

Chapter 2

Safeguarding Your Network

The Wireless-G Router Model WGR614v9 provides highly effective security features, which are covered in detail in this chapter.

This chapter includes the following sections:

- [“Choosing Appropriate Wireless Security”](#)
- [“Recording Basic Wireless Settings Setup Information” on page 2-4](#)
- [“Changing Wireless Security Settings” on page 2-5](#)
- [“Viewing Advanced Wireless Settings” on page 2-10](#)
- [“Restricting Wireless Access by MAC Address” on page 2-11](#)
- [“Restricting Wireless Access by MAC Address” on page 2-11](#)
- [“Changing the Administrator Password” on page 2-14](#)
- [“Backing Up Your Configuration” on page 2-15](#)
- [“Understanding Your Firewall” on page 2-15](#)

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 802.11g/n 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.

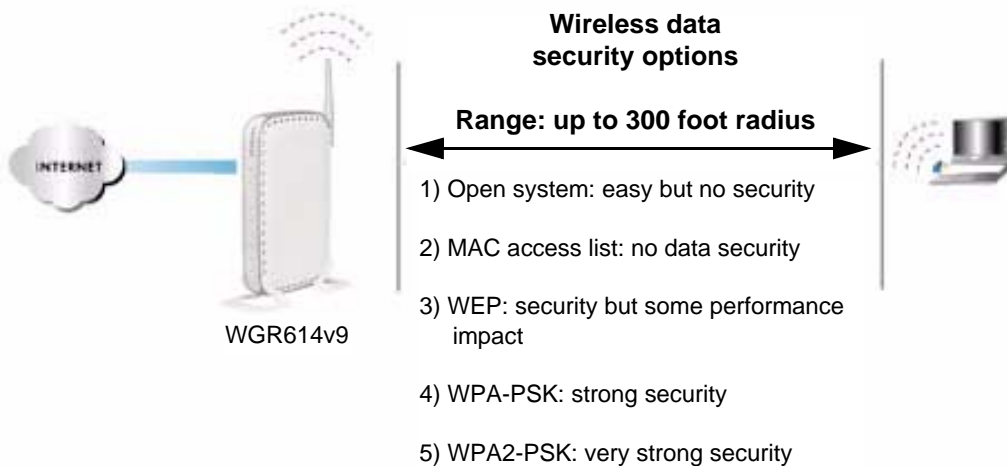
The time it takes to establish a wireless connection can vary depending on both your security settings and router placement.

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 2-14.



Note: Use these with other features that enhance security ([Table 2-2 on page 2-3](#)).

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 2-5), and the Advanced Wireless Settings screen, which you access under Advanced (see [“Changing Wireless Security Settings”](#) on page 2-5).

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 2-3](#). 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.
<p>WPA-PSK (TKIP). WPA-PSK standard encryption with TKIP encryption type.</p> <p>WPA2-PSK (AES). Wi-Fi Protected Access version 2 with Pre-Shared Key; WPA2-PSK standard encryption with the AES encryption type.</p> <p>WPA-PSK (TKIP) + WPA2-PSK (AES). Mixed mode.</p>	<p>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.</p> <p>For more information, see “Configuring WPA-PSK and WPA2-PSK Wireless Security” on page 2-9.</p>

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.

Table 2-2. Other Features That Enhance Security

Security Type	Description
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 2-15.

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.

Wireless Settings

Wireless Network

Name (SSID):

Region:

Channel:

Mode:

Security Options

None

WEP

WPA-PSK [TKIP]


WPA2-PSK [AES]

WPA-PSK [TKIP] + WPA2-PSK [AES]

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 WGR614v9 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.

Security Encryption (WEP)

Authentication Type:

Encryption Strength:

Security Encryption (WEP) Key

Passphrase:

Key 1:

Key 2:

Key 3:

Key 4:

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] + WPA2-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.

Security Options

None

WEP

WPA-PSK [TKIP]

WPA2-PSK [AES]

WPA-PSK [TKIP] + WPA2-PSK [AES]

Security Options (WPA-PSK + WPA2-PSK)

Passphrase:
(8-63 characters or 64 hexdigits)

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.

Advanced Wireless Settings

Wireless Router Settings

Enable Wireless Router Radio

Enable SSID Broadcast

Enable WMM

Fragmentation Threshold (256 - 2346):

CTS/RTS Threshold (1 - 2347):

Preamble Mode: ▾

Wireless Card Access List

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.

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



Figure 2-6

- 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.

Changing the Administrator Password

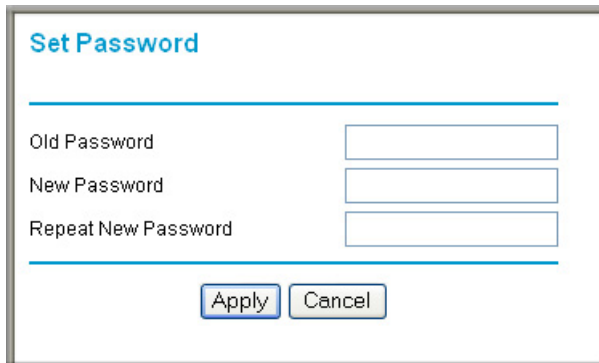
The default password for the router's Web Configuration Manager is **password**. NETGEAR recommends that you change this password to a more secure password.



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 6-6.

To change the administrator password:

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



The screenshot shows a web form titled "Set Password". It contains three input fields: "Old Password", "New Password", and "Repeat New Password". Below the fields are two buttons: "Apply" and "Cancel".

Figure 2-8

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 WGR614v9 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.