Chapter 4
Wireless Configuration

This chapter describes how to configure the wireless features of your DG834GT 108 Mbps Super Wireless ADSL Router.

Considerations for a Wireless Network

In planning your wireless network, you should consider the level of security required. You should also select the physical placement of your router in order to maximize the network speed. For further information, refer to Appendix D, "Wireless Networking Basics".

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

Observe Performance, Placement, and Range Guidelines

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

Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router. For complete range/ performance specifications, please see Appendix A, "Technical Specifications".

For best results, place your firewall:

- 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)
- Away from sources of interference, such as computers, microwaves, and cordless phones
- With the Antenna tight and in the upright position
- Away from large metal surfaces

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.

Implement Appropriate Wireless Security

	Note: 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 of 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 DG834GT Super Wireless ADSL Router provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

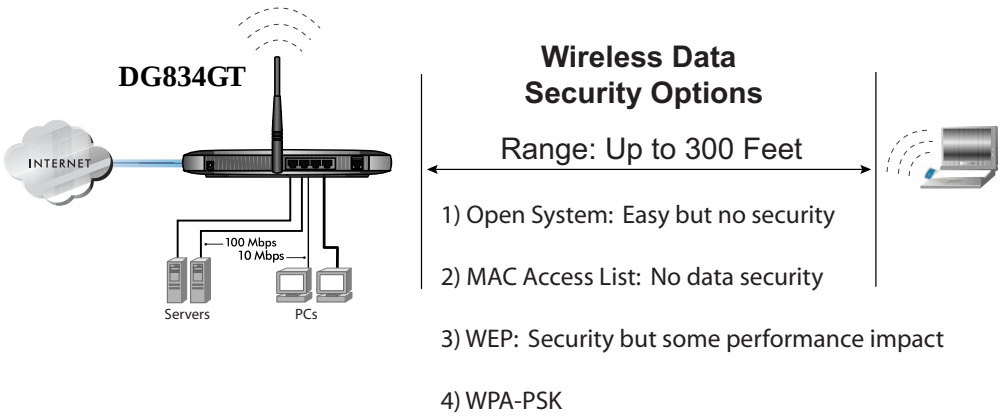

Figure 4-1: DG834GT wireless data security options

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 DG834GT. 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.

- **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.
- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption will block all but the most determined eavesdropper.
- **WPA-PSK**. Wi-Fi Protected Access (WPA) data encryption provides data security. The very strong authentication along with dynamic per frame re-keying of WPA make it virtually impossible to compromise. Because this is a new standard, wireless device driver and software availability may be limited.

Understanding Wireless Settings

To configure the Wireless interface of your router, click the Wireless link in the main menu of the browser interface. The following Wireless Settings menu will appear after WEP (Wired Equivalent Privacy) under Security Options is subsequently selected:

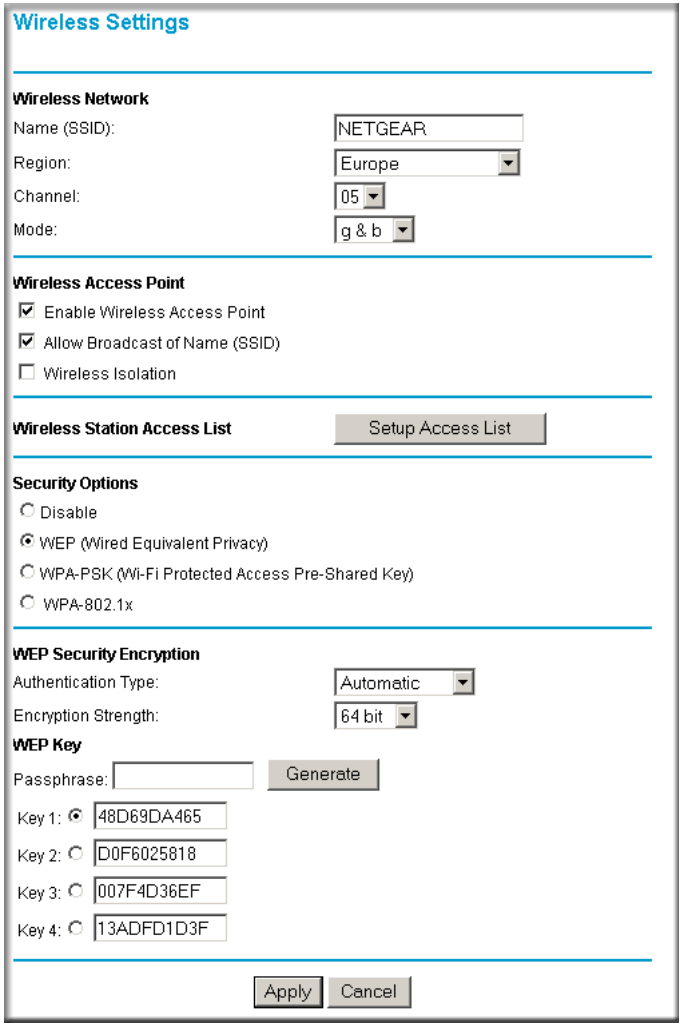

Figure 4-2: Wireless Settings menu

The following parameters are in the Wireless Settings menu:

- **Wireless Network**.
  - **Name (SSID)**. The Service Set ID, also known as the wireless network name. Enter a value of up to 32 alphanumeric characters. The same Name (SSID) must be assigned to all wireless devices in your network. The default SSID is **NETGEAR**, but NETGEAR strongly recommends that you change your network Name to a different value.

Note: This value is case sensitive. For example, **Wireless** is not the same as **wireless**.

— **Region**. Select your region from the drop-down list. This field displays the region of operation for which the wireless interface is intended. It may not be legal to operate the router in a region other than the region shown here.

— **Channel**. This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby access point.

— **Mode**.

- "g & b" allows both "g" and "b" wireless stations to access this device (**default**).
- “g only” allows only 802.11g wireless stations to be used.
- “b only” allows 802.11b wireless stations; 802.11g wireless stations can still be used if they can operate in 802.11b mode.
- “Auto 108 Mbps” means all 802.11g, 802.11b, and Netgear 108 Mbps wireless stations can be used. The Auto 108 Mbps mode is the second fastest mode.
- “108 Mbps only” means only compatible 802.11g wireless stations that support 108 Mbps can connect. The 108 Mbps only mode is the fastest mode.

  Note: Only use the 108 Mbps only mode when all wireless adapters in your open network bear the 108 Mbps logo.

Figure 4-3: 108 Mbps Logo

- **Wireless Access Point**.

— **Enable Wireless Access Point**. This field lets you turn off or turn on the wireless access point built in to the router. The wireless icon on the front of the router will also display 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.

— **Allow Broadcast of Name (SSID)**. If enabled, the SSID is broadcast to all Wireless Stations. Stations which have no SSID (or a "null" value) can then adopt the correct SSID for connections to this Access Point.

— **Wireless Isolation.** If enabled, Wireless Stations will not be able to communicate with each other or with Stations on the wired network. This feature should normally be disabled.

- **Wireless Station Access List**.

— By default, any wireless computer that is configured with the correct wireless network name or SSID will be allowed 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. Click Setup Access List to display the Wireless Station Access List menu.

- **Security Options**

Table 4-1. Wireless Security Options

Field	Description
Disable **WEP** (Wired Equivalent Privacy)	Wireless security is not used. You can select the following WEP options: **Authentication Type** • Open: the DG834GT does not perform any authentication. • Shared: WEP shared key authentication. For a full explanation of WEP shared key, see "Authentication and WEP Data Encryption" on page D-2. **Encryption Strength** • If Shared or Open Network Authentication is enabled, you can choose 64- or 128-bit WEP data encryption. **Note**: With Open Network Authentication and 64- or 128-bit WEP Data Encryption, the DG834GT *does* perform 64- or 128-bit data encryption but *does not* perform any authentication. **Security Encryption (WEP) Key** These key values must be identical on all wireless devices in your network (key 1 must be the same for all, key 2 must be the same for all, and so on). The DG834GT provides two methods for creating WEP encryption keys: • Passphrase. These characters *are* case sensitive. Enter a word or group of printable characters in the Passphrase box and click the Generate button. **Note**: Not all wireless adapters support passphrase key generation. • Manual. These values *are not* case sensitive. 64-bit WEP: enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F). 128-bit WEP: enter 26 hexadecimal digits (any combination of 0-9, a-f, or A-F).

Table 4-1. Wireless Security Options

Field	Description
WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)	WPA 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. For a full explanation of WPA, see "WPA Wireless Security" on page D-8. **Note**: Not all wireless adapters support WPA. 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.
WPA-802.1x	User authentication is implemented using 802.1x and RADIUS servers. For a full explanation of WPA, see "WPA Wireless Security" on page D-8. Fill in the following: • Radius Server Name/IP Address This field is required. Enter the name or IP address of the Radius Server on your LAN. • Radius Port Enter the port number used for connections to the Radius Server. • Radius Shared Key Enter the desired value for the Radius shared key. This key enables the DG834GT to log in to the Radius server and must match the value used on the Radius server.

How to Set Up and Test Basic Wireless Connectivity

Follow the instructions below 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. Log in to the DG834GT firewall 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. Click the Wireless Settings link in the main menu of the DG834GT firewall.
3. Choose a suitable descriptive name for the wireless network name (SSID). In the SSID box, enter a value of up to 32 alphanumeric characters. The default SSID is **Wireless**.

   Note: The SSID of any wireless access adapters must match the SSID you configure in the DG834GT 108 Mbps Super Wireless ADSL Router. If they do not match, you will not get a wireless connection to the DG834GT.

4. Set the Region. Select the region in which the wireless interface will operate.

5. Set the Channel. 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 firewall. For more information on the wireless channel frequencies please refer to "Wireless Channels" on page D-7.

6. 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 "Disabled."

7. Click Apply to save your changes.

	**Note:** If you are configuring the firewall from a wireless computer and you change the firewall'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 firewall's new settings.

8. Configure and test your computers for wireless connectivity.

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

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

How to Restricting Wireless Access to Your Network

By default, any wireless PC that is configured with the correct SSID will be allowed access to your wireless network. For increased security, the DG834GT 108 Mbps Super Wireless ADSL Router provides several ways to restrict wireless access to your network:

- 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 below.

Figure 4-4: Wireless Access Point settings

Restricting Access to Your Network by Turning Off Wireless Connectivity

You can completely turn off the wireless portion of the DG834GT. For example, if your notebook computer is used to wirelessly connect to your router and you take a business trip, you can turn off the wireless portion of the router while you are traveling. Other members of your household who use computers connected to the router via Ethernet cables will still be able to use the router.

Restricting Wireless Access Based on the Wireless Network Name (SSID)

The DG834GT can restrict wireless access to your network by not broadcasting the wireless network name (SSID). However, by default, this feature is turned off. If you turn this feature on, wireless devices will not 'see' your DG834GT. You must configure your wireless devices to match the wireless network name (SSID) you configure in the DG834GT Super Wireless ADSL Router.

Note: The SSID of any wireless access adapters must match the SSID you configure in the DG834GT 108 Mbps Super Wireless ADSL Router. If they do not match, you will not get a wireless connection to the DG834GT.

Restricting Wireless Access Based on the Wireless Station Access List

This list determines which wireless hardware devices will be allowed to connect to the firewall.

To restrict access based on MAC addresses, follow these steps:

1. Log in to the DG834GT firewall 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. From the Wireless Settings menu, Wireless Station Access List section, click the Setup Access List button to display the list, shown below:

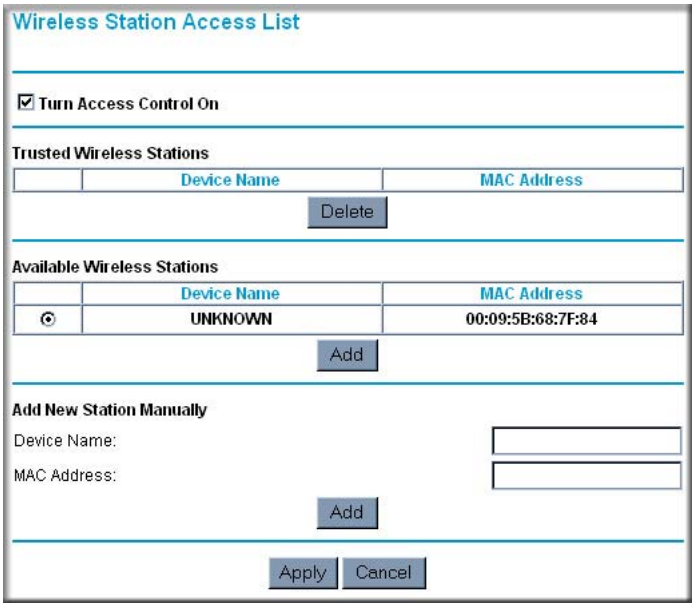

Figure 4-5. Wireless Access menu

3. Select the Turn Access Control On check box to enable restricting 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 may appear in the router's DHCP table. The MAC address will be 12 hexadecimal digits.

   Click Add to add your entry. You can add several stations to the list, but the entries will be discarded if you do not click Apply.

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

	Note: If you are configuring the 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 router from a wired computer to make any further changes.

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

Now, only devices on this list will be allowed to wirelessly connect to the DG834GT. This prevents unauthorized access to your network.

Choosing WEP Authentication and Security Encryption Methods

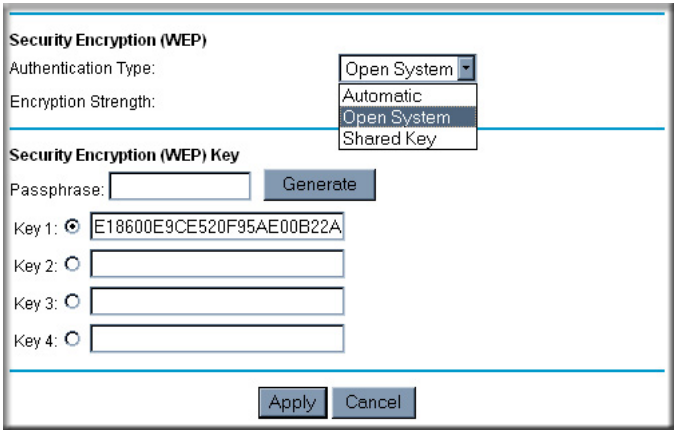

Figure 4-6. Security Encryption section

Restricting wireless access prevents intruders from connecting to your network. However, the wireless data transmissions are still vulnerable to snooping. Using the WEP data encryption settings described below 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.

Authentication Type Selection

The DG834GT lets you select the following wireless authentication schemes.

- Automatic
- Open System
- Shared key

	**Note:** The authentication scheme is separate from the data encryption. You can choose an authentication scheme which requires a shared key but still leave the data transmissions unencrypted. If you require strong security, use both the Shared Key and WEP encryption settings.

Set your wireless adapter according to the authentication scheme you choose for the DG834GT Super Wireless ADSL Router. Please refer to "Authentication and WEP Data Encryption" on page D-2 for a full explanation of each of these options, as defined by the IEEE 802.11g wireless communication standard.

Encryption Choices

Please refer to "Overview of WEP Parameters" on page D-5 for a full explanation of each of the following choices, as defined by the IEEE 802.11g wireless communication standard. Choose the encryption strength from the drop-down list:

Disable

No encryption will be applied. This setting is useful for troubleshooting your wireless connection, but leaves your wireless data fully exposed.

64 or 128 bit WEP

When 64 Bit WEP or 128 Bit WEP is selected, WEP encryption will be applied.

If WEP is enabled, 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.

There are two methods for creating WEP encryption keys:

- Passphrase. Enter a word or group of printable characters in the Passphrase box and click the Generate button.
- Manual. 64-bit WEP: Enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F). 128-bit WEP: Enter 26 hexadecimal digits (any combination of 0-9, a-f, or A-F).

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

How to Configure WEP

To configure WEP data encryption, follow these steps:

1. Log in to the DG834GT firewall 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. Click the Wireless Settings link in the main menu of the DG834GT router.
3. Go to the Security Encryption portion of the page:

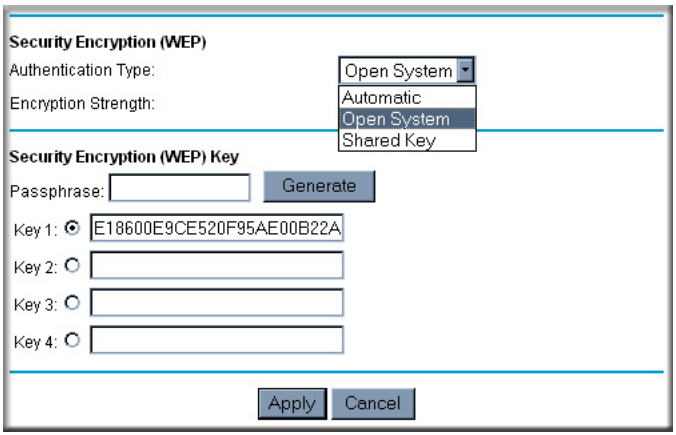

Figure 4-7. Wireless WEP menu

4. Select the Authentication Type.
5. Select the Encryption setting.
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 box and click the Generate button. The four key boxes will be automatically populated with key values.
   - Manual — enter hexadecimal digits (any combination of 0-9, a-f, or A-F). Select which of the four keys will be active.
7. Select the radio button for the key you want to make active.

   Be sure 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 only allow entry of one key which must match the default key you set in the DG834GT.

8. Click Apply to save your settings.

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

How to Configure WPA-PSK

Note: Not all wireless adapters support WPA. 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 WPA-PSK, follow these steps:

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. Click **Wireless Settings** in the Setup section of the main menu of the DG834GT.
3. Choose the **WPA-PSK** radio button. The WPA-PSK menu will open.
4. Enter the pre-shared key in the Passphrase field.
5. Click **Apply** to save your settings.