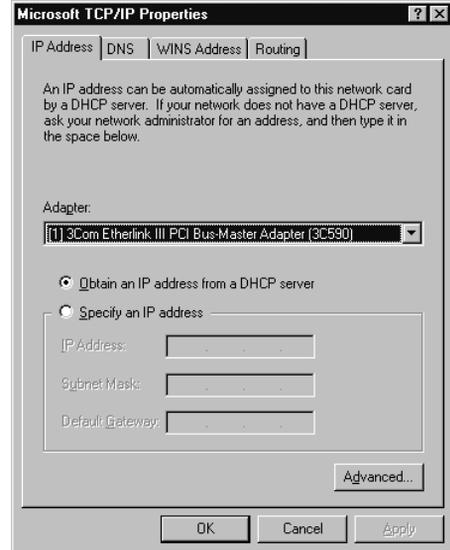
- a. Select the Protocols tab.
- b. Select "TCP/IP Protocol" in the Network Protocols box, and click the Properties button.



### 3. Set the TCP/IP Properties.

The TCP/IP Properties dialog box displays.

- a. Click the IP Address tab.
- b. Select the radio button marked “Obtain an IP address from a DHCP server”.
- c. Click OK. This completes the configuration of TCP/IP in Windows NT for this computer.
- d. Restart the computer.
- e. Repeat these steps for each computer with this version of Windows on your network.



## Verifying TCP/IP Properties for Windows XP, 2000, and NT4

To check your computer’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 is listed, and should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway.

TCP/IP Configuration	Current NETGEAR Standard	Previous NETGEAR Standard
Computer or workstation IP Address	192.168.1.2 through 192.168.1.254	192.168.0.2 through 192.168.0.254
Subnet mask	255.255.255.0	255.255.255.0
Gateway address for router	192.168.1.1 default address	192.168.0.1 default address

4. Type `exit`

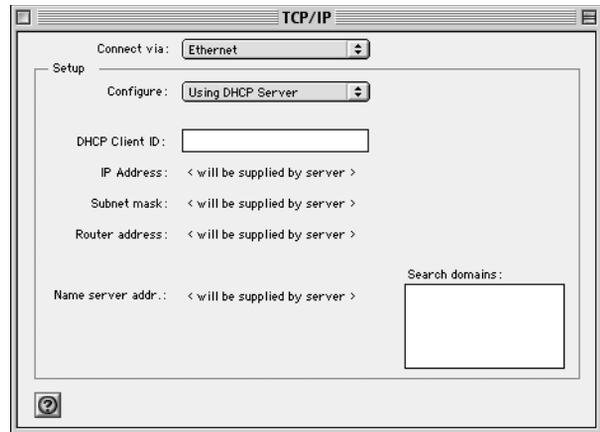
## Configuring the Macintosh for TCP/IP Networking

---

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

### MacOS 8.6 or 9.x

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



### MacOS X

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 TCP/IP Properties for Macintosh Computers

To check the TCP/IP configuration after you configured and rebooted your Macintosh, return to the TCP/IP Control Panel. From the Apple menu, select Control Panels, then TCP/IP.

The panel is updated to show your settings. They should match the values in the chart below if you are using the default TCP/IP settings that NETGEAR recommends.

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 switch back again to *Using DHCP Server*.

TCP/IP Configuration	Current NETGEAR Standard	Previous NETGEAR Standard
Computer or workstation IP Address	192.168.1.2 through 192.168.1.254	192.168.0.2 through 192.168.0.254
Subnet mask	255.255.255.0	255.255.255.0
Gateway address for router	192.168.1.1 default address	192.168.0.1 default address

## Verifying the Readiness of Your Internet Account

---

For broadband 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 computer. With a typical account, much of the configuration information is dynamically assigned when your computer 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 computer, and you need to configure it with the TCP/IP information that the single computer would normally use. When the router's Internet port is connected to the broadband modem, the router appears to be a single computer to the ISP. The router then allows the computers on the local network to masquerade as the single computer to access the Internet through the broadband modem. The method used by the router to accomplish this is called Network Address Translation (NAT) or IP masquerading.

## 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 Point-to-Point Protocol over Ethernet (PPPoE).

When you configure your router, you need to enter your login name and password in the router's configuration menus. 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 computer. 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 computer during the installation of the broadband modem, or if you configured it using instructions provided by your ISP, you need to copy the configuration information from your computer's Network TCP/IP Properties window or Macintosh TCP/IP Control Panel before reconfiguring your computer for use with the router. These procedures are described next.

## Obtaining ISP Configuration Information for Windows Computers

You may need configuration information from your computer in order to configure the router. You only need to collect this information if you have a static IP address (your ISP does not dynamically supply the account information).

To get the information you need to configure the router for Internet access follow the steps below. The selections vary somewhat according to which version of Windows you are running.

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 and 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 computer at the prompt. You may also be prompted to insert your Windows CD.

## Obtaining ISP Configuration Information for Macintosh Computers

You may need configuration information from your computer in order to configure the router. You only need to collect this information if you have a static IP address (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, and 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 have set up your computers to work with the router, you must reset the network for the devices to be able to communicate correctly. Restart any computer that is connected to the router.

After you configure all of your computers for TCP/IP networking, restart them, and connect them to the local network of your router. Then you are ready to access and configure the router.

# Appendix D

## Wireless Networking Basics

### Wireless Networking Overview

---

The CG814WG v2 Gateway conforms to the Institute of Electrical and Electronics Engineers (IEEE) 802.11g standard for wireless LANs (WLANs). On an 802.11 wireless link, data is encoded using direct-sequence spread-spectrum (DSSS) technology and is transmitted in the unlicensed radio spectrum at 2.5GHz. The maximum data rate for the 802.11g wireless link is 54 Mbps, but it will automatically back down from 54 Mbps when the radio signal is weak or when interference is detected.

The 802.11 standard is also called Wireless Ethernet or Wi-Fi by the Wireless Ethernet Compatibility Alliance (WECA, see <http://www.wi-fi.net>), an industry standard group promoting interoperability among 802.11 devices. The 802.11 standard offers two methods for configuring a wireless network—ad hoc and infrastructure.

### 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.

## 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.

## Network Name: 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 ESSID is used, but may still be referred to as SSID.

An SSID is a thirty-two character (maximum) alphanumeric key identifying the name of 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.

## Wireless Channels

IEEE 802.11 g/b wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4 GHz and 2.5 GHz. Neighboring channels are 5 MHz apart. However, due to spread spectrum effect of the signals, a node sending signals using a particular channel will utilize frequency spectrum 12.5 MHz above and below the center channel frequency. As a result, two separate wireless networks using neighboring channels (for example, channel 1 and channel 2) in the same general vicinity will interfere with each other. Applying two channels that allow the maximum channel separation will decrease the amount of channel cross-talk, and provide a noticeable performance increase over networks with minimal channel separation.

The radio frequency channels used are listed in [Table D-1](#):

**Table D-1. 802.11g Radio Frequency Channels**

Channel	Center Frequency	Frequency Spread
1	2412 MHz	2399.5 MHz - 2424.5 MHz
2	2417 MHz	2404.5 MHz - 2429.5 MHz
3	2422 MHz	2409.5 MHz - 2434.5 MHz
4	2427 MHz	2414.5 MHz - 2439.5 MHz
5	2432 MHz	2419.5 MHz - 2444.5 MHz
6	2437 MHz	2424.5 MHz - 2449.5 MHz
7	2442 MHz	2429.5 MHz - 2454.5 MHz
8	2447 MHz	2434.5 MHz - 2459.5 MHz
9	2452 MHz	2439.5 MHz - 2464.5 MHz
10	2457 MHz	2444.5 MHz - 2469.5 MHz
11	2462 MHz	2449.5 MHz - 2474.5 MHz
12	2467 MHz	2454.5 MHz - 2479.5 MHz
13	2472 MHz	2459.5 MHz - 2484.5 MHz

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

The preferred channel separation between the channels in neighboring wireless networks is 25 MHz (5 channels). This means that you can apply up to three different channels within your wireless network. There are only 11 usable wireless channels in the United States. It is recommended that you start using channel 1 and grow to use channel 6, and 11 when necessary, as these three channels do not overlap.

## WEP Wireless Security

---

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 computer can join any network and receive any messages that are not encrypted. With Shared Key authentication, only those computers that possess the correct authentication key can join the network. By default, IEEE 802.11 wireless devices operate in an Open System network. Recently, Wi-Fi, the Wireless Ethernet Compatibility Alliance (<http://www.wi-fi.net>) developed the Wi-Fi Protected Access (WPA), a new strongly enhanced Wi-Fi security. WPA will soon be incorporated into the IEEE 802.11 standard. WEP and WPA are discussed below.

### WEP Authentication

The 802.11 standard defines several services that govern how two 802.11 devices communicate. The following events must occur before an 802.11 Station can communicate with an Ethernet network through an access point such as the one built in to the CG814WG v2:

1. Turn on the wireless station.
2. The station listens for messages from any access points that are in range.
3. The station finds a message from an access point that has a matching SSID.
4. The station sends an authentication request to the access point.
5. The access point authenticates the station.
6. The station sends an association request to the access point.
7. The access point associates with the station.
8. The station can now communicate with the Ethernet network through the access point.

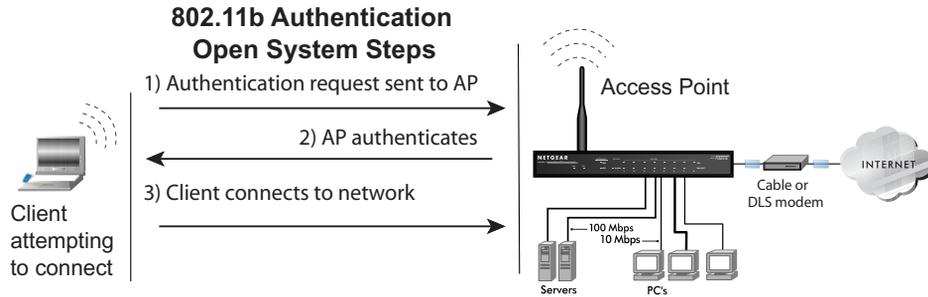
An access point must authenticate a station before the station can associate with the access point or communicate with the network. The IEEE 802.11 standard defines two types of WEP authentication: Open System and Shared Key.

- Open System Authentication allows any device to join the network, assuming that the device SSID matches the access point SSID. Alternatively, the device can use the “ANY” SSID option to associate with any available access point within range, regardless of its SSID.

- Shared Key Authentication requires that the station and the access point have the same WEP Key to authenticate. These two authentication procedures are described below.

## WEP Open System Authentication

This process is illustrated below.



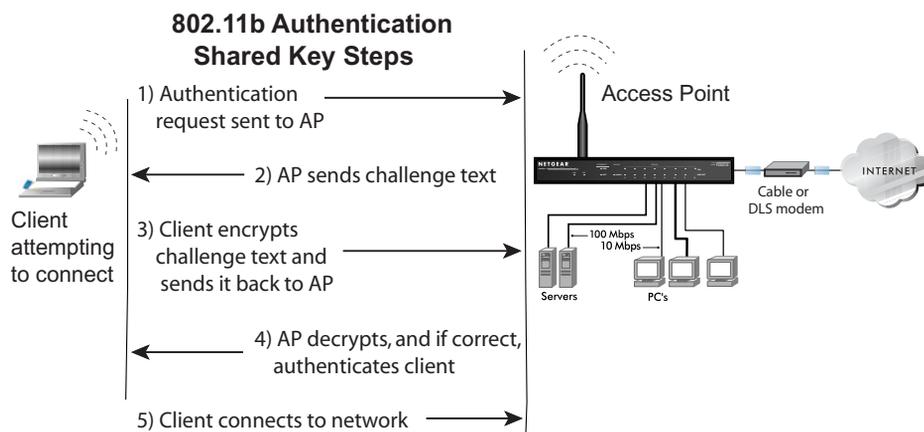
**Figure D-1: 802.11 open system authentication**

The following steps occur when two devices use Open System Authentication:

1. The station sends an authentication request to the access point.
2. The access point authenticates the station.
3. The station associates with the access point and joins the network.

## WEP Shared Key Authentication

This process is illustrated below.



**Figure D-2: 802.11 shared key authentication**

The following steps occur when two devices use Shared Key Authentication:

1. The station sends an authentication request to the access point.
2. The access point sends challenge text to the station.
3. The station uses its configured 64-bit or 128-bit default key to encrypt the challenge text, and sends the encrypted text to the access point.
4. The access point decrypts the encrypted text using its configured WEP key that corresponds to the station's default key. The access point compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, then the access point and the station share the same WEP key and the access point authenticates the station.
5. The station connects to the network.

If the decrypted text does not match the original challenge text (i.e., the access point and station do not share the same WEP key), then the access point will refuse to authenticate the station and the station will be unable to communicate with either the 802.11 network or Ethernet network.

## Key Size and Configuration

The IEEE 802.11 standard supports two types of WEP encryption: 40-bit and 128-bit.

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 user-configurable bits. Similar to the 40-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.

The 128-bit encryption is stronger than 40-bit encryption, but 128-bit encryption may not be available outside of the United States due to U.S. export regulations.

When configured for 40-bit encryption, 802.11 products typically support up to four WEP keys. Each 40-bit WEP Key is expressed as five sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90” is a 40-bit WEP key.

When configured for 128-bit encryption, 802.11g products typically support four WEP keys but some manufacturers support only one 128-bit key. The 128-bit WEP Key is expressed as 13 sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90 AB CD EF 12 34 56 78 90” is a 128-bit WEP key.

Typically, 802.11 access points can store up to four 128-bit WEP Keys but some 802.11 client adapters can only store one. Therefore, make sure that your 802.11 access and client adapters configurations match.

Whatever keys you enter for an access point, you must also enter the same keys for the client adapter in the same order. In other words, WEP key 1 on the AP must match WEP key 1 on the client adapter, WEP key 2 on the AP must match WEP key 2 on the client adapter, etc.

**Note:** The access point and the client adapters can have different default WEP keys as long as the keys are in the same order. In other words, the AP can use WEP key 2 as its default key to transmit while a client adapter can use WEP key 3 as its default key to transmit. The two devices will communicate as long as the access point’s WEP key 2 is the same as the client’s WEP key 2 and the AP’s WEP key 3 is the same as the client’s WEP key 3.

## How to Use WEP Parameters

Wired Equivalent Privacy (WEP) data encryption is used when the wireless devices are configured to operate in Shared Key authentication mode. There are two shared key methods implemented in most commercially available products, 64-bit and 128-bit WEP data encryption.

Before enabling WEP on an 802.11 network, you must first consider what type of encryption you require and the key size you want to use. Typically, there are three WEP Encryption options available for 802.11 products:

1. **Do Not Use WEP:** The 802.11 network does not encrypt data. For authentication purposes, the network uses Open System Authentication.
2. **Use WEP for Encryption:** A transmitting 802.11 device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving 802.11g device decrypts the data using the same WEP Key. For authentication purposes, the 802.11g network uses Open System Authentication.
3. **Use WEP for Authentication and Encryption:** A transmitting 802.11 device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving 802.11 device decrypts the data using the same WEP Key. For authentication purposes, the 802.11 network uses Shared Key Authentication.

**Note:** Some 802.11 access points also support **Use WEP for Authentication Only** (Shared Key Authentication without data encryption). However, the CG814WG v2 does not offer this option.

## WPA Wireless Security

---

Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements that increase the level of data protection and access control for existing and future wireless LAN systems.

The IEEE introduced the WEP as an optional security measure to secure 802.11g (Wi-Fi) WLANs, but inherent weaknesses in the standard soon became obvious. In response to this situation, the Wi-Fi Alliance announced a new security architecture in October 2002 that remedies the shortcomings of WEP. This standard, formerly known as Safe Secure Network (SSN), is designed to work with existing 802.11 products and offers forward compatibility with 802.11i, the new wireless security architecture being defined in the IEEE.

WPA offers the following benefits:

- Enhanced data privacy
- Robust key management
- Data origin authentication
- Data integrity protection

Starting in August of 2003, all new Wi-Fi certified products had to support WPA and all existing Wi-Fi certified products had one year to comply with the new standard or lose their Wi-Fi certification. NETGEAR has implemented WPA on client and access point products. As of August 2004, all Wi-Fi certified products must support WPA.

## How Does WPA Compare to WEP?

WEP is a data encryption method and is not intended as a user authentication mechanism. WPA user authentication is implemented using 802.1x and the Extensible Authentication Protocol (EAP). Support for 802.1x authentication is required in WPA. In the 802.11 standard, 802.1x authentication was optional. For details on EAP specifically, refer to IETF's RFC 2284.

With 802.11 WEP, all access points and client wireless adapters on a particular wireless LAN must use the same encryption key. A major problem with the 802.11 standard is that the keys are cumbersome to change. If you don't update the WEP keys often, an unauthorized person with a sniffing tool can monitor your network for less than a day and decode the encrypted messages. Products based on the 802.11 standard alone offer system administrators no effective method to update the keys.

For 802.11, WEP encryption is optional. For WPA, encryption using Temporal Key Integrity Protocol (TKIP) is required. TKIP replaces WEP with a new encryption algorithm that is stronger than the WEP algorithm, but that uses the calculation facilities present on existing wireless devices to perform encryption operations. TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. Through these enhancements, TKIP addresses all of known WEP vulnerabilities.

## How Does WPA Compare to IEEE 802.11i?

WPA is forward compatible with the IEEE 802.11i security specification currently under development. WPA is a subset of the current 802.11i draft and uses certain pieces of the 802.11i draft that were ready to bring to market in 2003, such as 802.1x and TKIP. The main pieces of the 802.11i draft that are not included in WPA are secure IBSS (Ad-Hoc mode), secure fast handoff (for specialized 802.11 VoIP phones), as well as enhanced encryption protocols such as AES-CCMP. These features are either not yet ready for market or will require hardware upgrades to implement.

## What are the Key Features of WPA Security?

The following security features are included in the WPA standard:

- WPA Authentication
- WPA Encryption Key Management
  - Temporal Key Integrity Protocol (TKIP)
  - Michael message integrity code (MIC)
  - AES Support
- Support for a Mixture of WPA and WEP Wireless Clients

These features are discussed below.

WPA addresses most of the known WEP vulnerabilities and is primarily intended for wireless infrastructure networks as found in the enterprise. This infrastructure includes stations, access points, and authentication servers (typically RADIUS servers). The RADIUS server holds (or has access to) user credentials (e.g., user names and passwords) and authenticates wireless users before they gain access to the network.

The strength WPA comes from an integrated sequence of operations that encompass 802.1X/EAP authentication and sophisticated key management and encryption techniques. Its major operations include:

- **Network security capability determination.** This occurs at the 802.11 level and is communicated through WPA information elements in Beacon, Probe Response, and (Re) Association Requests. Information in these elements includes the authentication method (802.1X or Pre-shared key) and the preferred cipher suite (WEP, TKIP, or AES).

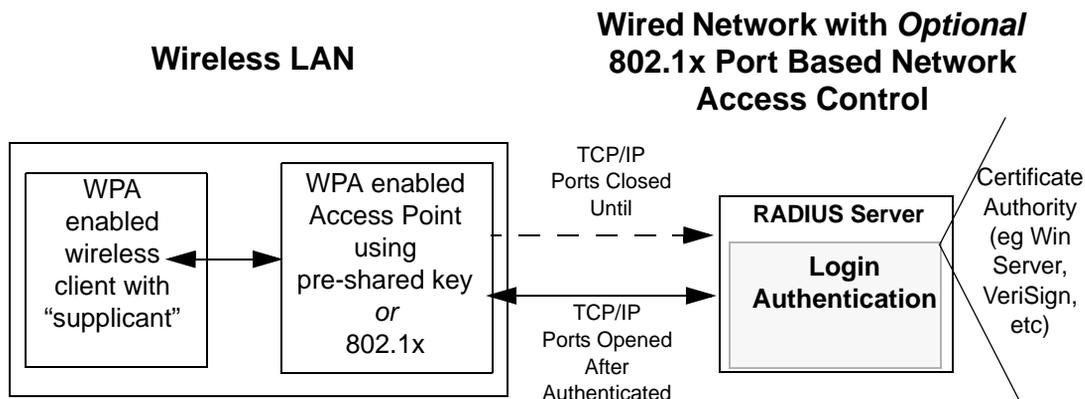
The primary information conveyed in the Beacon frames is the authentication method and the cipher suite. Possible authentication methods include 802.1X and Pre-shared key. Pre-shared key is an authentication method that uses a statically configured passphrase on both the stations and the access point. This removes the need for an authentication server, which in many home and small office environments will not be available nor desirable. Possible cipher suites include: WEP, TKIP, and AES (Advanced Encryption Standard). We'll talk more TKIP and AES when addressing data privacy below.

- **Authentication. EAP over 802.1X is used for authentication.** Mutual authentication is gained by choosing an EAP type supporting this feature and is required by WPA. The 802.1X port access control prevents full access to the network until authentication completes. The 802.1X EAPOL-Key packets are used by WPA to distribute per-session keys to those stations successfully authenticated.

The supplicant in the station uses the authentication and cipher suite information contained in the information elements to decide which authentication method and cipher suite to use. For example, if the access point is using the Pre-shared key method then the supplicant need not authenticate using full-blown 802.1X. Rather, the supplicant must simply prove to the access point that it is in possession of the pre-shared key. If the supplicant detects that the service set does not contain a WPA information element then it knows it must use pre-WPA 802.1X authentication and key management in order to access the network.

- **Key management.** WPA features a robust key generation/management system that integrates the authentication and data privacy functions. Keys are generated after successful authentication and through a subsequent four-way handshake between the station and access point (AP).
- **Data Privacy (Encryption).** Temporal Key Integrity Protocol (TKIP) is used to wrap WEP in sophisticated cryptographic and security techniques to overcome most of its weaknesses.
- **Data integrity.** TKIP includes a message integrity code (MIC) at the end of each plain text message to ensure messages are not being spoofed.

## WPA Authentication: Enterprise-level User Authentication via 802.1x/EAP and RADIUS



**Figure D-3: WPA Overview**

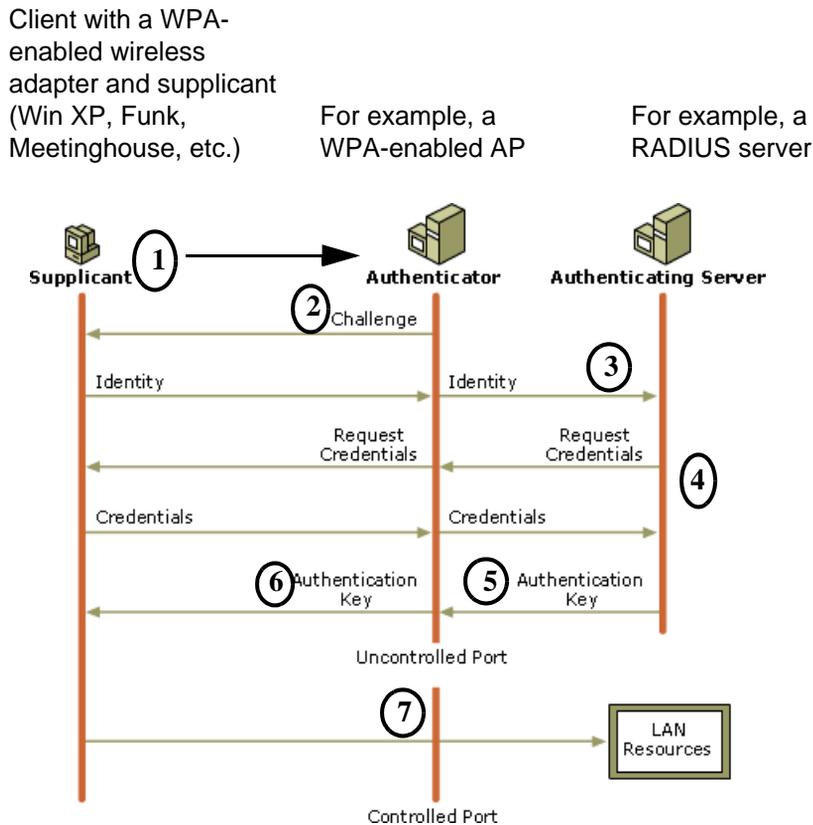
IEEE 802.1x offers an effective framework for authenticating and controlling user traffic to a protected network, as well as providing a vehicle for dynamically varying data encryption keys via EAP from a RADIUS server, for example. This framework enables using a central authentication server, which employs mutual authentication so that a rogue wireless user does not join the network.

It's important to note that 802.1x doesn't provide the actual authentication mechanisms. When using 802.1x, the EAP type, such as Transport Layer Security (EAP-TLS) or EAP Tunneled Transport Layer Security (EAP-TTLS) defines how the authentication takes place.

**Note:** For environments with a Remote Authentication Dial-In User Service (RADIUS) infrastructure, WPA supports Extensible Authentication Protocol (EAP). For environments without a RADIUS infrastructure, WPA supports the use of a preshared key.

Together, these technologies provide a framework for strong user authentication.

Windows XP implements 802.1x natively, and several Netgear switch and wireless access point products support 802.1x.



**Figure D-4: 802.1x Authentication Sequence**

The access point (AP) sends Beacon Frames with WPA information elements to the stations in the service set. Information elements include the required authentication method (802.1x or Pre-shared key) and the preferred cipher suite (WEP, TKIP, or AES). Probe Responses (AP to station) and Association Requests (station to AP) also contain WPA information elements.

1. Initial 802.1x communications begin with an unauthenticated supplicant (i.e., client device) attempting to connect with an authenticator (i.e., 802.11 access point). The client sends an EAP-start message. This begins a series of message exchanges to authenticate the client.
2. The access point replies with an EAP-request identity message.

3. The client sends an EAP-response packet containing the identity to the authentication server. The access point responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the access point. The access point blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the access point can verify the client's identity using an authentication server (e.g., RADIUS).
4. The authentication server uses a specific authentication algorithm to verify the client's identity. This could be through the use of digital certificates or some other EAP authentication type.
5. The authentication server will either send an accept or reject message to the access point.
6. The access point sends an EAP-success packet (or reject packet) to the client.
7. If the authentication server accepts the client, then the access point will transition the client's port to an authorized state and forward additional traffic.

The important part to know at this point is that the software supporting the specific EAP type resides on the authentication server and within the operating system or application “supplicant” software on the client devices. The access point acts as a “pass through” for 802.1x messages, which means that you can specify any EAP type without needing to upgrade an 802.1x-compliant access point. As a result, you can update the EAP authentication type to such devices as token cards (Smart Cards), Kerberos, one-time passwords, certificates, and public key authentication or as newer types become available and your requirements for security change.

### **WPA Data Encryption Key Management**

With 802.1x, the rekeying of unicast encryption keys is optional. Additionally, 802.11 and 802.1x provide no mechanism to change the global encryption key used for multicast and broadcast traffic. With WPA, rekeying of both unicast and global encryption keys is required.

For the unicast encryption key, the Temporal Key Integrity Protocol (TKIP) changes the key for every frame, and the change is synchronized between the wireless client and the wireless access point (AP). For the global encryption key, WPA includes a facility (the Information Element) for the wireless AP to advertise the changed key to the connected wireless clients.

If configured to implement dynamic key exchange, the 802.1x authentication server can return session keys to the access point along with the accept message. The access point uses the session keys to build, sign and encrypt an EAP key message that is sent to the client immediately after sending the success message. The client can then use contents of the key message to define applicable encryption keys. In typical 802.1x implementations, the client can automatically change encryption keys as often as necessary to minimize the possibility of eavesdroppers having enough time to crack the key in current use.

## **Temporal Key Integrity Protocol (TKIP)**

WPA uses TKIP to provide important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. TKIP also provides for the following:

- The verification of the security configuration after the encryption keys are determined.
- The synchronized changing of the unicast encryption key for each frame.
- The determination of a unique starting unicast encryption key for each preshared key authentication.

### **Michael**

With 802.11 and WEP, data integrity is provided by a 32-bit *integrity check value* (ICV) that is appended to the 802.11 payload and encrypted with WEP. Although the ICV is encrypted, you can use cryptanalysis to change bits in the encrypted payload and update the encrypted ICV without being detected by the receiver.

With WPA, a method known as *Michael* specifies a new algorithm that calculates an 8-byte *message integrity code* (MIC) using the calculation facilities available on existing wireless devices. The MIC is placed between the data portion of the IEEE 802.11 frame and the 4-byte ICV. The MIC field is encrypted together with the frame data and the ICV.

Michael also provides replay protection. A new frame counter in the IEEE 802.11 frame is used to prevent replay attacks.

### **AES Support**

One of the encryption methods supported by WPA beside TKIP is the advanced encryption standard (AES), although AES support will not be required initially for Wi-Fi certification. This is viewed as the optimal choice for security conscience organizations, but the problem with AES is that it requires a fundamental redesign of the NIC's hardware in both the station and the access point. TKIP was a pragmatic compromise that allows organizations to deploy better security while AES capable equipment is being designed, manufactured, and incrementally deployed.

## Is WPA Perfect?

WPA is not without its vulnerabilities. Specifically, it is susceptible to denial of service (DoS) attacks. If the access point receives two data packets that fail the Message Integrity Code (MIC) check within 60 seconds of each other then the network is under an active attack, and as a result, the access point employs counter measures, which includes disassociating each station using the access point. This prevents an attacker from gleaning information about the encryption key and alerts administrators, but it also causes users to lose network connectivity for 60 seconds. More than anything else, this may just prove that no single security tactic is completely invulnerable. WPA is a definite step forward in WLAN security over WEP and has to be thought of as a single part of an end-to-end network security strategy.

## Product Support for WPA

Starting in August, 2003, NETGEAR, Inc. wireless Wi-Fi certified products will support the WPA standard. NETGEAR, Inc. wireless products that had their Wi-Fi certification approved before August, 2003 will have one year to add WPA so as to maintain their Wi-Fi certification.

WPA requires software changes to the following:

- Wireless access points
- Wireless network adapters
- Wireless client programs

## Supporting a Mixture of WPA and WEP Wireless Clients

To support the gradual transition of WEP-based wireless networks to WPA, a wireless AP can support both WEP and WPA clients at the same time. During the association, the wireless AP determines which clients use WEP and which clients use WPA. The disadvantage to supporting a mixture of WEP and WPA clients is that the global encryption key is not dynamic. This is because WEP-based clients cannot support it. All other benefits to the WPA clients, such as integrity, are maintained.

However, a mixed mode supporting WPA and non-WPA clients would offer network security that is no better than that obtained with a non-WPA network, and thus this mode of operation is discouraged.

## Changes to Wireless Access Points

Wireless access points must have their firmware updated to support the following:

- **The new WPA information element**

To advertise their support of WPA, wireless APs send the beacon frame with a new 802.11 WPA information element that contains the wireless AP's security configuration (encryption algorithms and wireless security configuration information).

- **The WPA two-phase authentication**

Open system, then 802.1x (EAP with RADIUS or preshared key).

- **TKIP**

- **Michael**

- **AES** (optional)

To upgrade your wireless access points to support WPA, obtain a WPA firmware update from your wireless AP vendor and upload it to your wireless AP.

## Changes to Wireless Network Adapters

Wireless network adapters must have their firmware updated to support the following:

- **The new WPA information element**

Wireless clients must be able to process the WPA information element and respond with a specific security configuration.

- **The WPA two-phase authentication**

Open system, then 802.1x (EAP or preshared key).

- **TKIP**

- **Michael**

- **AES** (optional)

To upgrade your wireless network adapters to support WPA, obtain a WPA update from your wireless network adapter vendor and update the wireless network adapter driver.

For Windows wireless clients, you must obtain an updated network adapter driver that supports WPA. For wireless network adapter drivers that are compatible with Windows XP (Service Pack 1) and Windows Server 2003, the updated network adapter driver must be able to pass the adapter's WPA capabilities and security configuration to the Wireless Zero Configuration service.

Microsoft has worked with many wireless vendors to embed the WPA firmware update in the wireless adapter driver. So, to update you Windows wireless client, all you have to do is obtain the new WPA-compatible driver and install the driver. The firmware is automatically updated when the wireless network adapter driver is loaded in Windows.

## **Changes to Wireless Client Programs**

Wireless client programs must be updated to permit the configuration of WPA authentication (and preshared key) and the new WPA encryption algorithms (TKIP and the optional AES component).

To obtain the Microsoft WPA client program, visit the Microsoft Web site.

# 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>802.11b</b>	IEEE specification for wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz.
<b>802.11g</b>	IEEE specification for wireless networking at 54Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz.
<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>DSLAM</b>	DSL Access Multiplexor. The piece of equipment at the telephone company central office that provides the ADSL signal.
<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>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>MTU</b>	<i>See</i> Maximum Transmission Unit.
<b>Maximum Transmit</b>	The size in bytes of the largest packet that can be sent or received.
<b>Unit</b>	
<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>PPPoA</b>	<i>See</i> PPP over ATM
<b>PPPoE</b>	<i>See</i> PPP over Ethernet
<b>PPP over ATM</b>	PPPoA. PPP over ATM is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
<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>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>VCI</b>	Virtual Channel Identifier. Together with the VPI, defines a Virtual Channel through an ATM network. Used by ATM switching equipment to route data through the network.
<b>VPI</b>	Virtual Path Identifier. Together with the VCI, defines a Virtual Channel through an ATM network. Used by ATM switching equipment to route data through the network.
<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.