Chapter 2
Configuring Your Wireless Network and Security Settings

This chapter describes how to configure the wireless features of your DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router. For a wireless connection, the SSID, also called the wireless network name, and the wireless security setting must be the same for the modem router and wireless computers or wireless adapters. NETGEAR strongly recommends that you use wireless security.

This chapter includes:
- “Planning Your Wireless Network” on this page
- “Configuring Your Wireless Network” on page 2-4
- “Configuring Your Wireless Security” on page 2-10

Planning Your Wireless Network

For compliance and compatibility between similar products in your area, the operating channel and region must be set correctly.

To manually configure the wireless settings, you must know the following:
- SSID. The default SSID for the modem router is NETGEAR.
- The wireless mode (802.11n, 802.11g, or 802.11b) that each wireless adapter supports.
- Wireless security option. To successfully implement wireless security, check each wireless adapter to determine which wireless security option it supports.

Wireless Placement and Range Guidelines

The range of your wireless connection can vary significantly based on the physical placement of the modem router. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

For best results, place your modem router according to the following guidelines:

• Near the center of the area in which your PCs will operate.
• In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
• Away from sources of interference, such as PCs, microwave ovens, and 2.4 GHz cordless phones.
• Away from large metal surfaces.
• Put the antenna in a vertical position to provide the best side-to-side coverage. Put the antenna in a horizontal position to provide the best up-and-down coverage.
• If using multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use Channels 1 and 6, or 6 and 11).

The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

Wireless Security Options

Indoors, computers can connect over 802.11g wireless networks at a maximum range of up to 300 feet. Such distances can allow for others outside your immediate area to access your network.

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The modem router provides highly effective security features, which are covered in detail in this chapter. Deploy the security features appropriate to your needs.
There are several ways you can enhance the security of your wireless network:

- **Restrict access based on MAC address.** You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the modem router. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed (see “Restricting access by MAC address” on page 2-11).

- **Turn off the broadcast of the wireless network name SSID.** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies wireless network discovery feature of some products, such as Windows XP, but the data is still exposed (see “Hiding your wireless network name (SSID)” on page 2-11).

- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK (see “Configuring WEP” on page 2-14).

- **WPA-802.1x.** Wi-Fi Protected Access (WPA) with user authentication implemented using IEE 802.1x and RADIUS servers (see “Configuring WPA-802.1x” on page 2-16).

- **WPA-PSK (TKIP) + WPA2-PSK (AES).** Wi-Fi Protected Access (WPA) using a pre-shared key to perform authentication and generate the initial data encryption keys. The very strong authentication along with dynamic per frame re-keying of WPA makes it virtually impossible to compromise (see “Configuring Mixed WPA-PSK+WPA2-PSK Security” on page 2-13).
Configuring Your Wireless Network

You can view or manually configure the wireless settings and wireless security for the modem router in the Wireless Settings screen. If you want to make changes, make sure to note the current settings first. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.

| Note: | If you use a wireless computer to change the wireless network name (SSID) or wireless security settings, you will be disconnected when you click Apply. To avoid this problem, use a computer with a wired connection to access the modem router. |

To manually configure the wireless settings:

1. Log in to the modem router at its default LAN address of http://192.168.0.1 with its default user name of admin and default password of password, or using whatever LAN address and password you have set up.
Table 2-1 on page 2-7 describes the information that is displayed in the Wireless Settings screen.

3. Choose a suitable descriptive name for the wireless network name (SSID). In the SSID field, enter a value of up to 32 alphanumeric characters. The default SSID is **NETGEAR**.

**Note:** The SSID of any wireless access adapters must match the SSID you specify in the modem router. If they do not match, you will not get a wireless connection.
4. Select the region in which the wireless interface will operate.

5. Set the channel if necessary. The default channel is 11.

   This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your modem router. For more information about the wireless channel frequencies, see the online document that you can access from “Preparing Your Network” in Appendix A.

   | Note: Up to 270Mbps mode uses two channels, but in this mode only the first channel is listed in the channel pulldown menu. The associated channels in this mode are: 1+5, 2+6, 3+7, 4+8, 5+9, 6+10, and 7+11. When you select another wireless network mode, the channel pulldown displays all available channels: 1 through 13. However, available wireless channels depend on the selected wireless region. |

6. Select the mode in which the wireless interface will operate.

7. For initial configuration and test, leave the Wireless Card Access List set to allow everyone access by making sure that Turn Access Control On is not selected in the Wireless Station Access List. In addition, leave the encryption strength set to None.

8. Click Save to save your settings or click Apply to allow your changes to take effect immediately.

9. Configure and test your computers for wireless connectivity.

   Program the wireless adapter of your computers to have the same SSID and channel that you specified in the router. Check that they have a wireless link and can obtain an IP address by DHCP from the modem router.

Once your computers have basic wireless connectivity to the modem router, you can configure the advanced wireless security functions of the firewall.

Table 2-1 on page 2-7 shows the wireless settings.
Table 2-1. Wireless Settings

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| Wireless LAN              | The pulldown menu just below Wireless Settings allows for the selection of one of four wireless LANs (WLANs) with the following default names:  
  • NETGEAR  
  • NETGEAR2  
  • NETGEAR3  
  • NETGEAR4  
  You can change the default name of the selected WLAN in the Name (SSID) field.  
  Note: The region, channel, and mode can be set only for the primary wireless LAN (NETGEAR). In addition, access control can be turned on only for the primary wireless LAN. |
| Wireless Network          | Name (SSID)                                                                                                                                                                                                  |
|                           | The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive.  
  The default SSID is NETGEAR, but NETGEAR strongly recommends that you change your network name to a different value.  
  In a setting in which there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you that want to let participate in a wireless network must use the SSID. |
| Region                    | The location where the firewall is used. Select your region from the drop-down list. It might not be legal to operate the modem router in a region other than the regions shown here.  
  Note: The region can be set only for the primary wireless LAN (NETGEAR) but applies to all wireless LANs. |
| Channel                   | The wireless channel used by the gateway: 1 through 13. The available channels depend on the region setting.  
  Do not change the wireless channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, you might need to experiment with different channels to see which is the best. The default channel is 11.  
  The total number of channels varies by region. The mode that you select also determines how many channels are displayed in the channel pulldown menu.  
  Note: The channel can be set only for the primary wireless LAN (NETGEAR). |
### Table 2-1. Wireless Settings (continued)

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Network (continued)</td>
<td><strong>Mode</strong> Note: The mode can be set only for the primary wireless LAN (NETGEAR). <strong>Up to 270Mbps</strong> means that all 802.11g, 802.11b, and faster Draft-N wireless stations can be used. This mode expands the channel bandwidth from 20 MHz to 40 MHz to achieve the 270-Mbps rate. The router selects channel expansion on a frame-by-frame basis to avoid interference with the data transmissions of other access points or wireless stations. Up to 270Mbps mode uses two channels, but in this mode only the first channel is listed in the channel pulldown menu. The associated channels in this mode are: 1+5, 2+6, 3+7, 4+8, 5+9, 6+10, and 7+11. Up to 270Mbps mode is the fastest mode and is compatible with older wireless stations. <strong>Up to 130Mbps</strong> allows wireless stations that support speeds up to 130 Mbps. It is the default setting. In this case, the router transmits two streams with different data concurrently on the same channel. This mode restricts channel bandwidth to minimize interference with the data transmissions of other access points and wireless stations. <strong>g &amp; b</strong> allows older 802.11g and 802.11b wireless stations to access this device. You might want to select this mode if you have a wireless station that is using WEP security and does not support WPA-PSK or WPA2-PSK. <strong>g only</strong> allows only 802.11g wireless stations to access this device. <strong>b only</strong> allows only 802.11b wireless stations to access this device. However, note that in b only mode, 802.11g wireless stations can connect if they can operate in 802.11b mode.</td>
</tr>
<tr>
<td>Wireless Access Point</td>
<td><strong>Wireless Access Point Control</strong> <strong>Always On</strong> is selected by default. This setting enables the wireless radio, which allows the modem router to work as a wireless access point. The Wireless LED on the front of the modem router displays the current status of the wireless access point to let you know if it is disabled or enabled. The wireless access point must be enabled to allow wireless stations to access the Internet. <strong>Per Schedule Below (Use 24-hour clock)</strong>. You can specify when the Wireless Access Point is turned on and turned off by entering a start time in the <strong>Hour</strong> and <strong>Minute</strong> fields next to Turn on Wireless Access Point and an end time in the <strong>Hour</strong> and <strong>Minute</strong> fields next to Turn off Wireless Access Point. <strong>Always Off</strong>. Turning off the wireless radio can be helpful for configuration, network tuning, or troubleshooting.</td>
</tr>
</tbody>
</table>
### Wireless Settings (continued)

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Broadcast Name (SSID)</td>
<td>Selected by default, the modem router broadcasts its SSID, allowing wireless stations that have a null (blank) SSID to adopt the correct SSID. If you disable broadcast of the SSID, only devices with the correct SSID can connect. This nullifies the wireless network discovery feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers. For this reason NETGEAR recommends that you also enable wireless security.</td>
</tr>
<tr>
<td>Wireless Isolation</td>
<td>This feature is disabled by default. If it is enabled, wireless stations cannot communicate with each other or with stations on the wired network.</td>
</tr>
<tr>
<td>Turn Access Control On</td>
<td>Access control is disabled by default so that any computer configured with the correct wireless network name or SSID can access to your wireless network. For increased security, you can restrict access to the wireless network to only specific computers based on their MAC addresses. See “Restricting access by MAC address.” Note: Access control can be turned on only for the primary wireless LAN (NETGEAR).</td>
</tr>
<tr>
<td>Disable</td>
<td>Wireless security is not used.</td>
</tr>
<tr>
<td>WEP</td>
<td>In WEP (Wired Equivalent Privacy) mode you can select 64-bit or 128-bit data encryption. This mode has been superseded by WPA-PSK and WPA2-PSK, which should be selected if supported by your wireless client. See “Configuring WEP.”</td>
</tr>
<tr>
<td>WPA-PSK</td>
<td>WPA Pre-Shared-Key (Wi-Fi Protected Access Pre-Shared Key) uses a pre-shared key to perform the authentication and generate the initial data encryption keys. Then, it dynamically varies the encryption key. WPA-PSK uses TKIP (Temporal Key Integrity Protocol) data encryption, implements most of the IEEE 802.11i standard, and is designed to work with all wireless network interface cards, but not all wireless access points. See “Configuring Mixed WPA-PSK+WPA2-PSK Security.”</td>
</tr>
</tbody>
</table>
Configuring Your Wireless Security

This section discusses how to restrict wireless access to your network and how to configure wireless security such as Mixed WPA-PSK+WPA2-PSK, WEP, and WPA-802.1x.

Table 2-1. Wireless Settings (continued)

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Options</td>
<td>WPA Pre-Shared-Key (Wi-Fi Protected Access 2 with Pre-Shared Key) uses a pre-shared key to perform the authentication and generate the initial data encryption keys. Then, it dynamically varies the encryption key. WPA2-PSK provides the best throughput with 802.11N because the encryption is supported in the hardware. WPA2-PSK uses AES (Advanced Encryption Standard) data encryption, implements the full IEEE 802.11i standard, but does not work with some older wireless clients. See “Configuring Mixed WPA-PSK+WPA2-PSK Security.”</td>
</tr>
<tr>
<td>Mixed WPA-PSK+WPA2-PSK</td>
<td>Mixed WPA-PSK + WPA2-PSK uses both WPA-PSK + WPA2-PSK standard encryption. A high performance client such as the NETGEAR WN511B should connect using WPA2-PSK in order to achieve maximum performance. Wireless clients that connect to this router using WPA-PSK will run at reduced performance levels. See “Configuring Mixed WPA-PSK+WPA2-PSK Security.”</td>
</tr>
<tr>
<td>WPA-802.1x</td>
<td>In WPA-802.1x mode, user authentication is implemented using 802.1x and RADIUS servers. See “Configuring WPA-802.1x.”</td>
</tr>
</tbody>
</table>

Note: If you use a wireless computer to configure wireless security settings, you will be disconnected when you click Apply. Reconfigure your wireless computer to match the new settings, or access the modem router from a wired computer to make further changes.

Restricting Wireless Access to Your Network

By default, any wireless PC that is configured with the correct SSID can access your wireless network. For increased security, the modem router provides several ways to restrict wireless access to your network. You can do the following:

- Turn off wireless connectivity completely.
- Restrict access based on the wireless network name (SSID).
- Restrict access based on the Wireless Card Access List.
These options are discussed in the following sections.

**Turning off wireless connectivity completely**

You can completely turn off the wireless portion of the modem router. For example, if you use your notebook computer to wirelessly connect to your modem router and you take a business trip, you can turn off the wireless portion of the modem router while you are traveling. Other members of your household who use computers connected to the modem router through Ethernet cables can still use the modem router. To do this, clear the **Enable Wireless Access Point** check box on the Wireless Settings screen, and then click **Apply**.

**Hiding your wireless network name (SSID)**

By default, the modem router is set to broadcast its wireless network name (SSID). You can restrict wireless access to your network by not broadcasting the wireless network name (SSID). To do this, clear the **Allow Broadcast of Name (SSID)** check box on the Wireless Settings screen, and then click **Apply**. Wireless devices will not “see” your modem router. You must configure your wireless devices to match the wireless network name (SSID) of the modem router.

---

**Warning:** The SSID of any wireless access adapters must match the SSID you specify in the modem router. If they do not match, you will not get a wireless connection to the modem router.

---

**Restricting access by MAC address**

For increased security, you can restrict access to the wireless network to allow only specific PCs based on their MAC addresses. You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the Amodem router. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed. The Wireless Station Access list determines which wireless hardware devices will be allowed to connect to the modem router.
To restrict access based on MAC addresses:

1. Log in to the modem router at its default LAN address of http://192.168.0.1 with its default user name of admin and default password of password, or using whatever LAN address and password you have set up.

   ![Note: If you configure the modem router from a wireless computer, add your computer’s MAC address to the access list. Otherwise you will lose your wireless connection when you click Apply. You must then access the modem router from a wired computer, or from a wireless computer that is on the access control list, to make any further changes.]

2. In the Wireless Settings screen, under the Wireless Station Access List section, click the Setup Access List button to display the Wireless Station Access List.

   ![Figure 2-3](image)

   Figure 2-3

3. Select the Turn Access Control On check box to enable the restricting of wireless computers by their MAC addresses.

4. If the wireless station is currently connected to the network, you can select it from the Available Wireless Stations list. Click Add to add the station to the Trusted Wireless Stations list.
5. If the wireless station is not currently connected, you can enter its address manually. Enter the MAC address of the authorized computer. The MAC address is usually printed on the wireless card, or it might appear in the modem router’s DHCP table. The MAC address is 12 hexadecimal digits.

Click **Add** to add your entry. You can add several stations to the list. When you are finished adding stations, click **Apply**.

| **Note:** You can copy and paste the MAC addresses from the modem 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 modem router. The computer should then appear in the Attached Devices screen. |

| **Note:** If you are configuring the modem router from a wireless computer whose MAC address is not in the Trusted Wireless Stations list, and you select trusted wireless stations only, you will lose your wireless connection when you click **Apply**. You must then access the modem router from a wired computer to make any further changes. |

6. Make sure the **Turn Access Control On** check box is selected, and then click **Apply**.

Now, only devices on this list will be allowed to wirelessly connect to the modem router. This prevents unauthorized access to your network.

**Configuring Mixed WPA-PSK+WPA2-PSK Security**

A high-performance client such as the NETGEAR WN511B must connect to the modem router using WPA2-PSK to achieve maximum performance. Wireless clients that connect to the modem router using WPA-PSK run at no more than 802.11g speed. This option allows wireless clients to use either encryption method.

| **Note:** Not all wireless adapters support WPA or WPA2. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings. |
To configure Mixed WPA-PSK+WPA2-PSK:

1. Log in at the default LAN address of http://192.168.0.1, with the default user name of admin and default password of password, or using whatever LAN address and password you have set up.

2. Select Wireless Settings below Setup in the main menu of the modem router.

3. Select the Mixed WPA-PSK+WPA2-PSK radio button. The Wireless Settings screen expands to include the WPA2-PSK security encryption.

4. Enter the pre-shared key in the Network Key field using between 8 and 63 characters.

5. Click Save to save your settings or click Apply to allow your changes to take effect immediately.

For details about WPA-802.1x authentication options, see “Configuring WPA-802.1x” on page 2-16.

Choosing Alternative Authentication and Encryption Methods

Restricting wireless access prevents intruders from connecting to your network. However, the wireless data transmissions are still vulnerable to snooping. Using the data encryption settings described in this section will prevent a determined intruder from eavesdropping on your wireless data communications. Also, if you are using the Internet for such activities as purchases or banking, those Internet sites use another level of highly secure encryption called SSL. You can tell if a web site is using SSL because the Web address begins with HTTPS rather than HTTP.

Configuring WEP

Wired Equivalent Privacy (WEP) security is the most basic and simplest form of wireless security. It is the most often used, but least secure of the available options. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK.
To configure WEP data encryption:

1. Log in to the modem router at its default LAN address of http://192.168.0.1 with its default user name of admin and default password of password, or using whatever LAN address and password you have set up.

2. Select Wireless Settings in the main menu.

3. In the Security Options section of the screen, select WEP (Wired Equivalent Privacy). The WEP Security Encryption section displays.

![WEP Security Encryption](image)

*Figure 2-4*

4. Select the authentication type:
   - **Automatic.** This is the default setting.
   - **Open System.**
   - **Shared Key.**

5. Select the encryption strength setting:
   - **64-bit WEP.**
   - **128-bit WEP.**

6. Enter the encryption keys. 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. Enter a word or group of printable characters in the **Passphrase** field and click **Generate.** The four key boxes are automatically populated with key values.
- Manual. The number of hexadecimal digits that you must enter depends on the encryption strength setting:
  - 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 (any combination of 0–9, a–f, or A–F).

7. Select the radio button for the key you want to make active.

Be sure that you clearly understand how the WEP key settings are configured in your wireless adapter. Wireless adapter configuration utilities such as the one included in Windows XP allow entry of only one key, which must match the default key you set in the modem router.

8. Click **Save** to save your settings or click **Apply** to allow your changes to take effect immediately.

| Note: | When configuring the modem router from a wireless computer, if you specify WEP settings, you will lose your wireless connection when you click **Apply**. You must then either configure your wireless adapter to match the modem router WEP settings or access the modem router from a wired computer to make any further changes. |

---

### Configuring WPA-802.1x

This version of WPA requires the use of a RADIUS server for authentication. Each user (wireless client) must have a user login on the RADIUS server, and the modem router must have a client login on the RADIUS server. Data transmissions are encrypted using a key that is automatically generated.

1. Log in to the modem router at its default LAN address of [http://192.168.0.1](http://192.168.0.1) with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.

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

3. In the Security Options section of the screen, select **WPA-802.1x**.

4. In the **Radius Server Name/IP Address** field, enter the name or IP address of the RADIUS server on your LAN. This is a required field.

5. In the **Radius Port** field, enter the port number used for connections to the RADIUS server. The default port is 1812.

6. In the **Shared Key** field, enter the value that you want to use for the RADIUS shared key. This key enables the modem router to log in to the RADIUS server and must match the client login value used on the RADIUS server.