Wireless-G Router WGR614v10 Reference Manual

NETGEAR

Technical Support

Please refer to the support information card that shipped with your product. When you register your product at *http://www.netgear.com/register*, we can provide you with faster expert technical support and timely notices of product and software upgrades.

NETGEAR, INC. Support Information

Phone: 1-888-NETGEAR, for US & Canada only. For other countries, see your Support information card.

E-mail: support@netgear.com

North American NETGEAR website: *http://www.netgear.com*

Trademarks

NETGEAR, the NETGEAR logo, ProSafe, and Auto Uplink are trademarks or registered trademarks of NETGEAR, Inc. Microsoft, Windows, Windows NT and Vista 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.

Wireless Communications

Maximum Wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

FCC Statement

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 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.

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

1. This device may not cause harmful interference, and

2. This device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

The radio module has been evaluated under FCC Bulletin OET 65C (01-01) and found to be compliant to the requirements as set forth in CFR 47 Sections, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices. This model meets the applicable government requirements for exposure to radio frequency waves.

Europe – EU Declaration of Conformity $\mathsf{C}\,\mathsf{C}\,\textcircled{\scriptsize{!}}$

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN300 328, EN301 489-17, EN60950-1

Europe – Declaration of Conformity in Languages of the European Community

Èesky [Czech]	*NETGEAR Inc.* tímto prohlašuje, _e tento Radiolan je ve shodì se základními po_adavky a dalšími pøíslušnými ustanoveními smìrnice 1999/5/ES.
Dansk [Danish]	Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *NETGEAR Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *NETGEAR Inc.*, declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente *NETGEAR Inc.* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Åëëçíéêê [Greek]	ÌÅ ÔÇÍ ÐÁÑÏÕÓÁ *NETGEAR Inc.* ÄÇËÙÍÅÉ ÏÔÉ Radiolan ÓÕÌÌÏÑÖÙÍÅÔÁÉ ÐÑÏÓ ÔÉÓ ÏÕÓÉÙÄÅÉÓ ÁÐÁÉÔÇÓÅÉÓ ÊÁÉ ÔÉÓ ËÏÉÐÅÓ Ó×ÅÔÉÊÅÓ ÄÉÁÔÁÎÅÉÓ ÔÇÓ ÏÄÇÃÉÁÓ 1999/5/ÅÊ.
Français [French]	Par la présente *NETGEAR Inc.* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente *NETGEAR Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *NETGEAR Inc.* deklarç, ka Radiolan atbilst Direktîvas 1999/5/EK bûtiskajâm prasîbâm un citiem ar to saistîtajiem noteikumiem.

v1.0, February 2010

[lt] Lietuviø [Lithuanian]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
[nl] Nederlands [Dutch]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
[mt] Malti [Maltese]	Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
[hu] Magyar [Hungarian]	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
[pl] Polski [Polish]	Niniejszym NETGEAR Inc. oœwiadcza, ¿e Radiolan jest zgodny z zasadniczymi wymogami oraz pozosta³ymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
[pt] Português [Portuguese]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
[sl] Slovensko [Slovenian]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi doloèili direktive 1999/5/ES.
[sk] Slovensky [Slovak]	*NETGEAR Inc.* týmto vyhlasuje, _e Radiolan spåòa základné po_iadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
[fi] Suomi [Finnish]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[sv] Svenska [Swedish]	Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
[no] Norsk [Norwegian]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das Wireless-G Router Model WGR614v10 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 Wireless-G Router Model WGR614v10 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 see 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.

MIC Compliance, "Class B" Equipment (Household purpose info/tele-communications equipment)

As this equipment has undergone EMC registration for household purposes, this product can be used in any area including residential areas.

Product and Publication Details

Model Number:	WGR614v10
Publication Date:	February 2010
Product Family:	Wireless Router
Product Name:	Wireless-G Router Model WGR614v10
Home or Business Product:	Home
Language:	English
Publication Part Number:	202-10585-01
Publication Version Number:	1.0

Contents

Appendix A
Technical Specifications

Appendix B
Related Documents

Index

About This Manual

The user manual provides information for configuring the features of the NETGEAR® Wireless-G Router Model WGR614v10 beyond initial configuration settings. Initial configuration instructions can be found in the *NETGEAR Wireless-G Router WGR614v10 Setup Manual*. You should have basic to intermediate computer and Internet skills.

Conventions, Formats, and Scope

The conventions, formats, and scope of this manual are described in the following paragraphs:

- **Typographical conventions**. This manual uses the following typographical conventions:

Italic	Emphasis, books, CDs
Bold	User input, GUI screen text
Fixed	Command prompt, CLI text, code
Italic	URL links

- **Formats**. This manual uses the following formats to highlight special messages:

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

> **Tip:** This format is used to highlight a procedure that will save time or resources.

> **Warning:** Ignoring this type of note might result in a malfunction or damage to the equipment, a breach of security, or a loss of data.

> ⚠ **Danger:** This is a safety warning. Failure to take heed of this notice might result in personal injury or death.

- **Scope**. This manual is written for the Wireless-G Router according to these specifications:

Product Version	Wireless-G Router Model WGR614v10
Manual Publication Date	February 2010

For more information about network, Internet, firewall, and VPN technologies, click the links to the NETGEAR website in Appendix B, "Related Documents."

> → **Note:** Product updates are available on the NETGEAR, Inc. website at *http://www.netgear.com/support*.

How to Print This Manual

To print this manual, your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at *http://www.adobe.com*.

> 💡 **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.

Revision History

NETGEAR, Inc. is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since the Wireless-G Router was introduced.

Table 2-1. Publication Revision History

Part Number	Version Number	Date	Description
202-10585-01	v1.0	February 2010	First publication.

v1.0, February 2010

Chapter 1
Configuring Basic Connectivity

This chapter describes the settings for your Internet connection and your wireless local area network (LAN) connection. When you perform the initial configuration of your wireless router using the *Resource CD* as described in the *Setup Manual,* these settings are specified automatically for you. This chapter provides further details about these connectivity settings, as well as instructions on how to log in to the router for further configuration.

> **Note:** NETGEAR recommends using the Smart Wizard™ on the *Resource CD* for initial configuration, as described in the .

This chapter includes the following sections:

- "Using the Setup Manual"
- "Logging In to Your Wireless Router" on page 1-2
- "Selecting a Language for Your Screen Display" on page 1-5
- "Configuring Your Internet Connection Using the Setup Wizard" on page 1-6
- "Viewing and Configuring Basic ISP Settings" on page 1-6
- "Setting Up and Testing Basic Wireless Connectivity" on page 1-11

Using the Setup Manual

For first-time installation of your wireless router, refer to the *NETGEAR Wireless Router Setup Manual*. The *Setup Manual* explains how to launch the NETGEAR Smart Wizard on the *Resource CD* to step you through the procedure to connect your router, modem, and computers. The Smart Wizard will assist you in configuring your wireless settings and enabling wireless security for your network. After initial configuration using the *Setup Manual*, you can use the information in this *User Manual* to configure additional features of your wireless router.

For installation instructions in a language other than English, refer to the language options on the *Resource CD*.

Logging In to Your Wireless Router

When the wireless router is connected to your network, you can access and configure the router using your browser.

To access the Web Configuration Manager:

1. Connect to the wireless router by typing **http://www.routerlogin.net** or the router's LAN IP address (the default is 192.168.1.1) in the address field of your browser, and then press Enter. A login window opens:

Figure 1-1

> **Tip:** You can connect to the wireless router by typing either of these URLs in the address field of your browser, and then pressing Enter:
>
> • *http://www.routerlogin.net*
>
> • *http://www.routerlogin.com*
>
> If these URLs do not work, you must type the IP address of the router, for example, *http://www.192.168.1.1*.

2. Enter **admin** for the router user name and your password (or the default, **password**). For information about how to change the password, see "Changing the Administrator Password" on page 2-15.

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

The Checking for Firmware Updates screen appears unless you previously cleared the **Check for Updated Firmware Upon Log-in** check box.
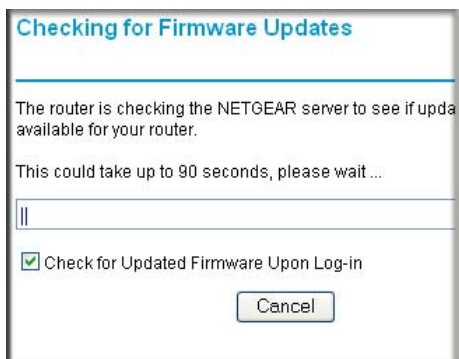
Figure 1-2

This message displays if the router discovers that new firmware is available. (If no new firmware is available, the router will proceed to the router status screen.)
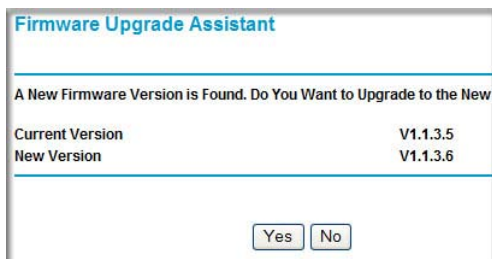
Figure 1-3

To automatically update to the new firmware, click **Yes** to allow the router to download and install the new firmware file from NETGEAR.

> ⚠️ **Warning:** When uploading firmware to the Wireless-G Router, *do not* interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.

The update process typically takes about 1 minute. When the upload is complete, your router automatically restarts.

3. If there is no new firmware, the login will take you to the Basic Settings screen displayed here.

Figure 1-4

> **Note:** If the **Check for New Version Upon Log-in** check box is selected, the home page is the Router Upgrade screen. Otherwise, it is the Basic Settings screen.
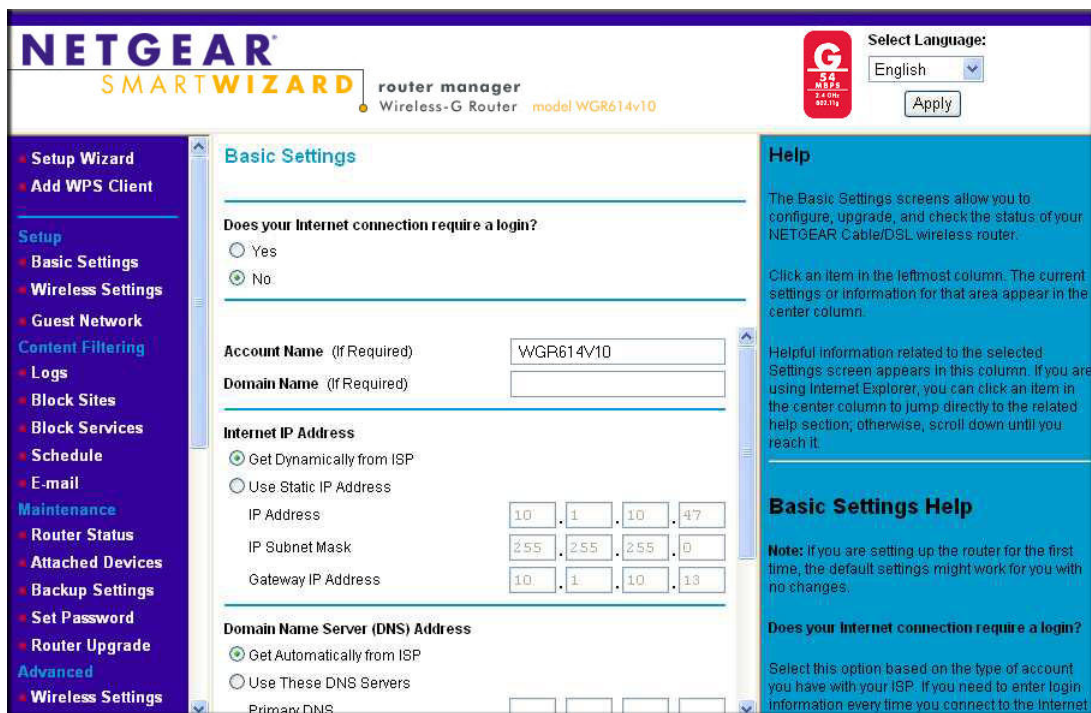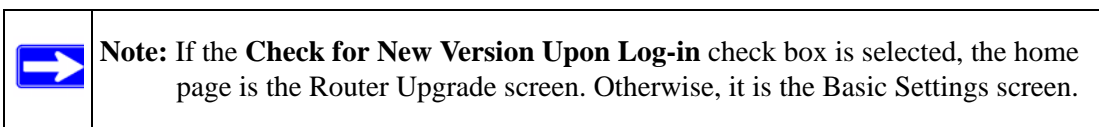
If the wireless router is connected to the Internet, you can select **Knowledge Base** or **Documentation** under Web Support in the main menu to view support information or the documentation for the wireless router.

If you do not click **Logout**, the wireless router will wait for 5 minutes after no activity before it automatically logs you out.

Selecting a Language for Your Screen Display

Using the Select Language drop-down menu, located in the upper right corner of the Router Manager screen, you can display the router manager screens in any of languages shown in Figure 1-5:
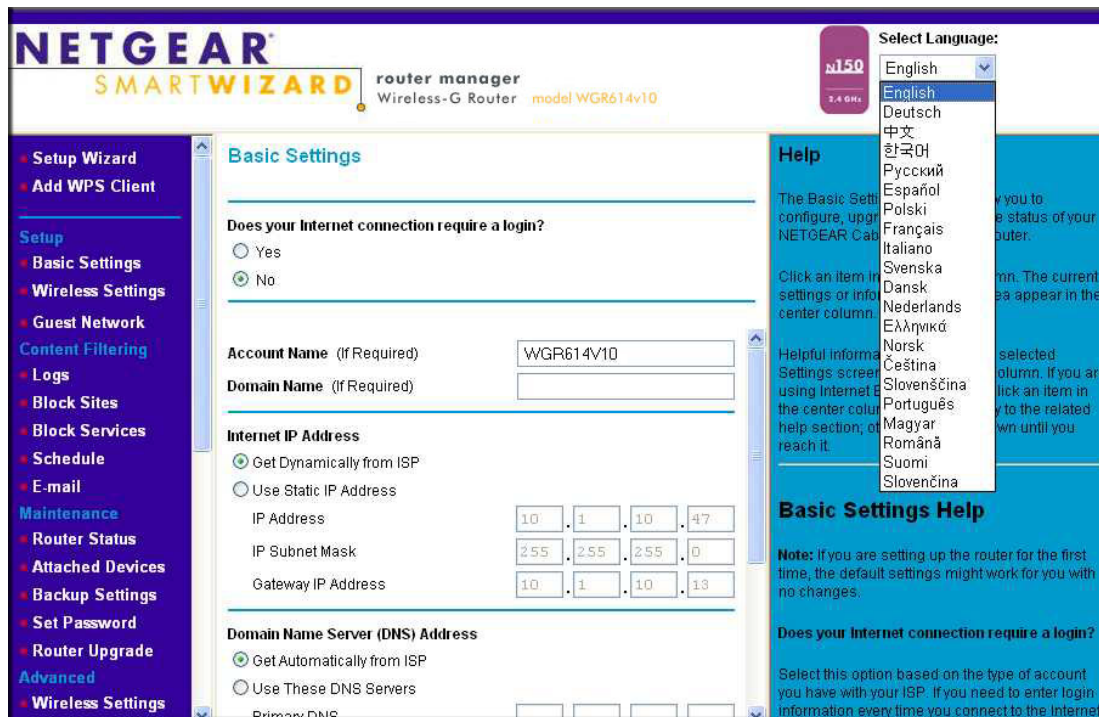
Figure 1-5

The language is set to English by default. The default language is always stored in memory. When you select a language other than the default, that language as well as English is stored in memory. The additional language stored is the most recently selected. For example, if you select Deutsch, German and English will be stored. If you next select Chinese, Chinese and English will be stored.

To specify a language to be used on your router manager screens, do the following:

1. Expand the list and select the language you want.

2. Click **Apply**.

v1.0, February 2010

The language you select is then downloaded and displayed in the language selection box, and your screen display will be in the selected language.

> **Note:** You can select from the entire list of supported languages only when the router is connected to the Internet. When the router is not connected to the Internet, you can select one of the stored languages only.

Configuring Your Internet Connection Using the Setup Wizard

You can manually configure your Internet connection using the Basic Settings screen, or you can allow the Smart Setup Wizard to determine your Internet Service Provider (ISP) configuration.

The Smart Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration. This feature is not the same as the Smart Wizard configuration assistant that appears only when the router is in its factory default state. To use the Smart Setup Wizard to assist with configuration or to verify the Internet connection settings:

1. From the top of the main menu of the browser interface, click **Setup Wizard**.

2. Click **Next** to proceed. Enter your ISP settings, as needed.

3. At the end of the Setup Wizard, click **Test** to verify your Internet connection. If you have trouble connecting to the Internet, see Chapter 7, "Troubleshooting."

Viewing and Configuring Basic ISP Settings

Settings related to your Internet service are specified in the Basic Settings screen. To access the Basic Settings screen, from the main menu of the router's Web Configuration Interface, under Setup, select **Basic Settings**.

The content you see in the Basic Settings screen depends on whether your ISP requires that you log in with a user name and password for Internet access.

Your Internet Connection *Does Not* Require a Login

If no login is required by your ISP, the following settings appear in the Basic Settings screen.

ISP *does not* require login

Figure 1-6

- **Account Name** (might also be called Host Name). The account name is provided to the ISP during a DHCP request from your router. In most cases, this setting is not required, but some ISPs require it for access to ISP services such as mail or news servers.

- **Domain Name**. The domain name is provided by your router to computers on your LAN when the computers request DHCP settings from your router. In most cases, this settings is not required.

- **Internet IP Address**. Determines how your router obtains an IP address for Internet access.

  – If your ISP assigns an IP address dynamically (by DHCP), select **Get Dynamically From ISP**.

  – If your ISP has assigned you a permanent, fixed (static) IP address for your computer, select **Use Static IP Address**. Enter the IP address that your ISP assigned. Also, enter the subnet mask and the gateway IP address. The gateway is the ISP's router to which your router will connect.

- **Domain Name Server (DNS) Address**. If you know that your ISP does not automatically transmit DNS addresses to the router during login, select **Use These DNS Servers**, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

  > **Note:** If you enter or change a DNS address, restart the computers on your network so that these settings take effect.

- **Router MAC Address**. This section determines the Ethernet MAC address that the router will use on the Internet port. Typically, you would leave **Use Default Address** selected. However, some ISPs (especially cable modem providers) register the Ethernet MAC address of the network interface card in your computer when your account is first opened. They then accept only traffic from the MAC address of that computer. This feature allows your router to masquerade as that computer by "cloning" or "spoofing" its MAC address.
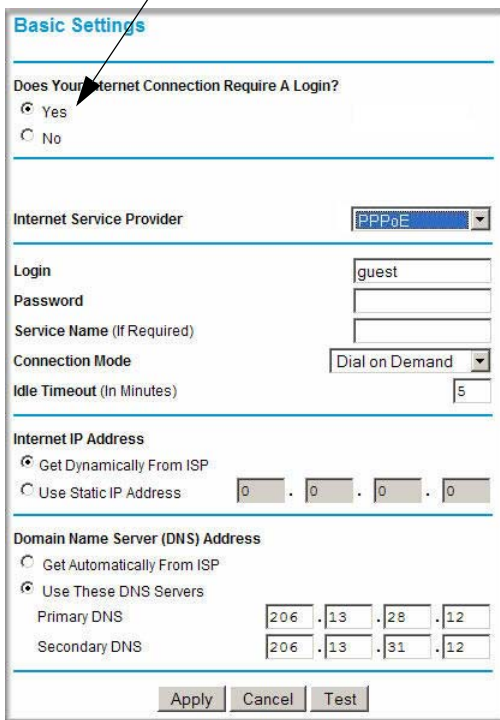
  To change the MAC address, select one of the following methods:

  – Select **Use Computer MAC Address**. The router will then capture and use the MAC address of the computer that you are now using. You must be using the one computer that is allowed by the ISP.

  – Select **Use This MAC Address**, and type it in here.

Your Internet Connection *Does* Require a Login

If a login is required by your ISP, the following settings appear in the Basic Settings screen:

Login required

Figure 1-7

- **Does Your Internet Connection Require A Login?** If you usually must use a login program such as WinPOET to access the Internet, your Internet connection requires a login. After you select **Yes**, the Basic Settings screen displays.

> **Note:** After you finish setting up your router, you will no longer need to launch the ISP's login program on your computer to access the Internet. When you start an Internet application, your router will automatically log you in.

- **Internet Service Provider**. This drop-down list contains a few ISPs that need special protocols for connection. The list includes:

– **PPTP** (Point to Point Tunneling Protocol), used primarily in Austrian DSL services

– **Telstra Bigpond**, an Australian residential cable modem service

> **Note:** The Telstra Bigpond setting is only for older cable modem service accounts still requiring a Bigpond login utility. Telstra has discontinued this type of account. Those with Telstra DSL accounts and newer cable modem accounts should select **No** for Does Your Internet Connection Require a Login.

– **PPPoE** (Point to Point Protocol over Ethernet), the protocol used by most DSL services worldwide.

Figure 1-8

> **Note:** Not all ISPs are listed here. The ones on this list have special requirements.

• **Login and Password**. This is the user name and password provided by your ISP. This name and password are used to log in to the ISP server.

• **Service Name**. If your connection is capable of connecting to multiple Internet services, this setting specifies which service to use.

• **Connection Mode**. This drop-down list (shown in Figure 1-7 on page 1-9) selects when the router will connect to and disconnect from the Internet. The list includes:

– **Always On**. The router logs in to the Internet immediately after booting and never disconnects.

– **Dial on Demand**. The router logs in only when outgoing traffic is present and logs out after the idle time-out.

– **Manually Connect**. The router logs in or logs out only when the user clicks **Connect** or **Disconnect** in the Router Status screen.

*   **Idle Timeout**. Your Internet connection is logged out if there is no data transfer during the specified time interval.

*   **Domain Name Server (DNS) Address**. If you know that your ISP does not automatically transmit DNS addresses to the router during login, select **Use These DNS Servers**, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

> **Note:** If you enter or change a DNS address, restart the computers on your network so that these settings take effect.
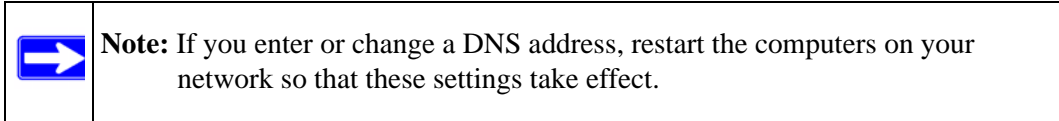
Setting Up and Testing Basic Wireless Connectivity

Follow these instructions to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.

1. Select **Wireless Settings** under Setup in the main menu of the WGR614v10 router.

Wireless Settings

Wireless Network

Name (SSID):	NETGEAR
Region:	United States
Channel:	Auto
Mode:	b and g

Security Options

*   ⦿ None
*   ◯ WEP
*   ◯ WPA-PSK [TKIP]
*   ◯ WPA2-PSK [AES]
*   ◯ WPA-PSK [TKIP] + WPA2-PSK [AES]

[Apply] [Cancel]

Figure 1-9

2. As appropriate, select the region in which the wireless interface will operate.

→ **Note:** In North America, you will not be able to change the region setting.

3. For the wireless network name (SSID), use the default name, or choose a suitable descriptive name. In the **Name (SSID)** field, you can enter a value of up to 32 alphanumeric characters. The default SSID is NETGEAR.

→ **Note:** The SSID is case-sensitive; NETGEAR is not the same as nETgear. Also, the SSID of any wireless access adapters must match the SSID you specify in the Wireless-G Router. If they do not match, you will not get a wireless connection to the Wireless-G Router.

4. For the remaining settings, accept the defaults.

- The default channel is **Auto**.

  It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your router. For more information about the wireless channel frequencies, click the link to the online document "Wireless Networking Basics" in Appendix B.

- The default mode is **b and g**.
- The default for Security Options is **None**.

5. Click **Apply** to save your changes.

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

6. Select **Wireless Settings** under Advanced in the main menu of the WGR614v10 router.

Figure 1-10

7. Make sure that the **Enable Wireless Router Radio, Enable SSID Broadcast,** and **Enable WMM** check boxes are selected.

8. Click **Setup Access List**.

9. Make sure that the **Turn Access Control On** check box is *not* selected.

10. Configure and test your wireless computer for wireless connectivity.

Program the wireless adapter of your computer to have the same SSID and channel that you specified in the router, and disable encryption. Check that your computer has a wireless link and can obtain an IP address by DHCP from the router.

Once your computer has basic wireless connectivity to the router, you can configure the advanced wireless security functions of the computer and router (for more information about security and these settings, see Chapter 2, "Safeguarding Your Network ").

The Wireless-G Router Model WGR614v10 provides highly effective security features, which are covered in detail in this chapter.

This chapter includes the following sections:

Choosing Appropriate Wireless Security

Unlike wired networks, wireless networks allow anyone with a compatible adapter to receive your wireless data transmissions well beyond your walls. Operating an unsecured wireless network creates an opportunity for outsiders to eavesdrop on your network traffic or to enter your network to access your computers and files. Indoors, computers can connect over 802.11b/g wireless networks at ranges of up to 300 feet. Such distances can allow for others outside your immediate area to access your network. Use the security features of your wireless equipment that are appropriate to your needs.

The time it takes to establish a wireless connection can vary depending on both your security settings and router placement.

Stronger security methods can entail a cost in terms of throughput, latency, battery consumption, and equipment compatibility. In choosing an appropriate security level, you can also consider the effort compared to the reward for a hacker to break into your network. As a minimum, however, NETGEAR recommends using WEP with Shared Key authentication. Do not run an unsecured wireless network unless it is your intention to provide free Internet access for the public.

WEP connections can take slightly longer to establish. Also, WEP, WPA-PSK, and WPA2-PSK encryption can consume more battery power on a notebook computer, and can cause significant performance degradation with a slow computer.

> **Note:** NETGEAR recommends that you change the administration password of your router. Default passwords are well known, and an intruder can use your administrator access to read or disable your security settings. For information about how to change the administrator password, see "Changing the Administrator Password" on page 2-15.

**Wireless data
security options**

Range: up to 300 foot radius

1) Open system: easy but no security

2) MAC access list: no data security

3) WEP: security but some performance impact

4) WPA-PSK: strong security

5) WPA2-PSK: very strong security

WGR614v10
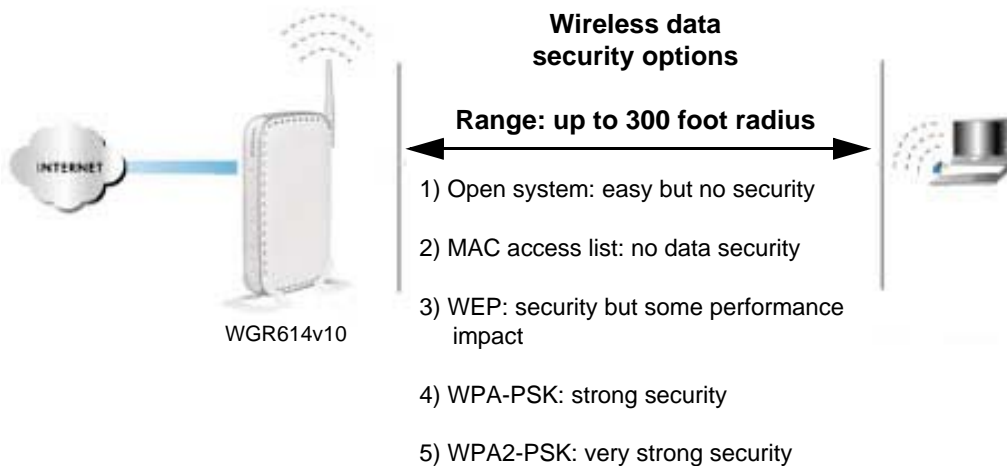
Note: Use these with other features that enhance security (Table 2-2 on page 2-4).

Figure 2-1

The Wireless-G Router provides two screens for configuring the wireless settings: the basic Wireless Settings screen, which you access under Setup in the main menu (see "Changing Wireless Security Settings" on page 2-6), and the Advanced Wireless Settings screen, which you access under Advanced (see "Changing Wireless Security Settings" on page 2-6).

Basic security options are listed in order of increasing effectiveness in Table 2-1 below. Other

features that affect security are listed in Table 2-2 on page 2-4. For more details on wireless security methods, see the online document "Wireless Networking Basics" in Appendix B.

Table 2-1.   Wireless Security Options

Security Type	Description
None.	No wireless security. Recommended only for troubleshooting wireless connectivity. Do not run an unsecured wireless network unless it is your intention to provide free Internet access for the public.
WEP. Wired Equivalent Privacy.	Wired Equivalent Privacy (WEP) data encryption provides moderate data security. WEP Shared Key authentication and WEP data encryption can be defeated by a determined eavesdropper using publicly available tools. For more information, see "Configuring WEP Wireless Security" on page 2-7.
WPA-PSK (TKIP). WPA-PSK standard encryption with TKIP encryption type. **WPA2-PSK (AES)**. Wi-Fi Protected Access version 2 with Pre-Shared Key; WPA2-PSK standard encryption with the AES encryption type. **WPA-PSK (TKIP) + WPA2-PSK (AES)**. Mixed mode.	Wi-Fi Protected Access with Pre-Shared Key (WPA-PSK and WPA2-PSK) data encryption provides extremely strong data security, very effectively blocking eavesdropping. Because WPA and WPA2 are relatively new standards, older wireless adapters and devices might not support them. For more information, see "Configuring WPA-PSK and WPA2-PSK Wireless Security" on page 2-9.

Table 2-2.   Other Features That Enhance Security

Security Type	Description
Disable the wireless router radio.	If you disable the wireless router radio, wireless devices cannot communicate with the router at all. You might disable this when you are away or when other users of your network all use wired connections. For more information, see "Viewing Advanced Wireless Settings" on page 2-10.
Turn off the broadcast of the wireless network name SSID.	If you disable the broadcast of the SSID, only devices that know the correct SSID can connect. This nullifies the wireless network discovery feature of some products such as Windows XP, but your data is still fully exposed to an intruder using available wireless eavesdropping tools. For more information, see "Viewing Advanced Wireless Settings" on page 2-10.
Restrict access based on MAC address.	You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the Wireless-G Router. MAC address filtering adds an obstacle against unwanted access to your network by the general public, but the data broadcast over the wireless link is fully exposed. This data includes your trusted MAC addresses, which can be read and impersonated by a hacker. For more information, see "Restricting Wireless Access by MAC Address" on page 2-11.
Modify your firewall's rules.	By default, the firewall allows any outbound traffic and prohibits any inbound traffic except for responses to your outbound traffic. However, you can modify the firewall's rules. For more information, see "Understanding Your Firewall" on page 2-17.

Recording Basic Wireless Settings Setup Information

Before customizing your wireless settings, print this section, and record the following information. If you are working with an existing wireless network, the person who set up or is responsible for the network can provide this information. Otherwise, you must choose the settings for your wireless network. Either way, record the settings for your wireless network in the spaces provided.

- **Wireless Network Name (SSID)**. _____ The SSID identifies the wireless network. You can use up to 32 alphanumeric characters. The SSID *is* case-sensitive. The SSID in the wireless adapter card must match the SSID of the wireless router. In some configuration utilities (such as in Windows XP), the term "wireless network name" is used instead of SSID.

- If **WEP Authentication** is used, circle one: **Open System**, **Shared Key**, or **Auto**.

> **Note:** If you select Shared Key, the other devices in the network will not connect unless they are also set to Shared Key and are configured with the correct key.

   – **WEP Encryption Key Size**. Choose one: **64-bit** or **128-bit**. Again, the encryption key size must be the same for the wireless adapters and the wireless router.

   – **Data Encryption (WEP) Keys**. There are two methods for creating WEP data encryption keys. Whichever method you use, record the key values in the spaces provided.

      - **Passphrase Method**. _____ These characters *are* case-sensitive. Enter a word or group of printable characters and click Generate. Not all wireless devices support the passphrase method.

      - **Manual Method**. These values *are not* case-sensitive. For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F). For 128-bit WEP, enter 26 hexadecimal digits.

         Key 1: _____

         Key 2: _____

         Key 3: _____

         Key 4: _____

- If WPA-PSK or WPA2-PSK authentication is used:

   – **Passphrase**. _____ These characters *are* case-sensitive. Enter a word or group of printable characters. When you use WPA-PSK, the other devices in the network will not connect unless they are also set to WPA-PSK and are configured with the correct passphrase. Similarly, when you use WPA2-PSK, the other devices in the network will not connect unless they are also set to WPA2-PSK and are configured with the correct passphrase.

Use the procedures described in the following sections to specify the Wireless-G Router. Store this information in a safe place.

Changing Wireless Security Settings

This section describes the wireless settings that you can view and configure in the Wireless Settings screen, which you access under Setup in the main menu.

Viewing Basic Wireless Settings

To specify the wireless security settings of your router:

1. Log in to the router as described in "Logging In to Your Wireless Router" on page 1-2.

2. Select **Wireless Settings** under Setup in the main menu.

Figure 2-2

The available settings in this screen are:

- **Name (SSID)**. The SSID is also known as the wireless network name. Enter a value of up to 32 alphanumeric characters. When more than one wireless network is active, different wireless network names provide a way to separate the traffic. For a wireless device to participate in a particular wireless network, it must be configured with the SSID for that network. The WGR614v10 default SSID is **NETGEAR**. You can disable this broadcast as described in "Viewing Advanced Wireless Settings" on page 2-10.

- **Region**. This field identifies the region where the Wireless-G Router can be used. It might not be legal to operate the wireless features of the wireless router in a region other than one of those identified in this field.

> **Note:** The region selection feature might not be available in all countries.

- **Channel**. This field determines which operating frequency is used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless network. The wireless router uses channel bonding technology to extend the bandwidth for data transmission. For more information about the wireless channel frequencies, see the online document that you can access from "Wireless Networking Basics" in Appendix B.

- **Mode**. This field determines which data communications protocol is used. You can choose from: b and g; or g only.

- **Security Options**. The selection of wireless security options can significantly affect your network performance. The time it takes to establish a wireless connection can vary depending on both your security settings and router placement.

  WEP connections can take slightly longer to establish. Also, WEP, WPA-PSK, and WPA2-PSK encryption can consume more battery power on a notebook computer, and can cause significant performance degradation with a slow computer. Instructions for configuring the security options can be found in "Choosing Appropriate Wireless Security" on page 2-1. A full explanation of wireless security standards is available in the online document that you can access from "Wireless Networking Basics" in Appendix B.

3. Click **Apply** to save your settings.

Configuring WEP Wireless Security

WEP Shared Key authentication and WEP data encryption can be defeated by a determined eavesdropper using publicly available tools.

WEP offers the following options:

- **Open System**. With Open System authentication and 64 or 128 bit WEP data encryption, the Wireless-G Router *does* perform data encryption but *does not* perform any authentication. Anyone can join the network. This setting provides very little practical wireless security.

- **Shared Key**. With Shared Key authentication, a wireless device must know the WEP key to join the network. Select the encryption strength (64 or 128 bit data encryption). Manually enter the key values, or enter a word or group of printable characters in the **Passphrase** field. Manually entered keys *are not* case-sensitive, but passphrase characters *are* case-sensitive.

To configure WEP data encryption:

> **Note:** If you use a wireless computer to configure WEP settings, you will be disconnected when you click **Apply**. You must then either configure your wireless adapter to match the wireless router WEP settings or access the wireless router from a wired computer to make any further changes. Not all wireless adapter configuration utilities support passphrase key generation.

1. Select **Wireless Settings** under Setup in the main menu.

2. In the Security Options section, select **WEP**. The WEP options display.

Figure 2-3

3. Select the authentication type and encryption strength.

4. You can manually or automatically program the four data encryption keys. These values must be identical on all computers and access points in your network.

- **Automatic**. In the **Passphrase** field, enter a word or group of printable characters, and click **Generate**. The passphrase is case-sensitive. For example, NETGEAR is not the same as nETgear. The four key fields are automatically populated with key values.

- **Manual**. Enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F). These entries are not case-sensitive. For example, AA is the same as aa.
Select which of the four keys to activate.

5. Click **Apply** to save your settings.

Configuring WPA-PSK and WPA2-PSK Wireless Security

Wi-Fi Protected Access with Pre-Shared Key (WPA-PSK and WPA2-PSK) data encryption provides extremely strong data security, very effectively blocking eavesdropping. Because WPA and WPA2 are relatively new standards, older wireless adapters and devices might not support them. Check whether newer drivers are available from the manufacturer. Also, you might be able to use the Push 'N' Connect feature to configure this type of security if it is supported by your wireless clients. See "Restricting Wireless Access by MAC Address" on page 2-11.

WPA–Pre-Shared Key *does* perform authentication. WPA-PSK uses TKIP (Temporal Key Integrity Protocol) data encryption, and WPA2-PSK uses AES (Advanced Encryption Standard) data encryption. Both methods dynamically change the encryption keys making them nearly impossible to circumvent.

Mixed mode allows clients using either WPA-PSK (TKIP) or WPA2-PSK (AES). This provides the most reliable security, and is easiest to implement, but it might not be compatible with older adapters.
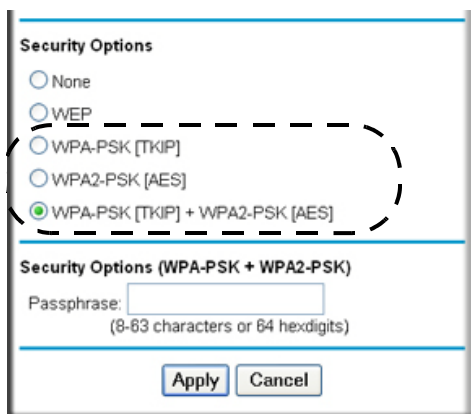
> **Note:** Not all wireless adapters support WPA. Furthermore, client software is also required. Windows XP with Service Pack 2 does include WPA support. Nevertheless, the wireless adapter hardware and driver must also support WPA. For instructions on configuring wireless computers or PDAs (personal digital assistants) for WPA-PSK security, consult the documentation for the product you are using.

To configure WPA-PSK, WPA2-PSK, or WPA-PSK+WPA2-PSK:

1. Select **Wireless Settings** under Setup in the main menu.

2. Select one of the WPA-PSK or WPA2-PSK options for the security type. The third option (WPA-PSK [TKIP] + WP2-PSK [AES]) is the most flexible, since it allows clients using either WPA-PSK or WPA2-PSK.

3. In the **Passphrase** field, enter a word or group of 8–63 printable characters. The passphrase is case-sensitive.

Figure 2-4

4. Click **Apply** to save your settings.

Viewing Advanced Wireless Settings

This section describes the wireless settings that you can view and specify in the Advanced Wireless Settings screen, which you access under Advanced in the main menu.

To configure the advanced wireless security settings of your router:

1. Log in to the router as described in "Logging In to Your Wireless Router" on page 1-2.

2. Select **Wireless Settings** under Advanced in the main menu.

Figure 2-5

The available settings in this screen are:

*   **Enable SSID Broadcast**. Clear this check box to disable broadcast of the SSID, so that only devices that know the correct SSID can connect. Disabling SSID broadcast nullifies the wireless network discovery feature of some products such as Windows XP.

*   **Enable Wireless Router Radio**. If you disable the wireless router radio, wireless devices cannot connect to the Wireless-G Router. If you will not be using your wireless network for a period of time, you can clear this check box and disable all wireless connectivity.

*   **Enable WMM**. Clear this check box to disable WMM. Disabling WMM turns off the wireless prioritization scheme. Note that wireless clients must also support WMM to take advantage of this feature.

*   **Wireless Card Access List**. For information about this list, see "Restricting Wireless Access by MAC Address" on page 2-11.

> **Note:** The Fragmentation Threshold, CTS/RTS Threshold, and Preamble Mode options are reserved for wireless testing and advanced configuration only. Do not change these settings.

Restricting Wireless Access by MAC Address

When a Wireless Card Access List is configured and enabled, the router checks the MAC address of any wireless device attempting a connection and allows only connections to computers identified on the trusted computers list.

The Wireless Card Access List displays a list of wireless computers that you allow to connect to the router based on their MAC addresses. These wireless computers must also have the correct SSID and wireless security settings to access the wireless router.

The MAC address is a network device's unique 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F only, and separated by colons (for example, 00:09:AB:CD:EF:01). It can usually be found on the bottom of the wireless card or network interface device. If you do not have access to the physical label, you can display the MAC address using the network configuration utilities of the computer. In WindowsXP, for example, typing the `ipconfig/all` command in an MSDOS command prompt window displays the MAC address as Physical Address. You might also find the MAC addresses in the router's Attached Devices screen.

To restrict access based on MAC addresses:

1. Select **Wireless Settings** under Advanced in the main menu.

2. In the Advanced Wireless Settings screen, click **Setup Access List** to display the Wireless Card Access List.

Figure 2-6

3. Click **Add** to add a wireless device to the wireless access control list. The Wireless Card Access Setup screen opens and displays a list of currently active wireless cards and their Ethernet MAC addresses.

Figure 2-7

4. If the computer you want appears in the Available Wireless Cards list, you can select the radio button of that computer to capture its MAC address; otherwise, you can manually enter a name and the MAC address of the authorized computer. You can usually find the MAC address on the bottom of the wireless device.

> **Tip:** You can copy and paste the MAC addresses from the router's Attached Devices screen into the MAC Address field of this screen. To do this, configure each wireless computer to obtain a wireless link to the router. The computer should then appear in the Attached Devices screen.

5. Click **Add** to add this wireless device to the Wireless Card Access List. The screen changes back to the list screen.

6. Repeat step 3 through step 5 for each additional device you want to add to the list.

7. Select the **Turn Access Control On** check box.

> **Note:** When configuring the router from a wireless computer whose MAC address is not in the Trusted PC list, if you select **Turn Access Control On**, you lose your wireless connection when you click **Apply**. You must then access the wireless router from a wired computer or from a wireless computer that is on the access control list to make any further changes.

8. Click **Apply** to save your Wireless Card Access List settings.

Now, only devices on this list can wirelessly connect to the Wireless-G Router.

> ⚠️ **Warning:** MAC address filtering adds an obstacle against unwanted access to your network by the general public. However, because your trusted MAC addresses appear in your wireless transmissions, an intruder can read them and impersonate them. Do not rely on MAC address filtering alone to secure your network.

Adding Guest Networks

Adding a guest network allows visitors at your home to use the Internet without having to know your wireless security key.

To add a guest network, do the following:

1. Select **Guest Network** from the Setup menu. The Guest Network Settings screen appears

Figure 2-8

2. Select any of the following Wireless settings:

– **Enable Guest Network** – When this check box is selected, the guest network is enabled, and guests can connect to your network using the SSID of this profile.

- **Enable SSID Broadcast** – If selected, the Wireless Access Point broadcasts its name (SSID) to all Wireless Stations. Stations can adopt the correct SSID for connections to this Access Point.

- **Allow Guest to access MY Local Network** – If selected any user who connects to this SSID can access local networks associated with the router like users in the primary SSID.

3. Give the wireless network a name.

The name is case-sensitive and can be up to 32 characters. The same name must be assigned to all wireless devices in your network. NETGEAR recommends that you change the name to a different value.

4. Select a Security option from the list.

5. Click **Apply** to save your selections.

Changing the Administrator Password

The default password for the router's Web Configuration Manager is **password**. NETGEAR recommends that you change this password to a more secure password.
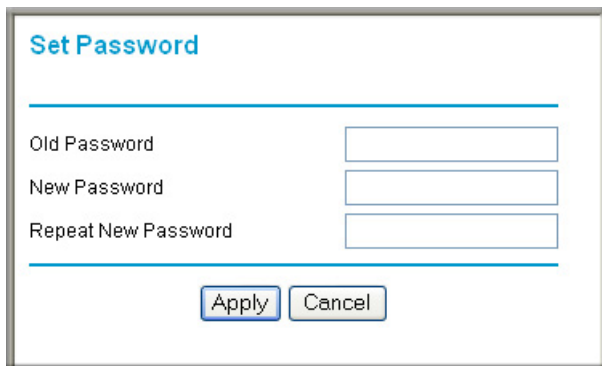
> **Tip:** Before changing the router password, back up your configuration settings with the default password of **password**. If you save the settings with a new password, and then you later forget the new password, you will have to reset the router back to the factory defaults, and log in using the default password of **password**. This means you will have to re-enter all the router configuration settings. For information about how to back up your settings, see "Backing Up and Restoring the Configuration" on page 6-7.

To change the administrator password:

1. On the main menu, under Maintenance, select **Set Password** to display the Set Password screen.

Figure 2-9

2. To change the password, first enter the old password, then enter the new password twice.

3. Click **Apply**.

Backing Up Your Configuration

The configuration settings of the Wireless-G Router are stored within the router in a configuration file. You can back up (save) this file and retrieve it later. NETGEAR recommends that you save your configuration file after you complete the configuration. If the router fails or becomes corrupted, or an administrator password is lost, you can easily re-create your configuration by restoring the configuration file.

For instructions on saving and restoring your configuration file, see "Managing the Configuration File" on page 6-6.

> **Tip:** Before saving your configuration file, change the administrator password to the default, **password**. Then change it again after you have saved the configuration file. If you save the file with a new password, and then you later forget the new password, you will have to reset the router back to the factory defaults and log in using the default password of **password**. This means you will have to re-enter all the router configuration settings.

Understanding Your Firewall

Your Wireless-G Router Model WGR614v10 contains a true firewall to protect your network from attacks and intrusions. A firewall is a device that protects one network from another while allowing communication between the two. Using a process called Stateful Packet Inspection, the firewall analyzes all inbound and outbound traffic to determine whether or not it will be allowed to pass through.

By default, the firewall allows any outbound traffic and prohibits any inbound traffic except for responses to your outbound traffic. However, you can modify the firewall's rules to achieve the following behavior:

*   **Blocking sites**. Block access from your network to certain Web locations based on Web addresses and Web address keywords. This feature is described in "Blocking Access to Internet Sites" on page 3-1.

*   **Blocking services**. Block the use of certain Internet services by specific computers on your network. This feature is described in "Blocking Access to Internet Services" on page 3-3.

*   **Scheduled blocking**. Block sites and services according to a daily schedule. This feature is described in "Scheduling Blocking" on page 3-5.

*   **Allow inbound access to your server**. To allow inbound access to resources on your local network (for example, a Web server or remote desktop program), you can open the needed services by configuring port forwarding as described in "Allowing Inbound Connections to Your Network" on page 5-1.

*   **Allow certain games and applications to function correctly**. Some games and applications need to allow additional inbound traffic in order to function. Port triggering can dynamically allow additional service connections, as described in "Allowing Inbound Connections to Your Network" on page 5-1. Another feature to solve application conflicts with the firewall is Universal Plug and Play (UPnP), described in "Using Universal Plug and Play" on page 5-12.

This chapter describes how to use the content filtering and reporting features of the Wireless-G Router Model WGR614v10 to protect your network. You can find these features by selecting the items under Content Filtering in the main menu of the browser interface.

This chapter includes the following sections:

- "Content Filtering Overview"
- "Blocking Access to Internet Sites"
- "Blocking Access to Internet Services" on page 3-3
- "Scheduling Blocking" on page 3-5
- "Viewing Logs of Web Access or Attempted Web Access" on page 3-7

Content Filtering Overview

The Wireless-G Router Model WGR614v10 provides you with Web content filtering options, plus browser activity reporting and instant alerts through e-mail. Parents and network administrators can establish restricted access policies based on time of day, Web addresses, and Web address keywords. You can also block Internet access by applications and services, such as chat rooms or games.

To configure these features of your router, select the items under Content Filtering in the main menu of the browser interface. This chapter describes the screens that display.

Blocking Access to Internet Sites

The Wireless-G Router allows you to restrict access based on Web addresses and Web address keywords. Up to 255 entries are supported in the Keyword list.

Keyword application examples:

- If the keyword **XXX** is specified, the URL www.zzzyyqq.com/xxx.html is blocked.

- If the keyword **.com** is specified, only websites with other domain suffixes (such as .edu, .org, or .gov) can be viewed.

To block access to Internet sites:

1. Select **Block Sites** under Content Filtering in the main menu. The Block Sites screen displays.

Figure 3-1

2. Enable keyword blocking by selecting either **Per Schedule** or **Always**.

To block by schedule, be sure to specify a time period in the Schedule screen. For information about scheduling, see "Scheduling Blocking" on page 3-5.

Block all access to Internet browsing during a scheduled period by entering a dot (**.**) as the keyword, and then set a schedule in the Schedule screen.

3. Add a keyword or domain by entering it in the keyword field and clicking **Add Keyword**. The keyword or domain name then appears the **Block sites containing these keywords or domain names** list.

Delete a keyword or domain name by selecting it from the list and clicking **Delete Keyword**.

4. You can specify one trusted user, which is a computer that is exempt from blocking and logging. Specify a trusted user by entering that computer's IP address in the **Trusted IP Address** fields.

Since the trusted user is identified by IP address, you should configure that computer with a fixed IP address.

5. Click **Apply** to save all your settings in the Block Sites screen.

Blocking Access to Internet Services

The Wireless-G Router allows you to block the use of certain Internet services by computers on your network. This is called service blocking or port filtering. Services are functions performed by server computers at the request of client computers. For example, Web servers serve Web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on your network sends a request for service to a server computer on the Internet, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (Web server) request.

To block access to Internet services:

1. Select **Block Services** under Content Filtering in the main menu. The Block Services screen displays.

Figure 3-2

2. Enable service blocking by selecting either **Per Schedule** or **Always**, and then click **Apply**.

To block by schedule, be sure to specify a time period in the Schedule screen. For information about scheduling, see "Scheduling Blocking" on page 3-5.

3. Specify a service for blocking by clicking **Add**. The Block Services Setup screen displays.

Figure 3-3

4. From the **Service Type** list, select the application or service to be allowed or blocked. The list already displays several common services, but you are not limited to these choices. To add any additional services or applications that do not already appear, select **User Defined**.

5. Select the radio button for the IP address configuration you want to block, and then enter the IP addresses in the appropriate fields.

6. Click **Add** to enable your Block Services Setup selections.

Configuring a User-Defined Service

To define a service, first you must determine which port number or range of numbers is used by the application. The service port numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application. You can often determine port number information by contacting the publisher of the application, by asking user groups or newsgroups, or by searching.

• Enter the starting port and ending port numbers. If the application uses a single port number, enter that number in both fields.

• If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select **Both**.

Blocking Services by IP Address Range

In the Filter Services For area, you can block the specified service for a single computer, a range of computers (having consecutive IP addresses), or all computers on your network.

Scheduling Blocking

The Wireless-G Router allows you to specify when blocking is enforced.

To schedule blocking:

1. Select **Schedule** under Content Filtering in the main menu. The Schedule screen displays.

Figure 3-4

2. Configure the schedule for blocking keywords and services.

    a. **Days to Block**. Select days on which you want to apply blocking by selecting the appropriate check boxes. Select **Every Day** to select the check boxes for all days. Click **Apply**.

b. **Time of Day to Block**. Select a start and end time in 24-hour format. Select **All Day** for 24-hour blocking.

c. **Time Zone**.

Select the time zone where you are located, and if you prefer to automatically adjust for daylight savings time.

> **Note:** Accurate time zone and daylight savings settings will assure that the scheduling and logging functions operate correctly.

The Wireless-G Router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet. To localize the time for your log entries, you must specify your time zone:

- **Time Zone**. Select your local time zone. This setting is used for the blocking schedule and for time-stamping log entries.
- **Automatically Adjust for Daylight Savings Time**. Select this check box if your region supports daylight savings time. The router will automatically adjust the time at the start and end of the daylight savings time period.

3. Click **Apply** to save your settings.

Viewing Logs of Web Access or Attempted Web Access

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

Select **Logs** under Content Filtering in the main menu. The Logs screen displays.
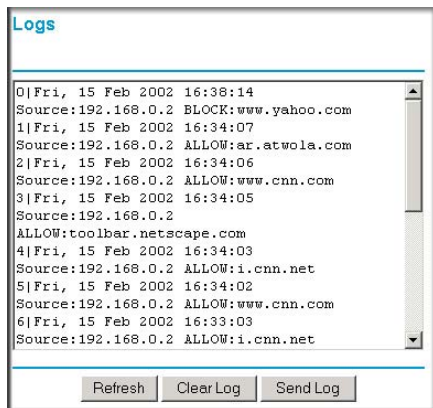
Figure 3-5

Table 3-1 describes the log entries.

Table 3-1. Log Entry Descriptions

Field	Description
Date and time	The date and time the log entry was recorded.
Source IP	The IP address of the initiating device for this log entry.
Target address	The name or IP address of the website or newsgroup visited or to which access was attempted.
Action	Whether the access was blocked or allowed.

To refresh the log screen, click the **Refresh** button.

To clear the log entries, click the **Clear Log** button.

This chapter describes how to configure advanced networking features of the
Wireless-G Router Model WGR614v10, including LAN, WAN, and routing settings.

It contains the following sections:

*   "Using the LAN IP Setup Options"
*   "Using a Dynamic DNS Service" on page 4-4
*   "Configuring the WAN Setup Options" on page 4-6
*   "Configuring Static Routes" on page 4-8
*   "Wireless Repeating (Also Called WDS)" on page 4-10

Using the LAN IP Setup Options

The LAN Setup screen allows configuration of LAN IP services such as Dynamic Host
Configuration Protocol (DHCP) and Routing Information Protocol (RIP).

To configure LAN IP settings, from the main menu of the browser interface, under Advanced,
click **LAN Setup**. The following screen displays:

Figure 4-1

Configuring a Device Name

The device name is a user-friendly name for the router. This name is shown in the Network on Windows Vista and the Network Explorer on all Windows systems. The **Device Name** field cannot be blank. The default name is WNR3500.

Configuring LAN TCP/IP Setup Parameters

The router is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server.

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

The router's default LAN IP configuration is:

*   LAN IP address. **192.168.1.1**
*   Subnet mask. **255.255.255.0**

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

The LAN IP settings are:

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

Using the Router as a DHCP Server

By default, the router functions as a DHCP server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the router's LAN. The assigned default gateway address is the LAN address of the router. The router assigns IP addresses to the attached computers from a pool of addresses specified in this screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the router are satisfactory. Click the link to the online document "TCP/IP Networking Basics" in Appendix B for an explanation of DHCP and information about how to assign IP addresses for your network.

Specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the router's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.1.2 and 192.168.1.254, although you might wish to save part of the range for devices with fixed addresses.

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

• An IP address from the range you have defined

• Subnet mask

• Gateway IP address (the router's LAN IP address)

• Primary DNS server (if you entered a primary DNS address in the Basic Settings screen; otherwise, the router's LAN IP address)

• Secondary DNS server (if you entered a secondary DNS address in the Basic Settings screen)

To use another device on your network as the DHCP server, or to manually specify the network settings of all of your computers, clear the **Use Router as DHCP Server** check box. Otherwise, leave it selected. If this service is not selected and no other DHCP server is available on your network, you need to set your computers' IP addresses manually or they will not be able to access the router.

Using Address Reservation

When you specify a reserved IP address for a computer on the LAN, that computer always receives the same IP address each time it accesses the router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.

To reserve an IP address:

1. Click **Add**.

2. In the **IP Address** field, type the IP address to assign to the computer or server. (Choose an IP address from the router's LAN subnet, such as **192.168.1.x**.)

3. Type the MAC address of the computer or server.

> **Tip:** If the computer is already present on your network, you can copy its MAC address from the Attached Devices screen and paste it here.

4. Click **Apply** to enter the reserved address into the table.

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

To edit or delete a reserved address entry:

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

2. Click **Edit** or **Delete**.

Using a Dynamic DNS Service

If your Internet Service Provider (ISP) gave you a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you do not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service, which allows you to register your domain to their IP address, and forwards traffic directed at your domain to your frequently changing IP address.

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

Your router contains a client that can connect to the Dynamic DNS service provided by DynDNS.org. You must first visit their website at *www.dyndns.org* and obtain an account and host name, which you specify in the router. Then, whenever your ISP-assigned IP address changes, your router automatically contacts the Dynamic DNS service provider, logs in to your account, and registers your new IP address. If your host name is hostname, for example, you can reach your router at hostname.dyndns.org.

From the main menu of the browser interface, under Advanced, select **Dynamic DNS** to display the Dynamic DNS screen.
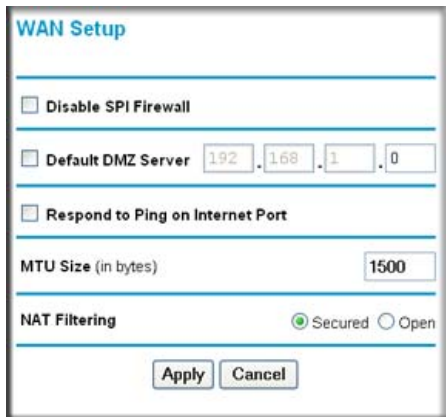

Figure 4-2

To configure Dynamic DNS:

1. Register for an account with one of the Dynamic DNS service providers whose names appear in the **Service Provider** list. For example, for DynDNS.org, select **www.dyndns.org**.

2. Select the **Use a Dynamic DNS Service** check box.

3. Select the name of your Dynamic DNS service provider.

4. Type the host name (or domain name) that your Dynamic DNS service provider gave you.

5. Type the user name for your Dynamic DNS account. This is the name that you use to log in to your account, not your host name.

6. Type the password (or key) for your Dynamic DNS account.

7. If your Dynamic DNS provider allows the use of wildcards in resolving your URL, you can select the **Use Wildcards** check box to activate this feature.
   For example, the wildcard feature causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org.

8. Click **Apply** to save your configuration.

Configuring the WAN Setup Options

The WAN Setup options let you configure a DMZ (demilitarized zone) server, change the Maximum Transmit Unit (MTU) size, and enable the wireless router to respond to a ping on the WAN (Internet) port. From the main menu of the browser interface, under Advanced, click **WAN Setup** to view the WAN Setup screen.

Figure 4-3

Disabling the SPI Firewall

The Stateful Packet Inspection (SPI) firewall protects your network and computers against attacks and intrusions. A stateful packet firewall carefully inspects incoming traffic packets, looking for known exploits such as malformed, oversized, or out-of-sequence packets. The firewall should be disabled only in special circumstances, such as when you are troubleshooting application issues.

Setting Up a Default DMZ Server

The default DMZ server feature is helpful when you are using some online games and videoconferencing applications that are incompatible with Network Address Translation (NAT). The router is programmed to recognize some of these applications and to work correctly with

them, but there are other applications that might not function well. In some cases, one local computer can run the application correctly if that computer's IP address is entered as the default DMZ server.

⚠	**Warning:** DMZ servers pose a security risk. A computer designated as the default DMZ server loses much of the protection of the firewall, and is exposed to exploits from the Internet. If compromised, the DMZ server computer can be used to attack other computers on your network.

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

The WAN Setup screen lets you configure a default DMZ server.

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

1. In the last **Default DMZ Server** field, type the last digit of the IP address for that computer. To remove the default DMZ server, enter 0 (zero).

2. Select the **Default DMZ Server** check box, and click **Apply**.

Responding to a Ping on the Internet (WAN) Port

If you want the router to respond to a ping from the Internet, select the **Respond to Ping on Internet Port** check box. This should be used only as a diagnostic tool, since it allows your router to be discovered by Internet scanners. Do not select this check box unless you have a specific reason to do so, such as when troubleshooting your connection.

Setting the MTU Size

The normal MTU value for most Ethernet networks is 1500 bytes, 1492 bytes for PPPoE connections, or 1450 for PPTP connections. For some ISPs, you might need to reduce the MTU size, but this is rarely required and should not be done unless you are sure it is necessary for your ISP connection. For more information, see "Changing the MTU Size" on page 5-21.

To change the MTU size:

1. In the **MTU Size** field, enter a new size between 64 and 1500.

2. Click **Apply** to save the new configuration.

Configuring NAT Filtering

Network Address Translation (NAT) determines how the router processes inbound traffic. Secured NAT provides a secured firewall to protect the computers on the LAN from attacks from the Internet, but might prevent some Internet games, point-to-point applications, or multimedia applications from functioning. Open NAT provides a much less secured firewall, but allows almost all Internet applications to function. For more information about NAT, see "How Your Computer Accesses a Remote Computer through Your Router" on page 5-2.

To change the NAT option:

1. In the NAT Filtering area, select either the **Secured** or the **Open** radio button.

2. Click **Apply** to save the new configuration.

Configuring Static Routes

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

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

*   Your primary Internet access is through a cable modem to an ISP.

*   You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.1.100.

*   Your company's network address is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.1.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company's firewall.

In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.1.100.

In this example:

*   The **Destination IP Address** and **IP Subnet Mask** fields specify that this static route applies to all 134.177.x.x addresses.

- The **Gateway IP Address** field specifies that all traffic for these addresses should be forwarded to the ISDN router at 192.168.1.100.

- A **Metric** value of 1 will work since the ISDN router is on the LAN.

- **Private** is selected only as a precautionary security measure in case RIP is activated.

Select **Static Routes** under Advanced in the main menu. The Static Routes screen displays.

Figure 4-4

To add or edit a static route:

1. Click **Add** to expand the Static Routes screen.

Figure 4-5

2. In the **Route Name** field, type a name for this static route. (This is for identification purposes only.)

3. Select the **Private** check box if you want to limit access to the LAN only. If Private is selected, the static route is not reported in RIP.

4. Select the **Active** check box to make this route effective.

5. Type the IP address of the final destination.

6. Type the IP subnet mask for this destination.
   If the destination is a single host, type **255.255.255.255**.

7. Type the gateway IP address, which must be a router on the same LAN segment as the Wireless-G Router.

8. Type a number between 1 and 15 as the metric value.
   This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.

9. Click **Apply** to have the static route entered into the table.

Wireless Repeating (Also Called WDS)

The Wireless-G Router can be used with a wireless access point (AP) to build large bridged wireless networks. Wireless repeating is a type of Wireless Distribution System (WDS).

> ⚠️ **Warning:** If you use the wireless repeating function, your options for wireless security are limited to None or WEP. For more information about wireless security, see Chapter 2, "Safeguarding Your Network."

The following figure shows a wireless repeating scenario:

This wireless computer is associated with AP 1.

This wireless computer is associated with AP 2.

Internet

PCs

AP 2 is in Repeater mode.

Modem

Wireless Router (AP 1) is in Wireless Base Station mode.
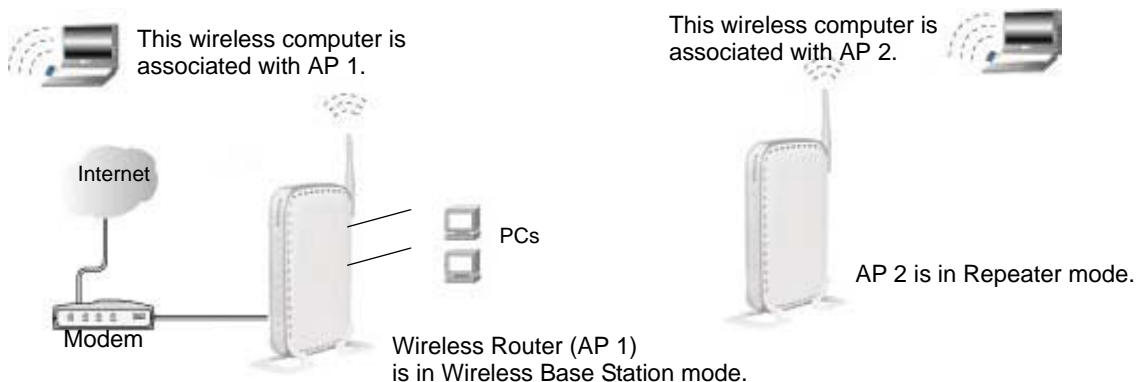
Figure 4-6

In the scenario shown, the following conditions must be met for both APs:

*   Both APs must use the same SSID, wireless channel, and encryption mode (see information about WEP in "Configuring WEP Wireless Security" on page 2-7").

*   Both APs must be on the same LAN IP subnet. That is, all the AP LAN IP addresses are in the same network.

*   All LAN devices (wired and wireless computers) must be configured to operate in the same LAN network address range as the APs.

Wireless Repeating Function

You can view or change wireless repeater settings for the wireless router. From the main menu of the browser interface, under Advanced, click **Wireless Repeating Function** to display the Wireless Repeating Function screen.

Figure 4-7

The wireless router supports two modes of the wireless repeating function, and allows you to control wireless client association:

*   **Wireless Base Station mode**. The wireless router acts as the parent AP, bridging traffic to and from the child repeater AP, as well as handling wireless and wired local computers. To configure this mode, you must know the MAC addresses of the child repeater AP.

*   **Wireless Repeater mode**. The wireless router sends all traffic from its local wireless or wired computers to a remote AP. To configure this mode, you must know the MAC address of the remote parent AP.

*   **Disable Wireless Client Association**. Usually this check box is cleared so that the router is an access point for wireless computers.

If this check box is selected, the router communicates wirelessly only with other APs whose MAC addresses are listed in this screen. The router still communicates with wire-connected LAN devices.

Setting Up the Base Station

The wireless repeating function works only in hub and spoke mode. The units cannot be daisy chained. You must know the wireless settings for both units. You must know the MAC address of the remote unit. First, set up the base station, and then set up the repeater.

To set up the base station:

1. Set up both units with exactly the same wireless settings (SSID, mode, channel, and security). Note that the wireless security option must be set to **None** or **WEP**.

2. From the main menu of the browser interface on the wireless router base unit, under Advanced, click **Wireless Repeating Function** to display the Wireless Repeating Function screen.

Figure 4-8

3. Select the **Enable Wireless Repeating Function** check box and the **Wireless Base Station** radio button.

4. Enter the MAC address for the repeater units.

5. Click **Apply** to save your changes.

Setting Up a Repeater Unit

Use a wired Ethernet connection to set up the repeater unit to avoid conflicts with the wireless connection to the base station.

> **Note:** If you are using the WGR614v10 base station with a non-NETGEAR wireless router as the repeater, you might need to change additional configuration settings. In particular, you should disable the DHCP server function on the wireless repeater AP.

To configure a Wireless-G Router as a repeater unit:

1. If you are using the same model of wireless router for both the base station and repeaters, you must change the LAN IP address for each repeater to a different IP address in the same subnet (see "Using the LAN IP Setup Options" on page 4-1).

   > **Note:** Failing to change the LAN IP address will cause an IP address conflict in the network because the factory default LAN IP is the same for both units.

2. Check the Wireless Settings screen, and verify that the wireless settings match the base unit exactly. The wireless security option must be set to **WEP** or **None**.

3. In the Wireless Repeating Function screen, select the **Enable Wireless Repeater Mode** radio button.

   This IP address must be in the same subnet as the base station but different from the LAN IP of the base station.

4. Fill in the **Base Station MAC Address** field.

5. Click **Apply** to save your changes.

6. Verify connectivity across the LANs.

   A computer on any wireless or wired LAN segment of the wireless router should be able to connect to the Internet or share files and printers with any other wireless or wired computer or server connected to the other AP.

Chapter 5
Fine-Tuning Your Network

This chapter describes how to modify the configuration of the Wireless-G Router Model WGR614v10 to allow specific applications to access the Internet or to be accessed from the Internet, and how to make adjustments to enhance your network's performance.

This chapter includes the following sections:

Allowing Inbound Connections to Your Network

By default, the Wireless-G Router blocks any inbound traffic from the Internet to your computers except for replies to your outbound traffic. However, you might need to create exceptions to this rule for the following purposes:

*   To allow remote computers on the Internet to access a server on your local network.
*   To allow certain applications and games to work correctly when their replies are not recognized by your router.

Your router provides two features for creating these exceptions: port forwarding and port triggering. This section explains how a normal outbound connection works, followed by two examples explaining how port forwarding and port triggering operate and how they differ.

How Your Computer Accesses a Remote Computer through Your Router

When a computer on your network needs to access a computer on the Internet, your computer sends your router a message containing source and destination address and process information. Before forwarding your message to the remote computer, your router must modify the source information and must create and track the communication session so that replies can be routed back to your computer.

Here is an example of normal outbound traffic and the resulting inbound responses:

1. You open Internet Explorer, beginning a browser session on your computer. Invisible to you, your operating system assigns a service number (port number) to every communication process running on your computer. In this example, let's say Windows assigns port number 5678 to this browser session.

2. You ask your browser to get a Web page from the Web server at www.example.com. Your computer composes a Web page request message with the following address and port information:

    *   The source address is your computer's IP address.

    *   The source port number is 5678, the browser session.

    *   The destination address is the IP address of www.example.com, which your computer finds by asking a DNS server.

    *   The destination port number is 80, the standard port number for a Web server process.

    Your computer then sends this request message to your router.

3. Your router creates an entry in its internal session table describing this communication session between your computer and the Web server at www.example.com. Before sending the Web page request message to www.example.com, your router stores the original information and then modifies the source information in the request message, performing Network Address Translation (NAT):

    *   The source address is replaced with your router's public IP address.
        This is necessary because your computer uses a private IP address that is not globally unique and cannot be used on the Internet.

    *   The source port number is changed to a number chosen by the router, such as 33333. This is necessary because two computers could independently be using the same session number.

    Your router then sends this request message through the Internet to the Web server at www.example.com.

4. The Web server at www.example.com composes a return message with the requested Web page data. The return message contains the following address and port information:

   • The source address is the IP address of www.example.com.

   • The source port number is 80, the standard port number for a Web server process.

   • The destination address is the public IP address of your router.

   • The destination port number is 33333.

   The Web server then sends this reply message to your router.

5. Upon receiving the incoming message, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router then modifies the message, restoring the original address information replaced by NAT. The message now contains the following address and port information:

   • The source address is the IP address of www.example.com.

   • The source port number is 80, the standard port number for a Web server process.

   • The destination address is your computer's IP address.

   • The destination port number is 5678, the browser session that made the initial request.

   Your router then sends this reply message to your computer, which displays the Web page from www.example.com.

6. When you finish your browser session, your router eventually senses a period of inactivity in the communications. Your router then removes the session information from its session table, and incoming traffic is no longer accepted on port number 33333.

How Port Triggering Changes the Communication Process

In the preceding example, requests are sent to a remote computer by your router from a particular service port number, and replies from the remote computer to your router are directed to that port number. If the remote server sends a reply back to a different port number, your router will not recognize it and will discard it. However, some application servers (such as FTP and IRC servers) send replies back to multiple port numbers. Using the port triggering function of your router, you can tell the router to open additional incoming ports when a particular outgoing port originates a session.

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port, but also sends an "identify" message to your computer on port 113. Using port triggering, you can tell the router,

"When you initiate a session with destination port 6667, you must also allow incoming traffic on port 113 to reach the originating computer." Using steps similar to the preceding example, the following sequence shows the effects of the port triggering rule you have defined:

1. You open an IRC client program, beginning a chat session on your computer.

2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your router.

3. Your router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.

4. Noting your port triggering rule, and having observed the destination port number of 6667, your router creates an additional session entry to send any incoming port 113 traffic to your computer.

5. The IRC server sends a return message to your router using the NAT-assigned source port (as in the previous example, let's say port 33333) as the destination port. The IRC server also sends an "identify" message to your router with destination port 113.

6. Upon receiving the incoming message to destination port 33333, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router restores the original address information replaced by NAT and sends this reply message to your computer.

7. Upon receiving the incoming message to destination port 113, your router checks its session table and learns that there is an active session for port 113, associated with your computer. The router replaces the message's destination IP address with your computer's IP address and forwards the message to your computer.

8. When you finish your chat session, your router eventually senses a period of inactivity in the communications. The router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

To configure port triggering, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application, or user groups or newsgroups.

> **Note:** Only one computer at a time can use the triggered application.

How Port Forwarding Changes the Communication Process

In both of the preceding examples, your computer initiates an application session with a server computer on the Internet. However, you might need to allow a client computer on the Internet to initiate a connection to a server computer on your network. Normally, your router ignores any inbound traffic that is not a response to your own outbound traffic. You can configure exceptions to this default rule by using the port forwarding feature.

A typical application of port forwarding can be shown by reversing the client-server relationship from our previous Web server example. In this case, a remote computer's browser needs to access a Web server running on a computer in your local network. Using port forwarding, you can tell the router, "When you receive incoming traffic on port 80 (the standard port number for a Web server process), forward it to the local computer at 192.168.1.123." The following sequence shows the effects of the port forwarding rule you have defined:

1. The user of a remote computer opens Internet Explorer and requests a Web page from www.example.com, which resolves to the public IP address of your router. The remote computer composes a Web page request message with the following destination information:

   • The destination address is the IP address of www.example.com, which is the address of your router.

   • The destination port number is 80, the standard port number for a Web server process.

   The remote computer then sends this request message through the Internet to your router.

2. Your router receives the request message and looks in its rules table for any rules covering the disposition of incoming port 80 traffic. Your port forwarding rule specifies that incoming port 80 traffic should be forwarded to local IP address 192.168.1.123. Therefore, your router modifies the destination information in the request message:

   The destination address is replaced with 192.168.1.123.

   Your router then sends this request message to your local network.

3. Your Web server at 192.168.1.123 receives the request and composes a return message with the requested Web page data. Your Web server then sends this reply message to your router.

4. Your router performs Network Address Translation (NAT) on the source IP address, and sends this request message through the Internet to the remote computer, which displays the Web page from www.example.com.

To configure port forwarding, you need to know which inbound ports the application needs. You usually can determine this information by contacting the publisher of the application or user groups or newsgroups.

How Port Forwarding Differs from Port Triggering

The following points summarize the differences between port forwarding and port triggering:

- Port triggering can be used by any computer on your network, although only one computer can use it at a time.
- Port forwarding is configured for a single computer on your network.
- Port triggering does not need to know the computer's IP address in advance. The IP address is captured automatically.
- Port forwarding requires that you specify the computer's IP address during configuration, and the IP address must never change.
- Port triggering requires specific outbound traffic to open the inbound ports, and the triggered ports are closed after a period of no activity.
- Port forwarding is always active and does not need to be triggered.

Configuring Port Forwarding to Local Servers

Using the port forwarding feature, you can allow certain types of incoming traffic to reach servers on your local network. For example, you might make a local Web server, FTP server, or game server visible and available to the Internet.

Use the Port Forwarding screen to configure the router to forward specific incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a default DMZ server to which all other incoming protocols are forwarded. The DMZ server is configured in the WAN Setup screen, as discussed in "Setting Up a Default DMZ Server" on page 4-6.

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

> **Tip:** To ensure that your server computer always has the same IP address, use the reserved IP address feature of your Wireless-G Router. See "Using Address Reservation" on page 4-3 for instructions on how to use reserved IP addresses.

To configure port forwarding to a local server:

1. Select **Port Forwarding/Port Triggering** under Advanced in the main menu.

Figure 5-1

2. From the **Service Name** list, select the service or game that you will host on your network. If the service does not appear in the list, see the following section, "Adding a Custom Service."

3. In the corresponding **Server IP Address** box, enter the last digit of the IP address of your local computer that will provide this service.

4. Click **Add**. The service appears in the list in the screen.

Adding a Custom Service

To define a service, game, or application that does not appear in the Service Name list, you must first determine which port number or range of numbers is used by the application. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups. When you have the port number information, follow these steps:

1. Select **Port Forwarding/Port Triggering** under Advanced in the main menu.

2. Click **Add Custom Service**.

Figure 5-2

3. In the **Service Name** field, enter a descriptive name.

4. In the **Service Type** field, select the protocol. If you are unsure, select **TCP/UDP**.

5. In the **Starting Port** field, enter the beginning port number.

- If the application uses only a single port, enter the same port number in the **Ending Port** field.

- If the application uses a range of ports, enter the ending port number of the range in the **Ending Port** field.

6. In the **Server IP Address** field, enter the IP address of your local computer that will provide this service.

7. Click **Apply**. The service appears in the list in the Port Forwarding/Port Triggering screen.

Editing or Deleting a Port Forwarding Entry

To edit or delete a port forwarding entry:

1. In the table, select the button next to the service name.

2. Click **Edit Service** or **Delete Service**.

Application Example: Making a Local Web Server Public

If you host a Web server on your local network, you can use port forwarding to allow Web requests from anyone on the Internet to reach your Web server.

To make a local Web server public:

1. Assign your Web server either a fixed IP address or a dynamic IP address using DHCP address reservation, as explained in "Using Address Reservation" on page 4-3. In this example, your router will always give your Web server an IP address of 192.168.1.33.

2. In the Port Forwarding screen, configure the router to forward the HTTP service to the local address of your Web server at **192.168.1.33**.
   HTTP (port 80) is the standard protocol for Web servers.

3. (Optional) Register a host name with a Dynamic DNS service, and configure your router to use the name as described in "Using a Dynamic DNS Service" on page 4-4.
   To access your Web server from the Internet, a remote user must know the IP address that has been assigned by your ISP. However, if you use a Dynamic DNS service, the remote user can reach your server by a user-friendly Internet name, such as mynetgear.dyndns.org.

Configuring Port Triggering

Port triggering is a dynamic extension of port forwarding that is useful in these cases:

- More than one local computer needs port forwarding for the same application (but not simultaneously).

- An application needs to open incoming ports that are different from the outgoing port.

When port triggering is enabled, the router monitors outbound traffic looking for a specified outbound "trigger" port. When the router detects outbound traffic on that port, it remembers the IP address of the local computer that sent the data. The router then temporarily opens the specified incoming port or ports, and forwards incoming traffic on the triggered ports to the triggering computer.

While port forwarding creates a static mapping of a port number or range to a single local computer, port triggering can dynamically open ports to any computer that needs them and can close the ports when they are no longer needed.

> **Note:** If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable Universal Plug and Play (UPnP) according to the instructions in "Using Universal Plug and Play" on page 5-12.

To configure port triggering, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

To set up port triggering:

1. Select **Port Forwarding/Port Triggering** under Advanced in the main menu. The Forwarding/Port Triggering screen displays.

2. Select the **Port Triggering** radio button. The port triggering information displays.

Figure 5-3

3. Clear the **Disable Port Triggering** check box.

> **Note:** If the Disable Port Triggering check box is selected after you configure port triggering, port triggering is disabled. However, any port triggering configuration information you added to the router is retained even though it is not used.

4. In the **Port Triggering Timeout** field, enter a value up to 9999 minutes. This value controls the inactivity timer for the designated inbound ports. The inbound ports close when the inactivity time expires. This is required because the router cannot be sure when the application has terminated.

5. Click **Add Service**.

Figure 5-4

6. In the **Service Name** field, type a descriptive service name.

7. In the **Service User** field, select **Any** (the default) to allow this service to be used by any computer on the Internet. Otherwise, select **Single address**, and enter the IP address of one computer to restrict the service to a particular computer.

8. Select the service type, either **TCP** or **UDP** or both (**TCP/UDP**). If you are not sure, select TCP/UDP.

9. In the **Triggering Port** field, enter the number of the outbound traffic port that will cause the inbound ports to be opened.

10. Enter the inbound connection port information in the **Connection Type**, **Starting Port**, and **Ending Port** fields.

11. Click **Apply**. The service appears in the Port Triggering Portmap table.

Using Universal Plug and Play

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, to access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

> **Note:** If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should enable UPnP.

To turn on Universal Plug and Play:

1. From the main menu of the browser interface, under Advanced, click **UPnP**. The UPnP screen displays.

Figure 5-5

2. The available settings and displays in this screen are:

   - **Turn UPnP On**. UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is disabled. If this check box is not selected, the router does not allow any device to automatically control the resources, such as port forwarding (mapping) of the router.

- **Advertisement Period**. The advertisement period is how often the router broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations might compromise the freshness of the device status but can significantly reduce network traffic.

- **Advertisement Time To Live**. The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. The time to live hop count is the number of steps a broadcast packet is allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it might be necessary to increase this value.

- **UPnP Portmap Table**. The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the router and which ports (Internal and External) that device has opened. The UPnP Portmap Table also displays what type of port is open and whether that port is still active for each IP address.

3. Click **Apply** to save your settings.

Optimizing Wireless Performance

The speed and operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless router. You should choose a location for your router that will maximize the network speed.

> **Note:** Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router. For complete range and performance specifications, click the link to the online document "Wireless Networking Basics" in Appendix B.

The following list describes how to optimize wireless router performance.

- **Identify critical wireless links.**
  If your network has several wireless devices, decide which wireless devices need the highest data rate, and locate the router near them. Many wireless products have automatic data-rate fallback, which allows increased distances without loss of connectivity. This also means that devices that are farther away might be slower. Therefore, the most critical links in your network are those where the traffic is high and the distances are great. Optimize those first.

- **Choose placement carefully.**
  For best results, place your router:

  - Near the center of the area in which your computers will operate.

  - In an elevated location such as a high shelf where the wirelessly connected computers have line-of-sight access (even if through walls).

  - Avoid obstacles to wireless signals.

  - Keep wireless devices at least 2 feet from large metal fixtures such as file cabinets, refrigerators, pipes, metal ceilings, reinforced concrete, and metal partitions.

  - Keep away from large amounts of water such as fish tanks and water coolers.

- **Reduce interference.**

  - Avoid windows unless communicating between buildings.

  - Place wireless devices away from various electromagnetic noise sources, especially those in the 2400–2500 MHz frequency band. Common noise-creating sources are:

    - Computers and fax machines (no closer than 1 foot)

    - Copying machines, elevators, and cell phones (no closer than 6 feet)

    - Microwave ovens (no closer than 10 feet)

- **Choose your settings.**

  - Use a scanning utility to determine what other wireless networks are operating nearby, and choose an unused channel.

  - Turn off SSID broadcast, and change the default SSID. Other nearby devices might automatically try to connect to your network several times a second, which can cause significant performance reduction.

- **Use WMM** to improve the performance of voice and video traffic over the wireless link.

Using WMM for Wireless Multimedia Applications

The Wireless-G Router supports Wi-Fi Multimedia (WMM) to prioritize wireless voice and video traffic over the wireless link. WMM provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM, both it and the client running that application must be WMM enabled. Legacy applications that do not support WMM, and applications that do not require, are assigned to the best effort category, which receives a lower priority than voice and video. WMM QoS is enabled by default.

Quality of Service

Quality of Service (QoS) is an advanced feature that can be used to prioritize some types of traffic ahead of others. The Wireless-G Router can provide QoS prioritization on the Internet connection. To configure QoS, use the QoS Setup screen.

From the main menu of the browser interface, under Advanced, select **QoS Setup**. The QoS Setup screen displays:
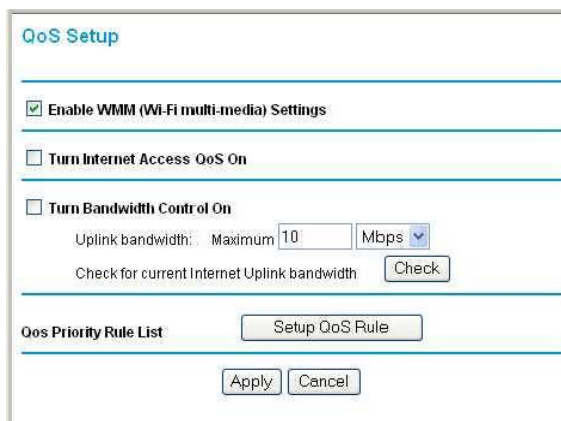
Figure 5-6

Using WMM QoS for Wireless Multimedia Applications

The Wireless-G Router supports Wi-Fi Multimedia Quality of Service (WMM QoS) to prioritize wireless voice and video traffic over the wireless link. WMM QoS provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both it and the client running that application must be WMM enabled. Legacy applications that do not support WMM, and applications that do not require QoS, are assigned to the best effort category, which receives a lower priority than voice and video.

WMM QoS is enabled by default. You can disable it in the QoS Setup screen, shown in Figure 5-6 on page 5-15, by clearing the **Enable WMM** check box and clicking **Apply**.

Configuring QoS for Internet Access

You can give prioritized Internet access to the following types of traffic:

- For specific applications
- For specific online games
- On individual Ethernet LAN ports of the router
- From a specific device by MAC address

To specify prioritization of traffic, you must create a policy for the type of traffic and add the policy to the QoS Policy table in the QoS Setup screen. For convenience, the QoS Policy table lists many common applications and online games that can benefit from QoS handling.

QoS for Applications and Online Gaming

To create a QoS policy for applications and online games:

1. From the main menu, under Advanced, select **QoS Setup**. The QoS Setup screen displays, as shown in Figure 5-6 on page 5-15.

2. Click **Setup QoS Rule**. The QoS Priority Rule List displays:

QoS Priority Rule List

	#	QoS Policy	Priority	Description
○	1	MSN Messenger	High	MSN Messenger application
○	2	Yahoo Messenger	High	Yahoo Messenger application
○	3	IP Phone	Highest	IP Phone application
○	4	Vonage IP Phone	Highest	Vonage IP Phone application
○	5	NetMeeting	High	NetMeeting application
○	6	AIM	High	AIM application
○	7	Google Talk	Highest	Google Talk application
○	8	Netgear EVA	Highest	Netgear EVA application
○	9	SSH	High	SSH application
○	10	Gnutella	Low	Gnutella application
○	11	BT / Azureus	Low	BT / Azureus application
○	12	Counter Strike	High	On-line gaming Counter Strike
○	13	Ages of Empires	High	On-line gaming Age of Empires
○	14	Everquest	High	On-line gaming Everquest
○	15	Quake 2	High	On-line gaming Quake 2
○	16	Quake 3	High	On-line gaming Quake 3
○	17	Unreal Tourment	High	On-line gaming Unreal Tourment
○	18	Warcraft	High	On-line gaming Warcraft

[Edit] [Delete] [Delete All]

[Add Priority Rule]

[Apply] [Cancel]

Figure 5-7

3. In the QOS Priority Rule List, select an existing item, or you can scroll to the bottom of the list and select **Add Priority Rule**.

a. If you chose to add a new entry, the screen expands as shown:

Figure 5-8

b. In the **QoS Policy for** field, enter a descriptive name for the new application or game.

c. Select the packet type, either **TCP, UDP,** or both (**TCP/UDP**), and specify the port number or range of port numbers used by the application or game.

4. From the **Priority** drop-down list, select the priority that this traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest.

5. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.

6. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.

7. Click **Apply**.
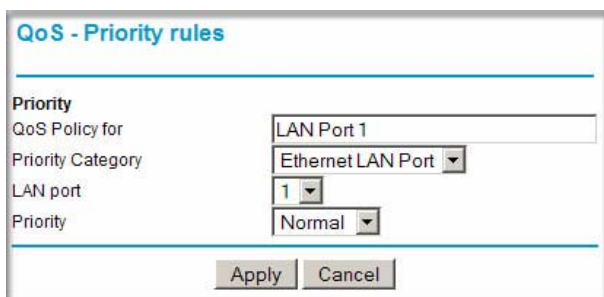
QoS for a Router LAN Port

To create a QoS policy for a device connected to one of the router's LAN ports:

1. From the main menu, under Advanced, select **QoS Setup**. The QoS Setup screen displays, as shown in .

2. Click **Setup QoS Rule** and then click **Add Priority Rule**.

3. On the QoS - Priority Rules screen, go to the Priority Category field, and select **Ethernet LAN Port** from the drop-down list:

Figure 5-9

4. From the **LAN port** list, select the LAN port that will have a QoS policy.

5. From the **Priority** drop-down list, select the priority that this port's traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest.

6. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.

7. Click **Apply**.

QoS for a MAC Address

To create a QoS policy for traffic from a specific MAC address:

1. From the main menu, under Advanced, select **QoS Setup**. The QoS Setup screen displays, as shown in .

2. Click **Setup QoS Rule** and then click **Add Priority Rule**.

3. On the QoS - Priority Rules screen, go to the Priority Category field, and select **MAC Address** from the drop-down list:

Figure 5-10

4. If the device to be prioritized appears in the MAC Device List, select it. The information from the MAC Device List is used to populate the policy name, MAC Address, and Device Name fields. If the device does not appear in the MAC Device List, click **Refresh**. If it still does not appear, you must complete these fields manually.

5. From the **Priority** drop-down list, select the priority that this device's traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest.

6. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.

7. Click **Apply**.

Editing or Deleting an Existing QoS Policy

To edit or delete an existing QoS policy:

1. From the main menu, under Advanced, select **QoS Setup**. The QoS Setup screen displays, as shown in Figure 5-6 on page 5-15.

2. Click **Setup QoS Rule**.

3. Select the radio button next to the QoS policy to be edited or deleted, and do one of the following:

- Click **Delete** to remove the QoS policy.

- Click **Edit** to edit the QoS policy. Follow the instructions in the preceding sections to change the policy settings.

4. Click **Apply** in the QoS Setup screen to save your changes.

Changing the MTU Size

The Maximum Transmission Unit (MTU) is the largest data packet a network device transmits. When one network device communicates across the Internet with another, the data packets travel through many devices along the way. If any device in the data path has a lower MTU setting than the other devices, the data packets must be split or "fragmented" to accommodate the one with the smallest MTU.

The best MTU setting for NETGEAR equipment is often just the default value, and changing the value might fix one problem but cause another. Leave MTU unchanged unless one of these situations occurs:

- You have problems connecting to your ISP, or other Internet service, and either the technical support of the ISP or of NETGEAR recommends changing the MTU size. These might require an MTU change:

    – A secure Web site that will not open, or displays only part of a Web page

    – Yahoo e-mail

    – MSN

    – America Online's DSL service

- You use VPN and have severe performance problems.

- You used a program to optimize MTU for performance reasons, and now you have connectivity or performance problems.

> **Note:** An incorrect MTU setting can cause Internet communication problems such as the inability to access certain Web sites, frames within Web sites, secure login pages, or FTP or POP servers.

If you suspect an MTU problem, a common solution is to change the MTU size to 1400. If you are willing to experiment, you can gradually reduce the MTU size from the maximum value of 1500 until the problem goes away. Table 5-1 describes common MTU sizes and applications.

Table 5-1. Common MTU Sizes

MTU	Application
1500	The largest Ethernet packet size and the default value. This is the typical setting for non-PPPoE, non-VPN connections, and is the default value for NETGEAR routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for pinging. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1460	Usable by AOL if you do not have large e-mail attachments, for example.
1436	Used in PPTP environments or with VPN.
1400	Maximum size for AOL DSL.
576	Typical value to connect to dial-up ISPs.

To change the MTU size:

1. In the main menu, under Advanced, select **WAN Setup**.

2. In the **MTU Size** field, enter a new size between 64 and 1500.

3. Click **Apply** to save the new configuration.

Overview of Home and Small Office Networking Technologies

Common connection types and their speed and security considerations are:

• **Broadband Internet**. Your Internet connection speed is determined by your modem type, such as ADSL or cable modem, as well as the connection speed of the sites to which you connect, and general Internet traffic. ADSL and cable modem connections are asymmetrical, meaning they have a lower data rate *to* the Internet (upstream) than *from* the Internet (downstream). Keep in mind that when you connect to another site that also has an asymmetrical connection, the data rate between your sites is limited by each side's upstream data rate. A typical residential ADSL or cable modem connection provides a downstream throughput of about 1 to 3 megabits per second (Mbps). Newer technologies such as ADSL2+ and Fiber to the Home (FTTH) will increase the connection speed to tens of Mbps.

- **Wireless**. Your Wireless-G Router Model WGR614v10 provides a wireless data throughput of up to 300 Mbps using technology called multiple input, multiple output (MIMO), in which multiple antennas transmit multiple streams of data. The use of multiple antennas also provides excellent range and coverage. With the introduction of the newer WPA and WPA2 encryption and authentication protocols, wireless security is extremely strong.

  To get the best performance, use RangeMax NEXT adapters such as the WN511B for your computers. Although the RangeMax NEXT router is compatible with older 802.11b and 802.11g adapters, the use of these older wireless technologies in your network can result in lower throughput overall (typically less than 10 Mbps for 802.11b and less than 40 Mbps for 802.11g). In addition, many older wireless products do not support the latest security protocols, WPA and WPA2.

- **Powerline**. For connecting rooms or floors that are blocked by obstructions or are distant vertically, consider networking over your building's AC wiring. NETGEAR's Powerline HD family of products delivers up to 200 Mbps to any outlet, while the older-generation XE family of products delivers 14 Mbps or 85 Mbps. Data transmissions are encrypted for security, and you can configure an individual network password to prevent neighbors from connecting.

  The Powerline HD family of products can coexist on the same network with older-generation XE family products or HomePlug 1.0 products, but they are not interoperable with these older products.

- **Wired Ethernet**. As gigabit-speed Ethernet ports (10/100/1000 Mbps) become common on newer computers, wired Ethernet remains a good choice for speed, economy, and security. Gigabit Ethernet can extend up to 100 meters with twisted-pair wiring of Cat 5e or better. A wired connection is not susceptible to interference, and eavesdropping would require a physical connection to your network.

> **Note:** Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, can lower actual data throughput rate.

Assessing Your Speed Requirements

Because your Internet connection is likely to operate at a much lower speed than your local network, faster local networking technologies might not improve your Internet experience. However, many emerging home applications require high data rates. For example:

- Streaming HD video requires 10 to 30 Mbps per stream. Because latency and packet loss can disrupt your video, plan to provide at least twice the capacity you need.

•   Streaming MP3 audio requires less than 1 Mbps per stream and does not strain most modern networks. Like video, however, streaming audio is also sensitive to latency and packet loss, so a congested network or a noisy link can cause problems.

•   Backing up computers over the network has become popular due to the availability of inexpensive mass storage. Table 5-2 shows the time to transfer 1 gigabyte (1 GB) of data using various networking technologies.

Table 5-2.   Theoretical Transfer Time for 1 Gigabyte

Network Connection	Theoretical Raw Transfer Time
Gigabit wired Ethernet	8 seconds
RangeMax NEXT Wireless-N	26 seconds
Powerline HD	40 seconds
100 Mbps wired Ethernet	80 seconds
802.11n wireless	45 seconds
802.11g wireless	150 seconds
802.11b wireless	700 seconds
10 Mbps wired Ethernet	800 seconds
Cable modem (3 Mbps)	2700 seconds
Analog modem (56 kbps)	144,000 seconds (40 hours)

Chapter 6
Using Network Monitoring Tools

This chapter describes how to use the maintenance features of your Wireless-G Router Model WGR614v10. You can access these features by selecting the items under Maintenance in the main menu of the browser interface.

This chapter includes the following sections:

Viewing Wireless Router Status Information

To view router status and usage information:

1. From the main menu of the browser interface, under Maintenance, select **Router Status**. The Router Status screen displays.

Figure 6-1

Table 6-1 describes the router status fields.

Table 6-1. Wireless Router Status Fields

Field		Description
Account Name		The host name assigned to the router.
Hardware Version		The hardware version of the router.
Firmware Version		The version of the current software installed in the router. This will change if you upgrade your router.
Internet Port		These settings apply to the Internet (WAN) port of the router.
	MAC Address	The Media Access Control address. This is the unique physical address being used by the Internet (WAN) port of the router.
	IP Address	The IP address being used by the Internet (WAN) port of the router. If no address is shown, or is 0.0.0.0, the router cannot connect to the Internet.
	DHCP	If set to None, the router is configured to use a fixed IP address on the WAN. If set to DHCP Client, the router is configured to obtain an IP address dynamically from the ISP.
	IP Subnet Mask	The IP subnet mask being used by the Internet (WAN) port of the router. For an explanation of subnet masks and subnet addressing, click the link to the online document "TCP/IP Networking Basics" in Appendix B.
	Domain Name Server	The Domain Name Server addresses being used by the router. A Domain Name Server translates human-language URLs such as www.netgear.com into IP addresses.

Table 6-1. Wireless Router Status Fields (continued)

Field		Description
LAN Port		These settings apply to the Ethernet (LAN) port of the router.
	MAC Address	The Media Access Control address. This is the unique physical address being used by the LAN port of the router.
	IP Address	The IP address being used by the Ethernet (LAN) port of the router. The default is 192.168.1.1.
	DHCP	Identifies whether the router's built-in DHCP server is active for the LAN-attached devices.
	IP Subnet Mask	The IP subnet mask being used by the Ethernet (LAN) port of the router. The default is 255.255.255.0.
Wireless Port		These settings apply to the wireless port of the router.
	Name (SSID)	The wireless network name (SSID) being used by the wireless port of the router. The default is NETGEAR.
	Region	The geographic region where the router is being used. It might be illegal to use the wireless features of the router in some parts of the world.
	Channel	Identifies the channel of the wireless port being used. Click the link to the online document "Wireless Networking Basics" in Appendix B for the frequencies used on each channel.
	Mode	Indicates the wireless communication mode: b and g; g only.
	Wireless AP	Indicates whether the radio feature of the router is enabled. If not enabled, the Wireless LED on the front panel is off.
	Broadcast Name	Indicates whether the router is broadcasting its SSID.

2. Click **Connection Status** to display the connection status.

Figure 6-2

Table 6-2 describes the connection status settings.

Table 6-2. Connection Status Settings

Item	Description
IP Address	The IP address that is assigned to the router.
Subnet Mask	The subnet mask that is assigned to the router.
Default Gateway	The IP address for the default gateway that the router communicates with.
DHCP Server	The IP address for the Dynamic Host Configuration Protocol server that provides the TCP/IP configuration for all the computers that are connected to the router.
DNS Server	The IP address of the Domain Name Service server that provides translation of network names to IP addresses.
Lease Obtained	The date and time that the lease was obtained.
Lease Expires	The date and time that the lease will expire.

Click the **Release** button to release the connection status items (that is, all items return to 0).

Click the **Renew** button to renew to the connection status items (that is, all items are refreshed).

Click the **Close Window** button to close the Connection Status screen.

3. Click **Show Statistics** to display router usage statistics.

Figure 6-3

Table 6-3 describes the router statistics.

Table 6-3. Router Statistics
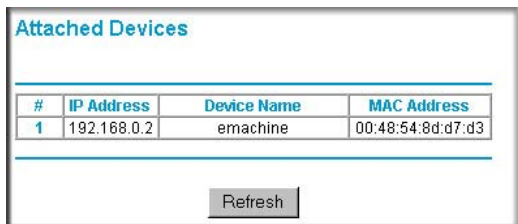
Item		Description
System Up Time		The time elapsed since the router was last restarted.
Port		The statistics for the WAN (Internet) and LAN (Ethernet) ports. For each port, the screen displays the following:
	Status	The link status of the port.
	TxPkts	The number of packets transmitted on this port since reset or manual clear.
	RxPkts	The number of packets received on this port since reset or manual clear.
	Collisions	The number of collisions on this port since reset or manual clear.
	Tx B/s	The current transmission (outbound) bandwidth used on the WAN and LAN ports.
	Rx B/s	The current reception (inbound) bandwidth used on the WAN and LAN ports.
	Up Time	The time elapsed since this port acquired the link.
Poll Interval		The intervals at which the statistics are updated in this screen.

To change the polling frequency, enter a time in seconds in the **Poll Interval** field, and click **Set Interval**.

To stop the polling entirely, click **Stop**.

Viewing a List of Attached Devices

The Attached Devices screen contains a table of all IP devices that the router has discovered on the local network. From the main menu of the browser interface, under Maintenance, select **Attached Devices** to view the table.

Figure 6-4

For each device, the table shows the IP address, NetBIOS host name or device name (if available), and the Ethernet MAC address. To force the router to look for attached devices, click **Refresh**.
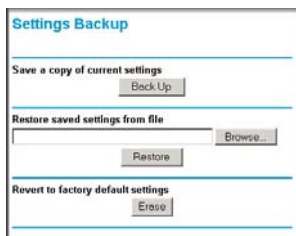
> **Note:** If the router is rebooted, the table data is lost until the router rediscovers the devices.

Managing the Configuration File

The configuration settings of the Wireless-G Router are stored within the router in a configuration file. You can back up (save) this file to your computer, restore it, or reset it to the factory default settings.

From the main menu of the browser interface, under Maintenance, select **Backup Settings**.

Figure 6-5

v1.0, February 2010

The following sections describe the three available options.

Backing Up and Restoring the Configuration

The Restore and Backup options in the Settings Backup screen let you save and retrieve a file containing your router's configuration settings.

To save your settings, click **Back Up**. Your browser extracts the configuration file from the router and prompts you for a location on your computer to store the file. You can give the file a meaningful name at this time, such as comcast.cfg.

> **Tip:** Before saving your configuration file, change the administrator password to the default, **password**. Then change it again after you have saved the configuration file. If you forget the password, you will need to reset the configuration to factory defaults.

To restore your settings from a saved configuration file, enter the full path to the file on your computer, or click **Browse** to browse to the file. When you have located it, click **Restore** to send the file to the router. The router then reboots automatically.

> **Warning:** Do not interrupt the reboot process.

Erasing the Configuration

Under some circumstances (for example, if you move the router to a different network or if you have forgotten the password) you might want to erase the configuration and restore the factory default settings. After an erase, the router's username is **admin**, the password is **password**, the LAN IP address is **192.168.1.1** (or **192.168.1.1**), and the router's DHCP server is enabled.

To erase the configuration, click the **Erase** button in the Settings Backup screen.

To restore the factory default configuration settings when you do not know the login password or IP address, you must use the restore factory settings button on the rear panel of the router (see).

Upgrading the Router Software

The routing software (also called firmware) of the Wireless-G Router is stored in flash memory, and can be upgraded as NETGEAR releases new software. Your router can download and install the new software, or you can download upgrade files from the NETGEAR website and manually send the upgrade file to the router using your browser.

> **Tip:** To ensure that you are always using the latest router firmware, enable the Firmware Upgrade Assistant feature so that the router will automatically detect a new version of the firmware on the Internet and alert you to its availability.

The Checking for Firmware Updates screen appears at login unless you clear the **Check for Updated Firmware Upon Log-in** check box.
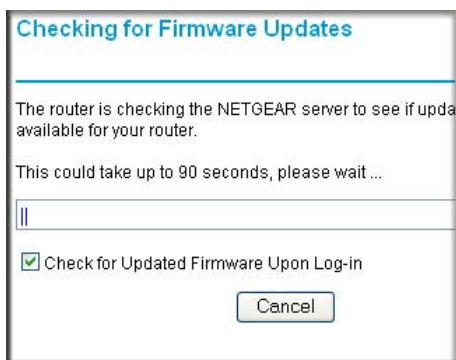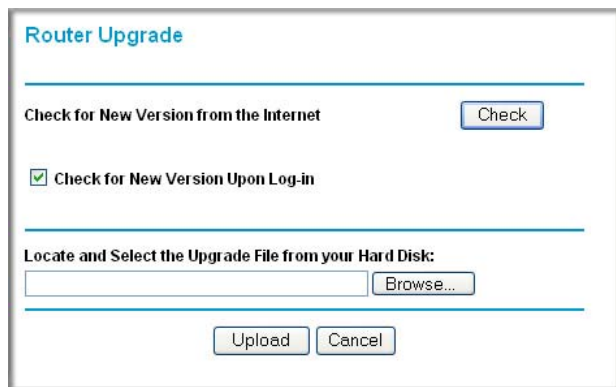
Figure 6-6

A screen is also provided for upgrading the router. From the main menu of the browser interface, under Maintenance, select **Router Upgrade** to display the Router Upgrade screen.

Figure 6-7

From this screen, you can check for new software versions by clicking the **Check** button. If a new version is found, you can download and install it in one step. To enable the Smart Wizard to automatically check for a new software version upon login, select the **Check for New Version Upon Log-in** check box.

Alternatively, you can manually install an upgrade file stored on your computer.

> **Tip:** Before upgrading the router software, use the router Settings Backup screen to save your configuration settings. A router upgrade might cause the router settings to revert to the factory defaults. If this happens, after completing the upgrade, you can restore your settings from the backup.

Upgrading Automatically to New Router Software

If you have selected **Check for New Version Upon Log-in**, your router alerts you to the new software when you log in. Otherwise, you can click the **Check** button in the Router Upgrade screen to search for new software.

If the router discovers a newer version of software, the message on the left displays when you log in. If no new software is available, the message on the right displays.

Firmware Version Check

A New Firmware Version is Found.

Do You Want to Upgrade to the New Version Now?

Current Version   V1.0.3.5

New Version   V1.0.3.8

     Yes   No

Firmware Version Check

No New Firmware Version Available.

Back
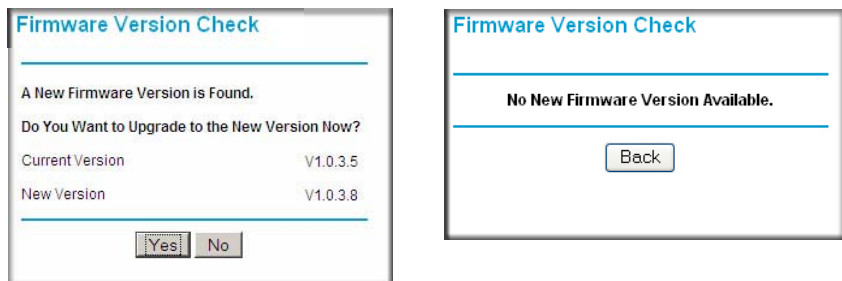
Figure 6-8

To automatically upgrade to the new software, click **Yes** to allow the router to download and install the new software file from NETGEAR.

> ⚠️ **Warning:** When uploading software to the Wireless-G Router, *do not* interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the software.

When the upload is complete, your router automatically restarts. The upgrade process typically takes about 1 minute. Read the new software release notes to determine whether you must reconfigure the router after upgrading.

Upgrading Manually to New Router Software

To manually select, download, and install new software to your router:

1. Under Maintenance on the main menu, select **Router Status**. Note the version number of your router firmware.

2. Go to the WGR614v10 support page on the NETGEAR website at *http://www.netgear.com/support*.

3. Check the most recent firmware version offered against the firmware version shown on your Router Status screen.

4. If the version on the NETGEAR website is more recent, download the file to your computer.

5. Under Maintenance on the main menu, select **Router Upgrade**.
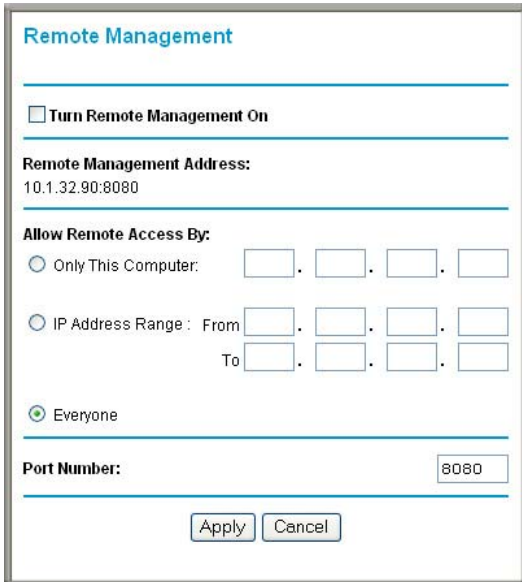
6. Click **Browse**, and locate the firmware image that you downloaded to your PC (the file ends in .img or .chk).

7. Click **Upload** to send the firmware to the router.

> ⚠️ **Warning:** When uploading software to the Wireless-G Router, *do not* interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the software.

When the upload is complete, your router automatically restarts. The upgrade process typically takes about 1 minute. Read the new software release notes to determine whether you must reconfigure the router after upgrading.

Enabling Remote Management Access

Using the Remote Management feature, you can allow a user on the Internet to configure, upgrade, and check the status of your Wireless-G Router. From the main menu of the browser interface, under Advanced, select **Remote Management**.

Figure 6-9

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

To configure your router for remote management:

1. Select the **Turn Remote Management On** check box.

2. Under Allow Remote Access By, specify what external IP addresses will be allowed to access the router's remote management.

> **Note:** For enhanced security, restrict access to as few external IP addresses as practical.

- To allow access from any IP address on the Internet, select **Everyone**.

- To allow access from a range of IP addresses on the Internet, select **IP Address Range**. Enter a beginning and ending IP address to define the allowed range.

- To allow access from a single IP address on the Internet, select **Only This Computer**. Enter the IP address that will be allowed access.

3. Specify the port number for accessing the management interface.

Normal Web browser access uses the standard HTTP service port 80. For greater security, enter a custom port number for the remote management Web interface. 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.

> **Note:** When accessing your router from the Internet, type your router's WAN IP address into your browser's address or location field, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, then enter **http://134.177.0.123:8080** in your browser.

Traffic Meter

Traffic Metering allows you to monitor the volume of Internet traffic passing through your router's Internet port. With the Traffic Meter utility, you can set limits for traffic volume, set a monthly limit, and get a live update of traffic usage.

To monitor traffic on your router, do the following:

1. On the Advanced menu, click **Traffic Meter**.

Figure 6-10

2. To enable the Traffic Meter, click the **Enable Traffic Meter** check box.

3. If you would like to record and restrict the volume of Internet traffic, click the **Traffic volume control by** radio button. You can select one of the following options for controlling the traffic volume:

   • No Limit – No restriction is applied when the traffic limit is reached.

   • Download only – The restriction is applied to incoming traffic only.

   • Both Directions – The restriction is applied to both incoming and outgoing traffic.

4. You can limit the amount of data traffic allowed per month:

   • By specifying how many Mbytes per month are allowed.

   • By specifying how many hours of traffic are allowed.

5. Set the **Traffic Counter** to begin at a specific time and date.

6. Set up **Traffic Control** to issue a warning message before the month limit of Mbytes or Hours is reached. You can select one of the following to occur when the limit is attained:

   • The Internet LED flashes green or amber.

   • The Internet connection is disconnected and disabled.

7. Set up **Internet Traffic Statistics** to monitor the data traffic.

8. Click the **Traffic Status** button if you want a live update on Internet traffic status on your router.

9. Click **Apply** to save your settings.

Chapter 7
Troubleshooting

This chapter provides information about troubleshooting your Wireless-G Router Model WGR614v10. After each problem description, instructions are provided to help you diagnose and solve the problem. As a first step, please review the Quick Tips.

> **Tip:** NETGEAR provides helpful articles, documentation, and the latest software updates at *http://www.netgear.com/support*.

This chapter includes the following sections:

Troubleshooting Quick Tips

This section describes tips for troubleshooting some common problems:

Be sure to restart your network in this sequence.

1. Turn off *and* unplug the modem.

2. Turn off the wireless router and computers.

3. Plug in the modem and turn it on. Wait 2 minutes.

4. Turn on the wireless router and wait 1 minute.

5. Turn on the computers.

Make sure that the Ethernet cables are securely plugged in.

• The Internet status light on the wireless router is on if the Ethernet cable connecting the wireless router and the modem is plugged in securely and the modem and wireless router are turned on.

• For each powered-on computer connected to the wireless router by an Ethernet cable, the corresponding numbered router LAN port light is on.

Make sure that the wireless settings in the computer and router match exactly.

• For a wirelessly connected computer, the wireless network name (SSID) and WEP or WPA security settings of the router and wireless computer must match exactly.

• If you have enabled the wireless router to restrict wireless access by MAC address, you must add the wireless computer's MAC address to the router's wireless card access list.

Make sure that the network settings of the computer are correct.

• Wired and wirelessly connected computers *must* have network (IP) addresses on the same network as the router. The simplest way to do this is to configure each computer to obtain an IP address automatically using DHCP. Click the link to the online document "Preparing Your Network" in Appendix B, or see the documentation that came with your computer.

• Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. Your wireless router can capture and use that MAC address, as described in "Configuring Your Internet Connection Using the Setup Wizard" on page 1-6.

Check the Test light to verify correct router operation.

If the Test light does not turn off within 2 minutes after you turn the router on, reset the router according to the instructions in "Restoring the Default Configuration and Password" on page 7-13.

Troubleshooting Basic Functions

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

1. When power is first applied, verify that the Power light $\boxed{\text{⏻}}$ is on.

2. After approximately 10 seconds, verify that:

   a. The Power light is solidly on.

   b. The Internet light is on.

   c. A numbered LAN port light is on for any local port that is connected to a computer. This indicates that a link has been established to the connected device.

If any of the above conditions does not occur, see the appropriate following section.

The Power light is not on or is blinking.

If the Power and other lights are off when your router is turned on:

- Make sure that the power cord is properly connected to your router and that the power adapter is properly connected to a functioning power outlet.

- Check that you are using the 12V DC 1A power adapter that NETGEAR supplied for this product.

- If the Power light blinks alternately green and amber every second, the router software is corrupted. This can happen if a firmware upgrade is interrupted, or if the router detects a problem with the firmware. For recovery instructions, contact Technical Support at *www.netgear.com/support*.

If the error persists, you have a hardware problem and should contact Technical Support at *www.netgear.com/support*.

The lights never turn off.

When the router is turned on, the lights turn on for about 10 seconds and then turn off. If all the lights stay on, there is a fault within the router.

If all lights are still on 1 minute after power-up:

- Cycle the power to see if the router recovers.

- Clear the router's configuration to factory defaults as explained in "Restoring the Default Configuration and Password" on page 7-13.

v1.0, February 2010

If the error persists, you might have a hardware problem and should contact Technical Support at *www.netgear.com/support*.

The Internet or Ethernet port lights are not on.

If either the Ethernet port lights or the Internet light does not come on when the Ethernet connection is made, check the following:

• Make sure that the Ethernet cable connections are secure at the router and at the modem or computer.

• Make sure that power is turned on to the connected modem or computer.

• Make sure that you are using the correct cable:

When connecting the router's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

The Wireless light is not on.

If the Wireless light does not come on, verify that the wireless feature is turned on according to the instructions in "Viewing Advanced Wireless Settings" on page 2-10.

Troubleshooting the Web Configuration Interface

If you are unable to access the router's Web Configuration Interface from a computer on your local network, check the following:

• If you are connecting from a wireless computer, try connecting from a wired computer.

• Check the Ethernet connection between the wired computer and the router as described in "Troubleshooting Basic Functions" on page 7-3.

• Make sure that your computer's IP address is on the same subnet as the router. For instructions, click the link to the online document "Preparing Your Network" in Appendix B to configure your computer.

> **Note:** If your computer's IP address is shown as 169.254.x.x: Windows and Mac OS generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in subnet 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router, and reboot your computer.

• Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.

• Try closing the browser and opening it again, or try a different browser.

• Make sure that you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when entering this information.

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

• When entering configuration settings, be sure to click **Apply** before moving to another screen or tab, or your changes could be lost.

• Click **Refresh** or **Reload** in the Web browser. The changes might have occurred, but the Web browser might be caching the old configuration.

Troubleshooting the Internet Connection

If you can access your router but you are unable to access the Internet, you should first determine whether the router can obtain an IP address from your Internet Service Provider (ISP). Unless your ISP provides a static IP address, your router must request an IP address from the ISP. You can determine whether the request was successful using the Web Configuration Manager.

To check the WAN IP address:

1. Start your browser, and select an external site such as *http://www.netgear.com*.

2. Access the main menu of the router's configuration at *http://www.routerlogin.net*.

3. Under Maintenance, select **Router Status**.

4. Check that an IP address is shown for the Internet port. If 0.0.0.0 is shown, your router has not obtained an IP address from your ISP.

If your router is unable to obtain an IP address from the ISP, you might need to force your cable or DSL modem to recognize your new router by restarting your network, as described in "Be sure to restart your network in this sequence." on page 7-1.

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

• Your ISP might require a login program.
Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.

- If your ISP requires a login, the login name or password might be set incorrectly.

- Your ISP might check for your computer's host name.
  Assign the computer host name of your ISP account as the account name in the Basic Settings screen.

- Your ISP allows only one Ethernet MAC address to connect to Internet and might check for your computer's MAC address. In this case, do one of the following:

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

  – Configure your router to spoof your computer's MAC address. This procedure is explained in "Configuring Your Internet Connection Using the Setup Wizard" on page 1-6.

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

- Your computer might not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically, your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your computer, and verify the DNS address as described in the online document you can access from "Preparing Your Network" in Appendix B. You can also configure your computer manually with DNS addresses, as explained in your operating system documentation.

- Your computer might not have the router configured as its TCP/IP gateway.

  If your computer obtains its information from the router by DHCP, reboot the computer, and verify the gateway address as described in the online document you can access from "Preparing Your Network" in Appendix B.

- You might be running login software that is no longer needed.

  If your ISP provided a program to log you in to the Internet (such as WinPoET), you no longer need to run that software after installing your router. You might need to go to Internet Explorer and select **Tools > Internet Options**, click the Connections tab, and select **Never dial a connection**.

Troubleshooting a Network Using the Ping Utility

Most network 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 network is made very easy by using the ping utility in your computer or workstation.

Testing the LAN Path to Your Router

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

To ping the router from a running Windows PC:

1. From the Windows toolbar, click Start, and then select **Run**.

2. In the field provided, type **ping** followed by the IP address of the router, as in this example:

   ping www.routerlogin.net

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

     – For a wired connection, make sure that the numbered LAN port light is on for the port to which you are connected. If the light is off, follow the instructions in "The Internet or Ethernet port lights are not on." on page 7-4.

     – Check that the corresponding Link lights are on for your network interface card. If your router and computer are connected to a separate Ethernet switch, make sure that the Link lights are on for the switch ports that are connected to your computer and router.

   • Wrong network configuration

     – Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.

– Verify that the IP address for your router and your computer are correct and that the addresses are on the same subnet.

Testing the Path from Your Computer to a Remote Device

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

1. From the Windows toolbar, click the Start button, and then select **Run**.

2. In the Windows Run window, 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 like those shown in the previous section are displayed. If you do not receive replies:

• Check that your computer has the IP address of your router listed as the default gateway. If the IP configuration of your computer is assigned by DHCP, this information is not be visible in your computer's Network Control Panel. Verify that the IP address of the router is listed as the default gateway as described in the online document you can access from "Preparing Your Network" in Appendix B.

• Check to see that the network address of your computer (the portion of the IP address specified by the subnet mask) is different from the network address of the remote device.

• Check that your cable or DSL modem is connected and functioning.

• If your ISP assigned a host name to your computer, enter that host name as the account name in the Basic Settings screen.

• Your ISP could be rejecting the Ethernet MAC addresses of all but one of your computers. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If this is the case, you must configure your router to "clone" or "spoof" the MAC address from the authorized computer. For more information, see "Configuring Your Internet Connection Using the Setup Wizard" on page 1-6.

Problems with Date and Time

Under Content Filtering in the main menu, select **E-mail** to display a screen that shows the current date and time of day. The Wireless-G Router uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include the following:

- Date shown is January 1, 2000.
  Cause: The router has not yet successfully reached a network time server. Check that your Internet access settings are correct. If you have just completed configuring the router, wait at least 5 minutes, and check the date and time again.

- Time is off by one hour.
  Cause: The router does not adjust for daylight savings time. In the E-mail screen, select the **Adjust for Daylight Savings Time** check box.

Solving Wireless Connection Problems

The first steps in solving wireless connection problems are these:

1. Using your wireless card's setup utility program, make sure that your wireless card can find your wireless router.

2. Configure and test with the simplest wireless connection possible, and then add security.

The topics in this section describe these steps.

Using Your Wireless Card Setup Program

When you install a NETGEAR wireless card in your computer, a Smart Wizard utility program is installed that can provide helpful information about your wireless network. You can find this program in your Windows Program menu or as an icon in your system tray. Other wireless card manufacturers might include a similar program.

If you have no specific wireless card setup program installed, you can use the basic setup utility in Windows by following these steps:

1. Open the Windows Control Panel, and double-click **Network Connections**.

2. In the LAN section, double-click **Wireless Network Connection**.

Use the setup program to scan for available wireless networks. Look for a network name (SSID) of NETGEAR or your custom SSID if you have changed it. If your wireless network does not appear, check these conditions:

- Is your router's wireless radio enabled? See "Viewing Advanced Wireless Settings" on page 2-10.
- Is your router's SSID broadcast enabled? See "Viewing Advanced Wireless Settings" on page 2-10.
- Is your router set to a wireless standard that is not supported by your wireless card? Check the Mode setting as described in "Viewing and Configuring Basic ISP Settings" on page 1-6.

If your wireless network appears, but the signal strength is weak, check these conditions:

- Is your router too far from your computer, or too close? Place your computer near the router, but at least 6 feet away, and see whether the signal strength improves.
- Is your wireless signal obstructed by objects between the router and your computer? See "Optimizing Wireless Performance" on page 5-13.

If your wireless network appears and has good signal strength, configure your wireless card and router for the simplest possible connection as described in the next section.

Setting Up and Testing Basic Wireless Connectivity

> **Note:** If you use a wireless computer to change wireless settings, you might be disconnected when you click **Apply**. Reconfigure your wireless adapter to match the new settings, or access the wireless router from a wired computer to make any further changes.

Follow these instructions to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.

1. Select **Wireless Settings** under Setup in the main menu of the WGR614v10 router.

Figure 7-1

2. For the wireless network name (SSID), use the default name, or choose a suitable descriptive name. In the **Name (SSID)** field, you can enter a value of up to 32 alphanumeric characters. The default SSID is NETGEAR.

> **Note:** The SSID is case-sensitive; NETGEAR is not the same as nETgear. Also, the SSID of any wireless access adapters must match the SSID you specify in the Wireless-G Router. If they do not match, you will not get a wireless connection to the Wireless-G Router.

3. Select the region in which the wireless interface will operate.

4. Set the channel. The default channel is **Auto**.
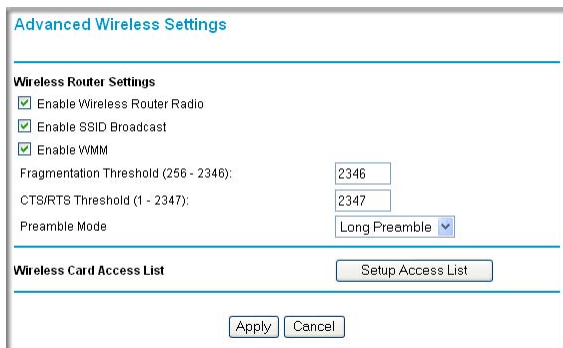
    This field determines which operating frequency is used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your router. For more information about the wireless channel frequencies, click the link to the online document "Wireless Networking Basics" in Appendix B.

5. Set the mode to **b and g**.

6. For Security Options, select **None**.

7. Click **Apply** to save your changes.

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

8. Select **Wireless Settings** under Advanced in the main menu of the WGR614v10 router.

Figure 7-2

9. Make sure that the **Enable Wireless Router Radio** and **Enable SSID Broadcast** check boxes are selected.

10. Click **Setup Access List**.

11. Make sure that the **Turn Access Control On** check box is *not* selected.

12. Configure and test your wireless computer for wireless connectivity.

Program the wireless adapter of your computer to have the same SSID and channel that you specified in the router, and disable encryption. Check that your computer has a wireless link and can obtain an IP address by DHCP from the router.

Once your computer has basic wireless connectivity to the router, you can configure the advanced wireless security functions of the computer and router (for more information about security, see Chapter 2, "Safeguarding Your Network").

Restoring the Default Configuration and Password

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

*   Use the Erase function of the router (see "Erasing the Configuration" on page 6-7).

*   Use the restore factory settings button on the rear panel of the router. Use this method for cases when the administration password or IP address is not known.

To restore the factory default configuration settings when you do not know the administration password or IP address, you must use the restore settings button on the rear panel of the router.

1. Press and hold the restore settings button for 10 seconds.

2. Release the restore settings button, and wait for the router to reboot.

If the wireless router fails to restart, or the Power light continues to blink or turns solid amber, the unit might be defective. If the error persists, you might have a hardware problem and should contact Technical Support at *http://www.netgear.com/support*.

Appendix A
Technical Specifications

This appendix provides technical specifications for the Wireless-G Router Model WGR614v10.

Specification	Description
Network Protocol and Standards Compatibility	
Data and routing protocols	TCP/IP, DHCP PPP over Ethernet (PPPoE)
Power Adapter	
North America	120V, 60 Hz, input
United Kingdom, Australia	230V, 50 Hz, input
Europe	230V, 50 Hz, input
Japan	100V, 50/60 Hz, input
All regions (output)	12V DC @ 1A output, 12W maximum
Physical Specifications	
Dimensions	28 x 175 x 119 mm (1.1 x 6.89 x 4.68 in.)
Weight	0.26 kg (0.57 lb)
Environmental Specifications	
Operating temperature	0° to 40° C (32º to 104º F)
Operating humidity	90% maximum relative humidity, noncondensing
Electromagnetic Emissions	
Meets requirements of	FCC Part 15 Class B
	EN301489, EN300328, EN60950 C-Tick
Interface Specifications	
LAN	10BASE-T or 100BASE-Tx, RJ-45
WAN	10BASE-T or 100BASE-Tx, RJ-45

Specification	Description
Wireless	
Radio data rates	1, 2, 5.5, 6, 9, 12, 18, 24, 36, 48, and 54 Mbps Auto Rate Sensing
Frequency	2.4-2.5Ghz
Data encoding	802.11b: Direct Sequence Spread Spectrum (DSSS) 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)
Maximum computers per wireless network	Limited by the amount of wireless network traffic each node generates. Typically 30–70 nodes.
Operating frequency ranges	2.412–2.462 GHz (US) 2.412–2.472 GHz (Japan) 2.412–2.472 GHz (Europe ETSI)
802.11 security	40-bit (also called 64-bit) and 128-bit WEP; and WPA-PSK, WPA2-PSK and WPA-PSK+WPA2-PSK
Default Factory Settings	
Wireless Access Point	Enabled
Wireless Access List (MAC filtering)	All wireless stations allowed
SSID Broadcast	Enabled
SSID	NETGEAR
11b/g RF Channel	11
Mode	g and b
Authentication Type	Open System
Security	Disabled

Appendix B
Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
TCP/IP Networking Basics	*http://documentation.netgear.com/reference/enu/tcpip/index.htm*
Wireless Networking Basics	*http://documentation.netgear.com/reference/enu/wireless/index.htm*
Preparing Your Network	*http://documentation.netgear.com/reference/enu/wsdhcp/index.htm*
Virtual Private Networking Basics	*http://documentation.netgear.com/reference/enu/vpn/index.htm*
Glossary	*http://documentation.netgear.com/reference/enu/glossary/index.htm*

In addition, you can find initial setup instructions for your wireless router in the .

Index