NETGEAR®

N300 Wireless ADSL2+ Modem Router DGN2200M Mobile Edition

User Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

November 2011
202-10604-02
v1.0

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, get support online, or for more information about the topics covered in this manual, visit the Support website at *http://support.netgear.com*.

Phone (US & Canada only): 1-888-NETGEAR

Phone (Other Countries): Check the list of phone numbers at *http://support.netgear.com/app/answers/detail/a_id/984*

Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. Other brand and product names are registered trademarks or trademarks of their respective holders. © 2011 NETGEAR, Inc. All rights reserved.

Statement of Conditions

To improve 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.

Contents

Chapter 1 Internet Configuration

Chapter 2 Wireless Settings

Chapter 3 Protecting Your Network

Chapter 4 Managing Your Network

Chapter 5 USB Storage

Chapter 6 Advanced Configuration

Chapter 7 Troubleshooting

Appendix A Technical Specifications and Factory Default Settings

Internet Configuration

1

This chapter describes how to configure your N300 Wireless ADSL2+ Modem Router DGN2200M Mobile Edition Internet connection. For help with installation, see the *N300 Wireless ADSL2+ Modem Router DGN2200M Mobile Edition Installation Guide.*

This chapter covers the following topics:

- *Hardware Features*
- *System Setup*
- *Log In to Your Wireless-N Modem Router*
- *Use the Setup Wizard after Installation*
- *Manually Configure Your Internet Settings*

For more information about the topics covered in this manual, visit the support website at *http://support.netgear.com*.

Hardware Features

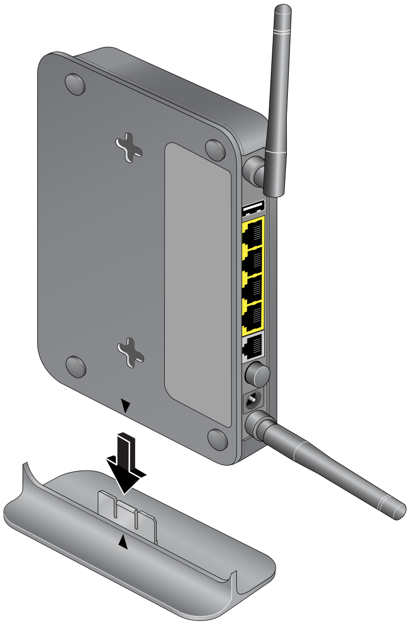
This section acquaints you with the physical aspects of your N300 Wireless ADSL2+ Modem Router.

Router Stand

Since the router is a vertical-only device, use the stand to position your wireless modem router upright.

➢ **To assemble the router and its stand:**

1. Insert the tabs of the stand into the slot on the bottom of your router.



2. Place your router near an AC power outlet in a location where you can connect cables as needed for your home network.

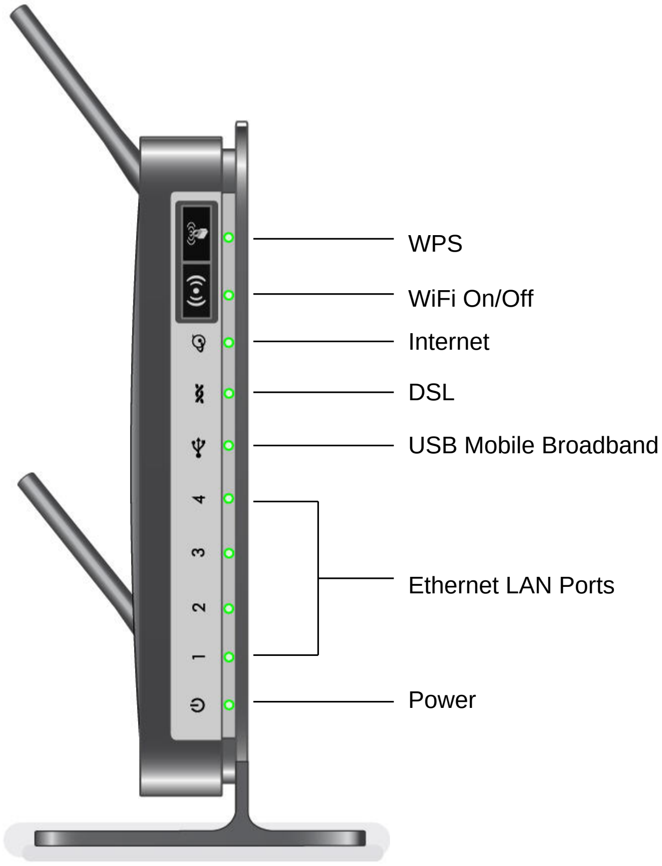
   If you are planning to connect to the Internet using mobile broadband, the router needs to be located where you can receive a strong mobile broadband signal while indoors.

   To mount the router to a wall, see *Wall-Mounting* on page 114.

   For additional considerations on router placement, see *Position Your Wireless Router* on page 13.

Router Front Panel

The wireless modem router front panel contains control buttons and status LEDs.



You can use the LEDs to verify status and connections. The following table lists and describes each LED and button on the front panel of the wireless modem router.

Table 1. Front panel button and LED descriptions

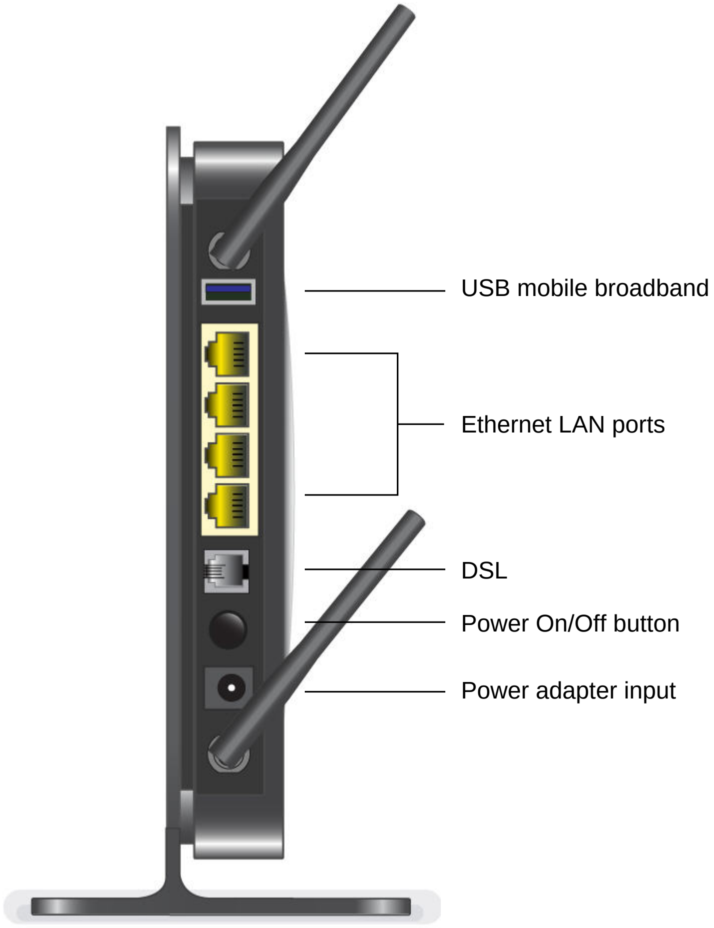
Button/LED	Activity	Description
WPS	Press this button to open a 2-minute window for the wireless modem router to connect with other WPS-enabled devices. For more information about using the WPS method to implement security, see *Wi-Fi Protected Setup (WPS) Method* on page 32.	
	Solid green	WPS wireless security is being enabled.
	Blinking green	The device is in the 2-minute interval to synchronize security.
	Off	WPS is not being set or enabled.

Table 1. Front panel button and LED descriptions (continued)

Button/LED	Activity	Description
WiF ((•))	Turn the wireless radio in the wireless modem router on and off. The wireless radio is on by default. The LED located below this button indicates if the wireless radio is on or off.	
	Solid green	Indicates that the wireless port is initialized.
	Blinking green	Data is being transmitted or received over the wireless link.
	Off	The wireless access point is turned off.
Internet Port	Solid green	There is an Internet session.
	Solid red	There is no Internet connection.
	Blinking green	Data is being transmitted over the Internet connection.
	Blinking green and red	Traffic meter limit has been reached.
	Off	No Internet connection detected or device in bridge mode.
DSL	Solid green	The ADSL port is synchronized with an ISP’s network access device.
	Blinking green	Indicates ADSL training—ADSL is synchronizing with the DSLAM.
	Off	The unit is off, or there is no IP connection.
USB	Off	• No USB device connected. • “Safely Remove Hardware” has been activated. • An error has occurred with the device.
	Solid blue	USB device is ready to use.
	Blinking blue	USB device is in use.
LAN Ports 1	Solid green	The local Ethernet ports have detected wired links with computers.
	Blinking	Data is being transmitted or received.
	Off	No link is detected on these ports.
Power ⏻	Solid green	The router is powered on and operating normally.
	Solid amber	POST (power-on self-test) in progress.
	Off	Power is not supplied to the router.
	Restore Factory Settings button	Press the **Restore Factory Settings** button for 6 seconds. The Power LED lights briefly. When the button is released, the LED blinks red three times and then turns green as the router resets to the factory defaults.

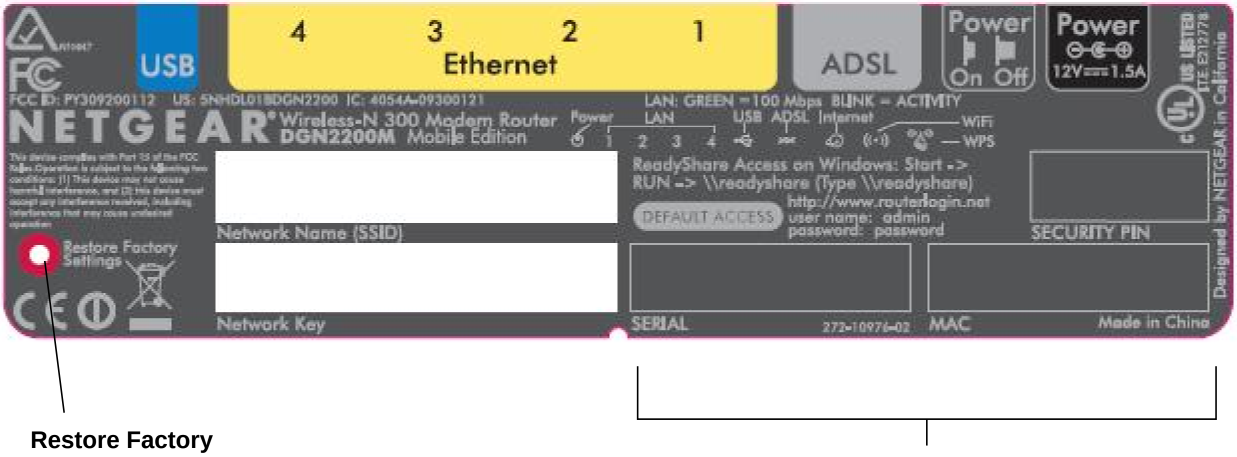
Router Back Panel

The back panel of the wireless modem router contains port connections.



Router Label

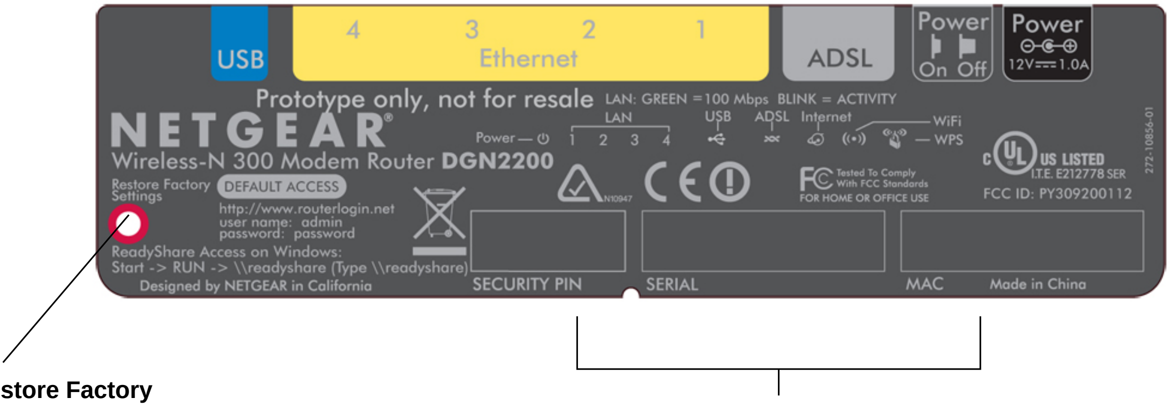
The label on the left side of the wireless modem router shows the router’s MAC address, serial number, security PIN, and factory default login information.


USB
4
3
2
1
Ethernet
ADSL
Power
On Off
Power
12V⎓1.5A
FCC ID: PY309200112 US: 5NHDL01BDGN2200 IC: 4054A-09300121
NETGEAR
Wireless-N 300 Modem Router
DGN2200M Mobile Edition
LAN: GREEN = 100 Mbps BLINK = ACTIVITY
Power
LAN
USB
ADSL
Internet
WiFi
WPS
Restore Factory Settings
Network Name (SSID)
Network Key
ReadyShare Access on Windows: Start -> RUN -> \\readyshare (Type \\readyshare)
DEFAULT ACCESS
http://www.routerlogin.net
user name: admin
password: password
SECURITY PIN
SERIAL
272-10976-02
MAC
Made in China
Designed by NETGEAR in California

Restore Factory Settings: Press for 6 seconds.

Router information
- Default access address
- Default user name and password
- Security PIN
- Serial number
- MAC address

Note: If the label on your router looks like the one in the following figure, then your router has no preset wireless security. You need to set the wireless security to protect your network.


USB
4
3
2
1
Ethernet
ADSL
Power
On Off
Power
12V⎓1.0A
Prototype only, not for resale
NETGEAR
Wireless-N 300 Modem Router DGN2200
LAN: GREEN = 100 Mbps BLINK = ACTIVITY
LAN
USB
ADSL
Internet
WiFi
WPS
Power
US LISTED
I.T.E. E212778 SER
Tested To Comply With FCC Standards
FOR HOME OR OFFICE USE
FCC ID: PY309200112
272-10856-01
Restore Factory Settings
DEFAULT ACCESS
http://www.routerlogin.net
user name: admin
password: password
ReadyShare Access on Windows:
Start -> RUN -> \\readyshare (Type \\readyshare)
Designed by NETGEAR in California
SECURITY PIN
SERIAL
MAC
Made in China

Restore Factory Settings: Press for 6 seconds.

Router information
- Default access address
- Default user name and password
- Security PIN
- Serial number
- MAC address

System Setup

The N300 Wireless ADSL2+ Modem Router DGN2200M Mobile Edition requires the considerations described in the following sections for successful operation.

- *Position Your Wireless Router*
- *Typical Systems* on page 14

Position Your Wireless Router

The wireless modem router lets you access your network from virtually anywhere within the operating range of your wireless network. However, the operating distance or range of your wireless connection can vary significantly depending on the physical placement of your router. For example, the thickness and number of walls the wireless signal needs to pass through might limit the range. For best results, place your router:

- Near the center of the area where your computers and other devices will operate, preferably within line of sight to your wireless devices.
- Accessible to an AC power outlet and near Ethernet cables for wired computers.
- In an elevated location such as a high shelf, keeping the number of walls and ceilings between the wireless modem router and your other devices to a minimum.
- Away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, or the base for a cordless phone.
- Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.

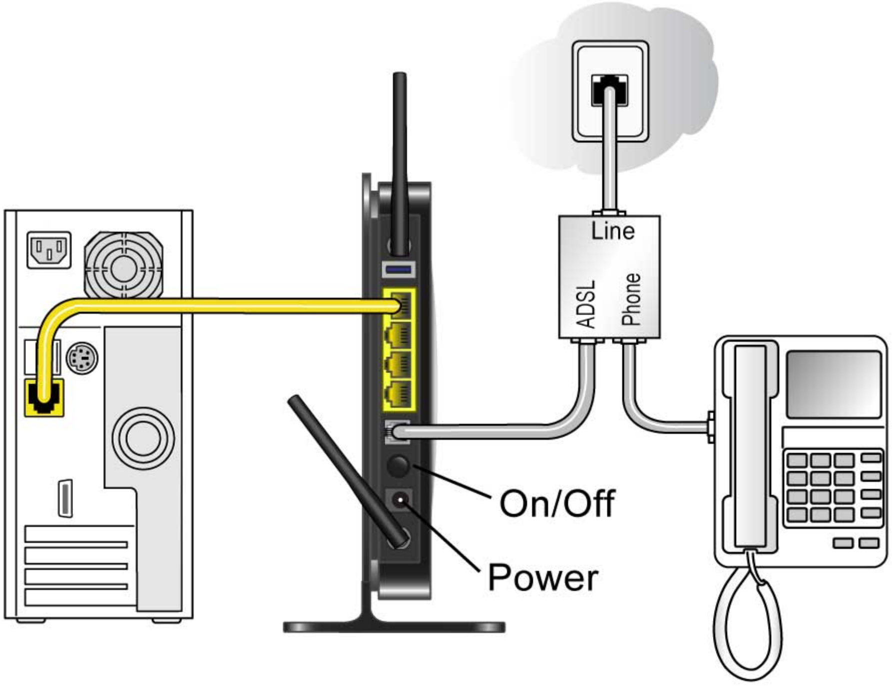
Note: Failure to follow these guidelines can result in significant performance degradation or an inability to wirelessly connect to the Internet.

Typical Systems

The wireless modem router allows you to have the types of systems described in the following sections. Your choice of system will determine how you configure the settings described in *Broadband Settings* on page 21.

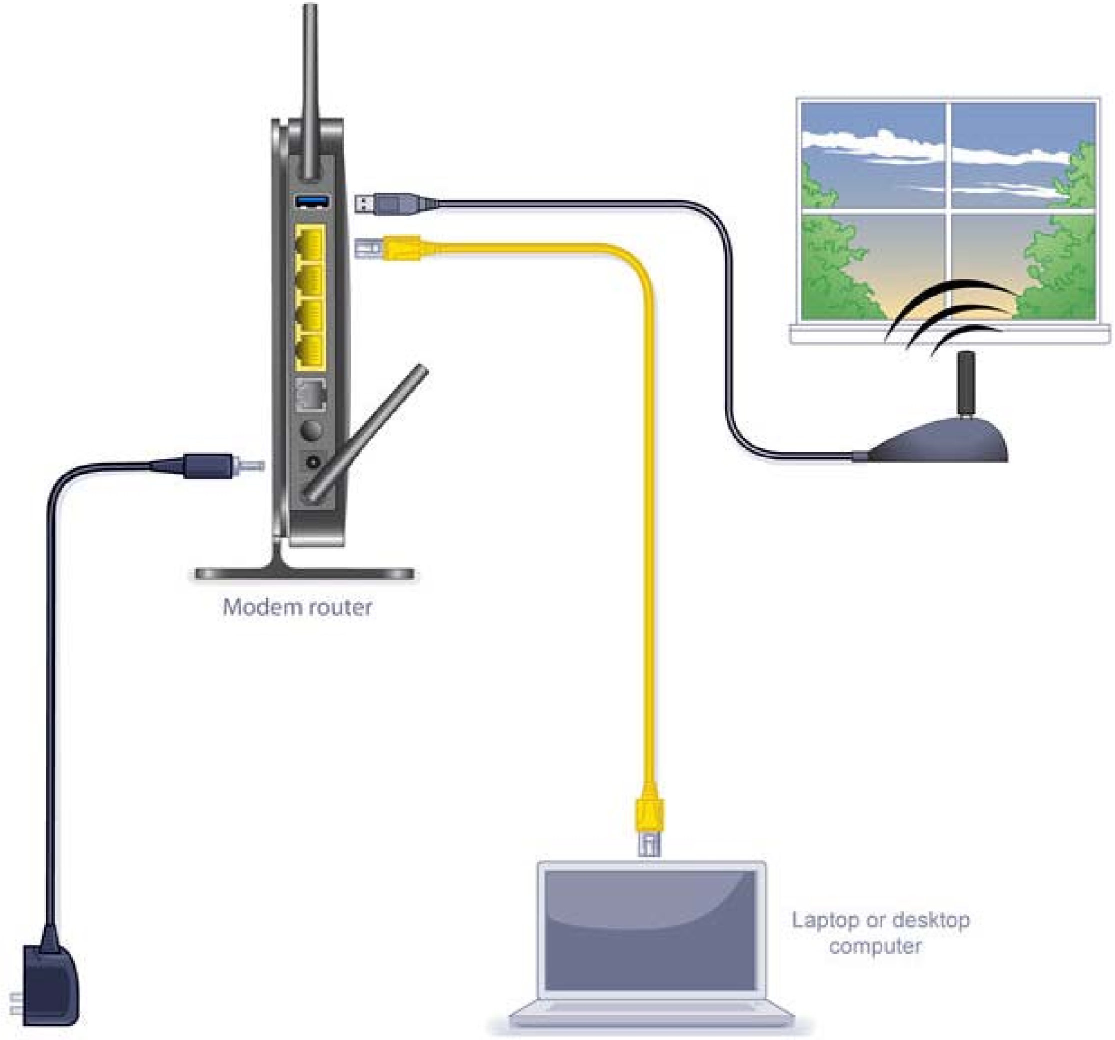
- *ADSL Only*
- *Mobile Broadband Only* on page 15
- *ADSL with Failover to Mobile Broadband* on page 16

ADSL Only



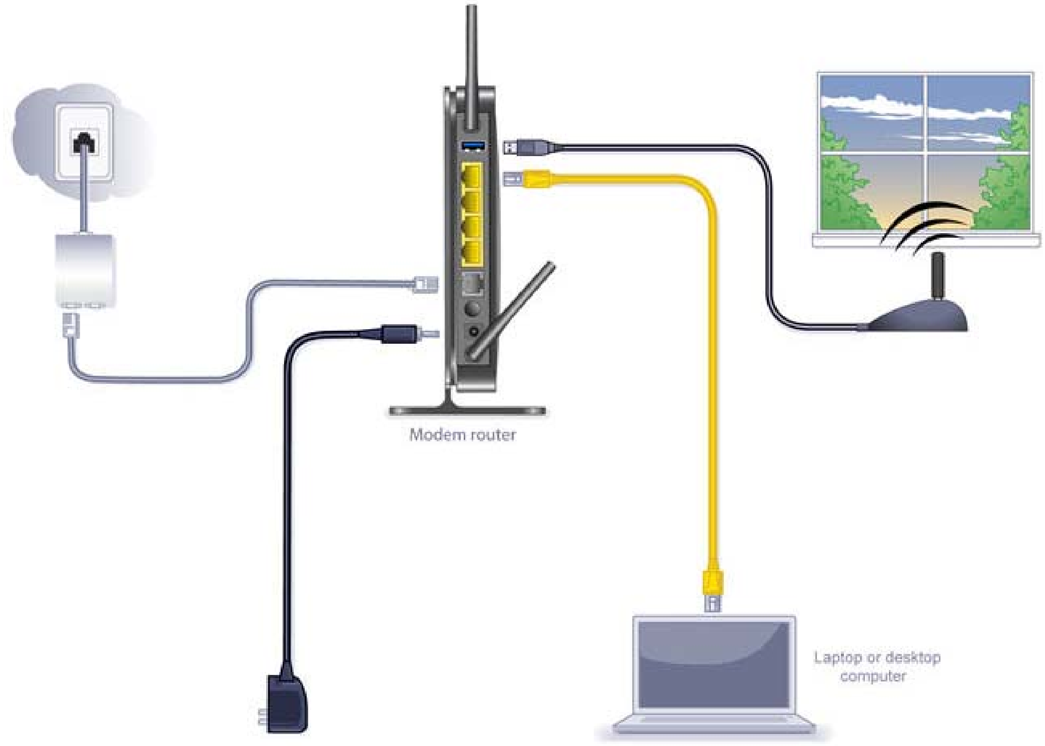
Note: Incorrectly connecting a filter to your wireless modem router will block your ADSL connection.

Mobile Broadband Only



Note: Because the USB port on the wireless modem router is used for connecting the broadband mobile modem cable, you are not able to use the USB port for both a ReadyShare storage and a broadband mobile Internet connection at the same time even when using a USB hub to fan out the USB port.

ADSL with Failover to Mobile Broadband



Note: Incorrectly connecting a filter to your wireless modem router will block your ADSL connection.

Note: Because the USB port on the wireless modem router is used for connecting the broadband mobile modem cable, you are not able to use the USB port for both a ReadyShare storage and a broadband mobile Internet connection at the same time even when using a USB hub to fan out the USB port.

Log In to Your Wireless-N Modem Router

When you first connect to your wireless modem router during installation, a Setup Wizard displays. For help using the Setup Wizard to configure your Internet and wireless network, see the *N300 Wireless ADSL2+ Modem Router DGN2200M Mobile Edition Installation Guide*.

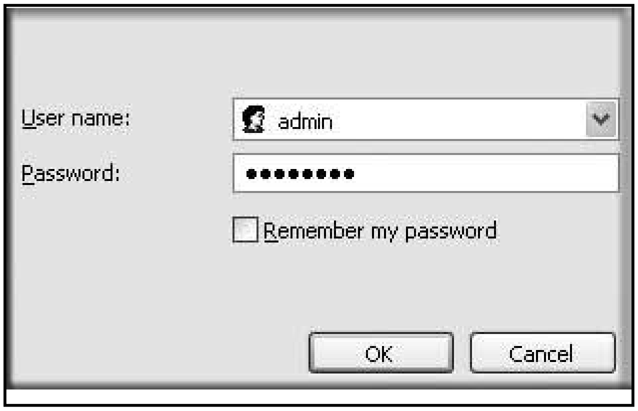
After the initial configuration, you can log in to the wireless modem router to view or change its settings, and to access the Knowledge Base and documentation.

Note: Your computer needs to be configured for DHCP.

When you have logged in, if you do not click **Logout**, the wireless modem router waits for 5 minutes after no activity before it automatically logs you out.

➢ **To log in to the wireless modem router:**

1. Type **http://www.routerlogin.net** in the address field of your browser, and then press **Enter** or **Return**. A login window displays:



User name: admin

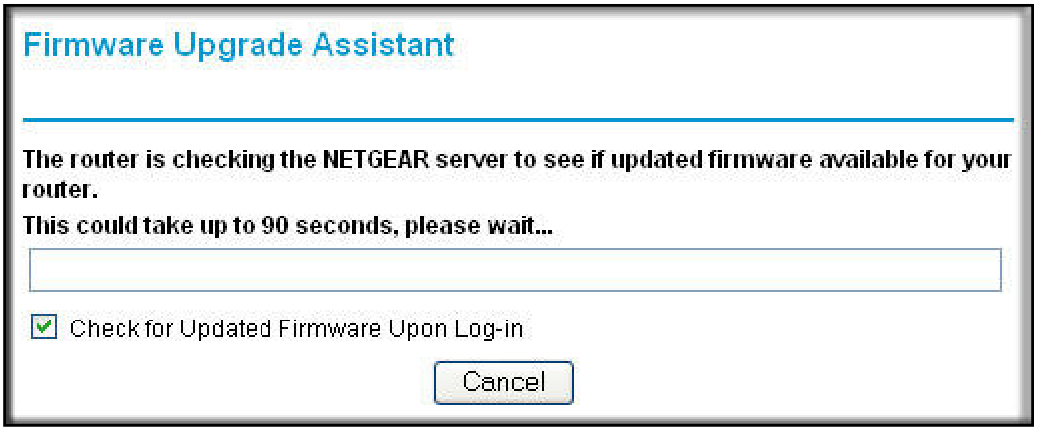
Password: •••••••••

2. Enter **admin** for the user name and your password (or the default, **password**). For information about how to change the password, see *Change the Built-In Password* on page 42.

Note: If you changed your password and do not remember what it is, you can restore the wireless modem router to its factory settings. See *Factory Default Configuration* on page 112.

3. If the router has not been configured, the Smart Wizard screen displays. After the router has been configured, one of the following screens displays:
   - **Firmware Upgrade Assistant screen**. After initial setup, the Firmware Upgrade Assistant screen displays unless the Check for Updated Firmware Upon Log-in check box is cleared.

> ***Note:*** You can disable this automatic checking and updating feature during future logins by clearing the **Check for Updated Firmware Upon Log-in** check box, but NETGEAR recommends that you keep this feature enabled to ensure that your router is using the latest updated firmware.



Firmware Upgrade Assistant

The router is checking the NETGEAR server to see if updated firmware available for your router.

This could take up to 90 seconds, please wait...

☑ Check for Updated Firmware Upon Log-in

- **Router Status screen**. The Router Status screen displays the current router connection status. See *Router Status and Usage Statistics* on page 56.

4. You can use different methods to configure your router.
   - Select Setup Wizard **from the router menu to set up your Internet connection and wireless network configuration**. See *Use the Setup Wizard after Installation* on page 19.
   - You can manually configure the router settings. See *Manually Configure Your Internet Settings* on page 21.

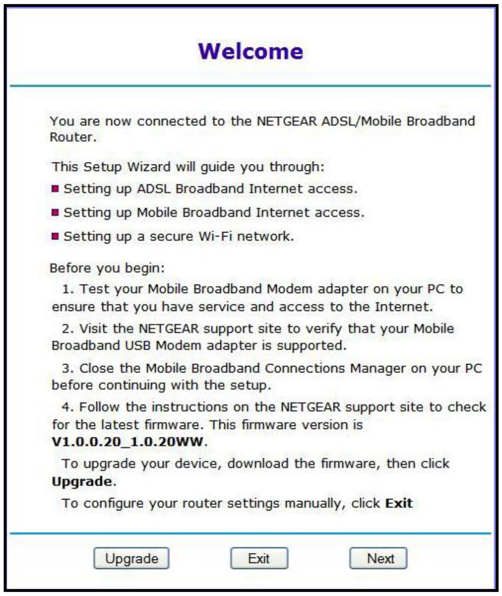
Use the Setup Wizard after Installation

The Setup Wizard can check your Internet connection for servers and protocols to determine your ISP configuration. You can also manually specify your Internet connection settings in the Basic Settings screen.

> ***Note:*** The Setup Wizard is also called the Configuration Assistant on some systems.

➢ **To use the Setup Wizard:**

1. From the top of the modem router main menu, select **Setup Wizard**.



Welcome

You are now connected to the NETGEAR ADSL/Mobile Broadband Router.

This Setup Wizard will guide you through:

- Setting up ADSL Broadband Internet access.
- Setting up Mobile Broadband Internet access.
- Setting up a secure Wi-Fi network.

Before you begin:

1. Test your Mobile Broadband Modem adapter on your PC to ensure that you have service and access to the Internet.
2. Visit the NETGEAR support site to verify that your Mobile Broadband USB Modem adapter is supported.
3. Close the Mobile Broadband Connections Manager on your PC before continuing with the setup.
4. Follow the instructions on the NETGEAR support site to check for the latest firmware. This firmware version is **V1.0.0.20_1.0.20WW**.

To upgrade your device, download the firmware, then click **Upgrade**.

To configure your router settings manually, click **Exit**

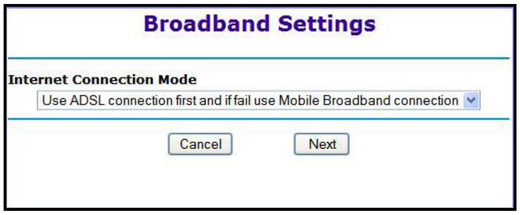
2. Click **Next**.

   The Setup Wizard prompts you to set up your Internet connection and wireless network as described in the *N300 Wireless ADSL2+ Modem Router DGN2200M Mobile Edition Installation Guide*.

   a. Select your Internet connection mode:

      - Use ADSL first and if fail use Mobile Broadband connection
      - Always use Mobile Broadband connection

- Always use ADSL connection



Broadband Settings

Internet Connection Mode

Use ADSL connection first and if fail use Mobile Broadband connection

b. Click **Next**.

c. Select your country and then your Internet service provider information.

d. Click **Next**.

> ***Note:*** When failover mode is selected, ADSL is configured first, and then mobile broadband is configured second.

3. Depending on the type of connection, you are prompted to enter your ISP settings.
   - For PPPoE or PPPoA, enter the login user name and password. These fields are case-sensitive.
   - For a dynamic IP account setup, no entries are needed.
   - For IP over ATM Classical IP assignment (RFC1577), enter the assigned IP address, subnet mask, and the IP address of your ISP’s primary DNS server. If a secondary DNS server address is available, enter it also. DNS servers translate an Internet name such as www.netgear.com to a numeric IP address.
   - For help with a static IP address, see *Fixed IP (Static) Account Setup* on page 20.
4. At the end of the Setup Wizard, click **Test** to check your Internet connection. If you have trouble connecting to the Internet, see *Troubleshooting* on page 100.

Fixed IP (Static) Account Setup

➢ **To set up a fixed IP (static) account:**

1. If required, enter the account name and domain name from your ISP.
2. Select **Use Static IP Address** or **Use IP Over ATM** (IPoA—RFC1483 Routed) according to the information from your ISP. If you select IPoA, the router will detect the gateway IP address, but you still need to provide the router IP address.
3. Enter your assigned IP address, subnet mask, and the IP address of your ISP’s gateway wireless modem router. This information should have been provided to you by your ISP.
4. Enter the IP address of your ISP’s primary DNS server. If a secondary DNS server address is available, enter it also. DNS servers translate an Internet name such as www.netgear.com to a numeric IP address.

Manually Configure Your Internet Settings

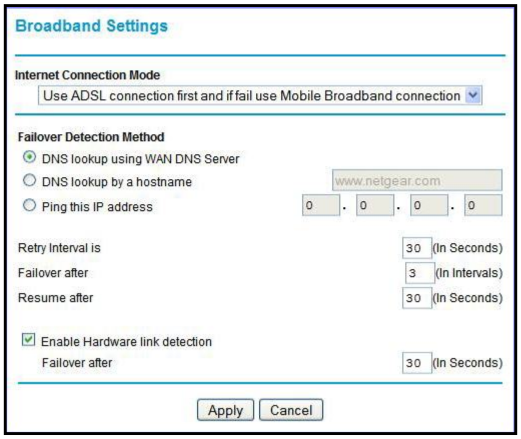
For you to connect to the network, an active broadband service account is required. Contact your ISP for your user name, password, and the network name. You also need to configure some or all of the settings described in the following sections, depending on how you have chosen to connect to the Internet:

- *Broadband Settings*
- *Basic ISP Settings* on page 22
- *ADSL Settings* on page 25 (not required if using mobile broadband connection only)
- *Mobile Broadband Settings* on page 26 (not required if using ADSL connection only)

Broadband Settings

➢ **To manually configure your broadband Internet settings:**

1. Log in to the router as described in *Log In to Your Wireless-N Modem Router* on page 17.
2. From the main menu, select **Broadband Settings**.



Broadband Settings

Internet Connection Mode
Use ADSL connection first and if fail use Mobile Broadband connection

Failover Detection Method
● DNS lookup using WAN DNS Server
○ DNS lookup by a hostname www.netgear.com
○ Ping this IP address 0 . 0 . 0 . 0

Retry Interval is 30 (In Seconds)
Failover after 3 (In Intervals)
Resume after 30 (In Seconds)

☑ Enable Hardware link detection
Failover after 30 (In Seconds)

3. Adjust the settings as needed based on your Internet connection. The fields in this screen are described in *Table 2*.
4. The following buttons are available:
   - **Apply**. Apply the changes that you made.
   - **Cancel**. Discard changes.

Table 2. Broadband Settings fields

Fields and check boxes	Description
Internet Connection Mode	The choices are: • Use ADSL first and if fail use Mobile Broadband connection • Always use Mobile Broadband connection • Always use ADSL connection
Failover Detection Method[1]	Select the failover method, and enter the related information: • DNS lookup using WAN DNS Server • Perform a DNS lookup by a hostname • Ping this IP address
Retry Interval is[1]	Enter the retry interval.
Failover after[1]	Enter how many retry attempts to make before failing over.
Resume after[1]	Enter how long to wait for the primary link to be stabilized before resuming use of the primary link.
Enable Hardware link detection	Enter when to fail over when the Ethernet link is dropped. This is independent of the DNS or Ping detection method.

[1] *This field is available only when the internet connection Mode is* ***Use ADSL first and if fail use Mobile Broadband connection.***

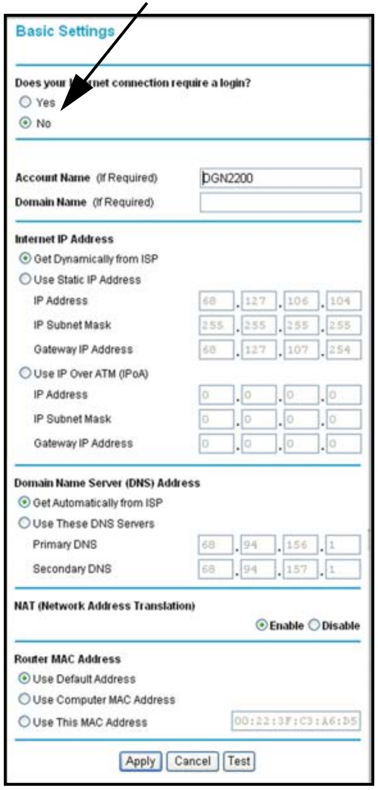
Basic ISP Settings

➢ **To view or configure the basic settings:**

1. From the router menu, select **Basic Settings**.

2. Select **Yes** or **No** depending on whether your ISP requires a login. This selection changes the fields available on the Basic Settings screen.

ISP *does not* require login



Basic Settings

Does your Internet connection require a login?

○ Yes

● No

Account Name (If Required): DGN2200

Domain Name (If Required):

Internet IP Address

● Get Dynamically from ISP

○ Use Static IP Address

IP Address: 68 . 127 . 106 . 104

IP Subnet Mask: 255 . 255 . 255 . 255

Gateway IP Address: 68 . 127 . 107 . 254

○ Use IP Over ATM (IPoA)

IP Address: 0 . 0 . 0 . 0

IP Subnet Mask: 0 . 0 . 0 . 0

Gateway IP Address: 0 . 0 . 0 . 0

Domain Name Server (DNS) Address

● Get Automatically from ISP

○ Use These DNS Servers

Primary DNS: 68 . 94 . 156 . 1

Secondary DNS: 68 . 94 . 157 . 1

NAT (Network Address Translation)

● Enable ○ Disable

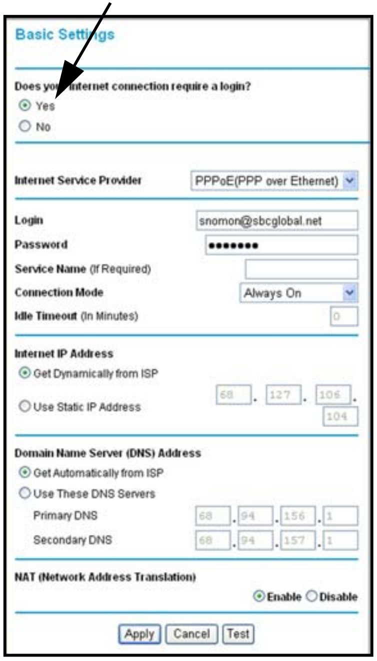
Router MAC Address

● Use Default Address

○ Use Computer MAC Address

○ Use This MAC Address: 00:22:3F:C3:A6:D5

ISP *does* require login



Basic Settings

Does your Internet connection require a login?

● Yes

○ No

Internet Service Provider: PPPoE(PPP over Ethernet)

Login: snomon@sbcglobal.net

Password: •••••••

Service Name (If Required):

Connection Mode: Always On

Idle Timeout (In Minutes): 0

Internet IP Address

● Get Dynamically from ISP

○ Use Static IP Address: 68 . 127 . 106 . 104

Domain Name Server (DNS) Address

● Get Automatically from ISP

○ Use These DNS Servers

Primary DNS: 68 . 94 . 156 . 1

Secondary DNS: 68 . 94 . 157 . 1

NAT (Network Address Translation)

● Enable ○ Disable

- **Yes**. If your ISP requires a login, select this radio button.
- **No**. If your ISP does not require a login, enter the account name, if required, and the domain name, if required.

3. Enter the settings for the IP address and DNS server. If you enter or change a DNS address, restart the computers on your network so that these settings take effect.
4. If no login is required, you can specify the MAC Address setting.
5. Click **Apply** to save your settings.
6. Click **Test** to test your Internet connection. If the NETGEAR website does not display within 1 minute, see *Troubleshoot the Internet Connection* on page 104.

When your Internet connection is working, you do not need to launch the ISP’s login program on your computer to access the Internet. When you start an Internet application, your wireless modem router automatically logs you in.

Table 3. Basic Settings screen fields

Settings		Description
Does Your ISP Require a Login?		• Yes • No
These fields display only if no login is required.	Account Name (If required)	Enter the account name provided by your ISP. This might also be called the host name.
	Domain Name (If required)	Enter the domain name provided by your ISP.
These fields display only if your ISP requires a login.	Login	The login name provided by your ISP. This is often an e-mail address.
	Password	The password that you use to log in to your ISP.
	Service Name	If your ISP provided a service name, enter it here.
	Connection Mode	Select the connection mode: Always on, Dial on Demand, or Manually Connect.
	Idle Timeout (In minutes)	If you want to change the Internet login time-out, enter a new value in minutes. This determines how long the wireless modem router keeps the Internet connection active after there is no Internet activity from the LAN. Entering an Idle Timeout value of 0 (zero) means never log out.
Internet IP Address		• **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses. • **Use Static IP Address**. Enter the IP address that your ISP assigned. Also enter the IP subnet mask and the gateway IP address. The gateway is the ISP’s wireless modem router to which your wireless modem router will connect. • **Use IP Over ATM (PoA)**. This option is available only if your ISP does not require a login.
Domain Name Server (DNS) Address		The DNS server is used to look up site addresses based on their names. • **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS server address automatically. • **Use These DNS Servers**. If you know your ISP does not automatically transmit DNS addresses to the wireless modem router during login, select this option, and enter the IP address of your ISP’s primary DNS server. If a secondary DNS server address is available, enter it also.

Table 3. Basic Settings screen fields (continued)

Settings		Description
NAT (Network Address Translation)		NAT automatically assigns private IP addresses (10.1.1.x) to devices on your LAN. • **Enable**. Usually NAT is enabled. • **Disable**. This disables NAT, but leaves the firewall active. Disable NAT only if you are sure that you do not require it. When NAT is disabled, only standard routing is performed by this router. Classical routing lets you directly manage the IP addresses that the wireless modem router uses. Classical routing should be selected only by experienced users.[1]
This field displays only if your ISP does not require a login.	Router MAC Address	Your computer's local address is its unique address on your network. This is also referred to as the computer's MAC (Media Access Control) address. • **Use Default MAC Address**. This is the usual setting. • **Use Computer MAC address**. If your ISP requires MAC authentication, you can use this setting to disguise the wireless modem router's MAC address with the computer's own MAC address. • **Use This MAC Address**. If your ISP requires MAC authentication, you can manually type the MAC address for a different computer. The format for the MAC address is XX:XX:XX:XX:XX:XX.

[1] Disabling NAT reboots the wireless modem router and resets its configuration settings to the factory defaults. Disable NAT only if you plan to install the wireless modem router in a setting where you will be manually administering the IP address space on the LAN side of the router.

ADSL Settings

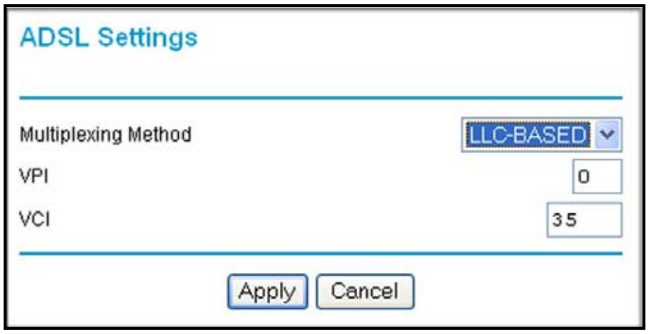
NETGEAR recommends that you use the Setup Wizard to automatically detect and configure your ADSL settings. This usually works fine. However, if you have technical experience and are sure of the multiplexing method and virtual circuit number for the virtual path identifier (VPI) and virtual channel identifier (VCI), you can specify those settings here.

Note: Use the Setup Wizard to select the correct country to optimize detection of the ADSL settings.

If your ISP provided you with a multiplexing method or VPI/VCI number, then enter the setting.

➤ **To manually specify ADSL settings:**

1. From the main menu, select **ADSL Settings**, and the ADSL Settings screen displays.



ADSL Settings

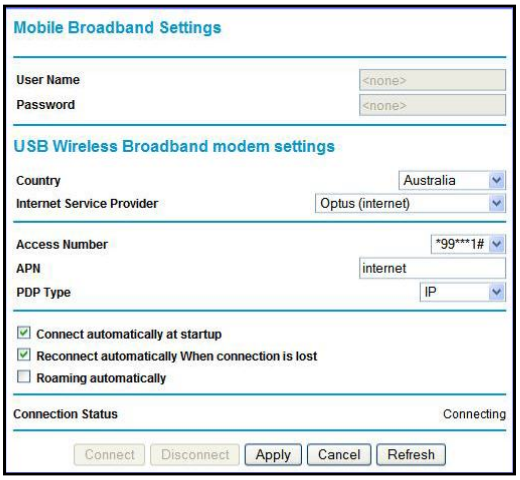
Multiplexing Method	LLC-BASED
VPI	0
VCI	35

2. In the Multiplexing Method drop-down list, select **LLC-based** or **VC-based**.
3. For the VPI, type a number between 0 and 255. The default is 8.
4. For the VCI, type a number between 32 and 65535. The default is 35.
5. Click **Apply**.

Mobile Broadband Settings

➤ **To manually configure your mobile broadband Internet settings:**

1. Log in to the router as described in *Log In to Your Wireless-N Modem Router* on page 17.
2. From the main menu, select **Mobile Broadband Settings**.



Mobile Broadband Settings

User Name	<none>
Password	<none>

USB Wireless Broadband modem settings

Country	Australia
Internet Service Provider	Optus (internet)
Access Number	*99***1#
APN	internet
PDP Type	IP

☑ Connect automatically at startup

☑ Reconnect automatically When connection is lost

□ Roaming automatically

Connection Status: Connecting

3. Adjust the settings as needed based on your Internet connection. The fields in this screen depend on the network and are described in *Table 4*.
4. The following buttons are available:
   - **Connect**. Manually connect to the network.
   - **Disconnect**. Disconnect from the current network.
   - **Apply**. Apply the changes that you made.

- **Cancel**. Discard changes.
- **Refresh**. Update the connection status.

Table 4. Mobile Broadband Settings fields[1]

Fields and check boxes	Description
User Name	Internet account login user name.
Password	Internet account password for authentication.
Country	Select your country from the drop-down list.
Internet Service Provider	Select your Internet service provider from the drop-down list.
Access Number	The remote site's phone number.
PIN code	PIN code of the SIM card, where applicable.
APN	Access point name.
PDP type	Select the type of packet data protocol: • **IP** • **PDP-IP** • **PPP** • **PPP-IP**
Connect automatically at startup	When this check box is selected, the modem automatically connects to the network when powered up. This should be selected after login information is provided.
Reconnect automatically when connection is lost	When this check box is selected, the modem attempts to reconnect to the network when the connection is lost. Under normal situations, this setting check box should be selected.
Roaming automatically	When this check box is selected, the unit might roam to any available operator in range and might incur roaming charges.
Wireless Button Configuration	Select the option to determine the behavior of the WPS button on the front panel when it is pressed. • **Control WiFi Only**: Pressing the button toggles the WiFi function. If WiFi is turned on, pressing the button turns off the WiFi. Pressing it again turns on the WiFi. This function is available only if the WiFi function is enabled. The wireless broadband function is unaffected. • **Control Both WiFi and Wireless Broadband**: Pressing the button toggles both the WiFi function and wireless broadband at the same time. If WiFi is turned on, pressing the button turns off the WiFi. At the same time, the wireless broadband connection is disconnected. If you press the button again, WiFi is turned on, and the router attempts to reestablish the wireless broadband connection. Depending on the coverage, wireless broadband coverage might or might not be connected successfully.
Connection status	Current WAN port status.

[1] *These fields and check boxes depend on the network.*

2. Wireless Settings 2

This chapter describes how to use the Wireless Settings screen to view and change (if needed) your wireless network settings. Security features to prevent objectionable content from reaching your computers are covered in *Chapter 3, Protecting Your Network* and *Chapter 6, Advanced Configuration*.

This chapter contains the following sections:

Wireless Adapter Compatibility

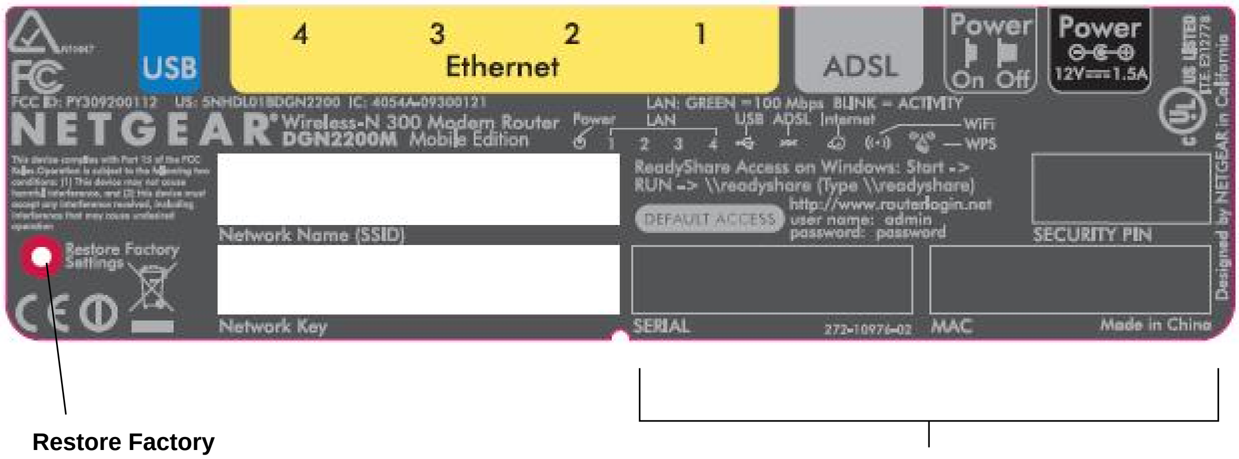
A wireless adapter is the wireless radio in your computer or laptop that lets the computer or laptop connect to a wireless network. Most computers and laptops come with an adapter already installed, but if it is outdated or slow, you can purchase a USB adapter to plug into a USB port.

Make sure the wireless adapter in each computer in your wireless network supports the same security settings as the wireless modem router. See *Preset Security* on page 29 for information about the wireless modem router's preconfigured security settings.

Note: If you connect devices to your wireless modem router using WPS as described in *Wi-Fi Protected Setup (WPS) Method* on page 32, those devices assume the security settings of the wireless modem router.

Preset Security

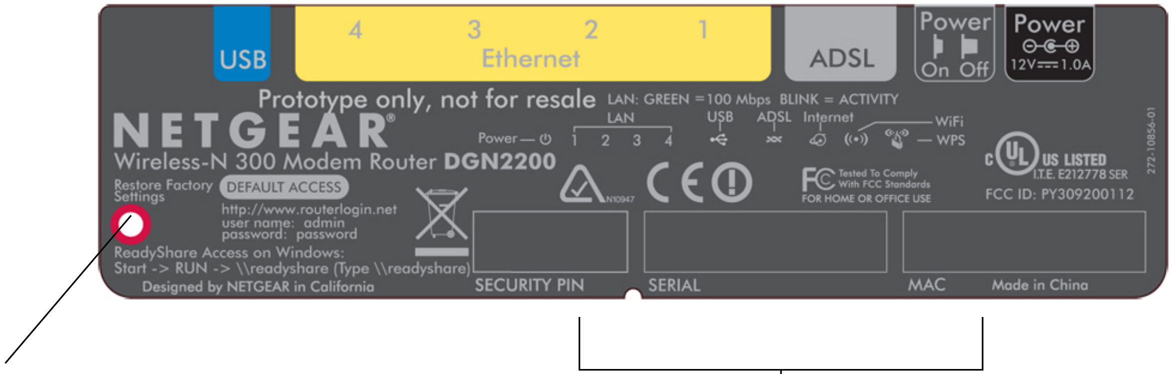
If label on your router looks like this, then it has preset security.


USB
4 3 2 1
Ethernet
ADSL
Power On Off
Power 12V 1.5A
FCC ID: PY309200112 US: 5NHDL01BDGN2200 IC: 4054A-09300121
NETGEAR
Wireless-N 300 Modem Router DGN2200M Mobile Edition
LAN: GREEN = 100 Mbps BLINK = ACTIVITY
Power LAN USB ADSL Internet WiFi WPS
ReadyShare Access on Windows: Start -> RUN -> \\readyshare (Type \\readyshare)
DEFAULT ACCESS
http://www.routerlogin.net
user name: admin
password: password
Network Name (SSID)
Network Key
SECURITY PIN
SERIAL
MAC
Restore Factory Settings
272-10976-02
Made in China
Designed by NETGEAR in California
US LISTED I.T.E. E212778

Restore Factory Settings: Press for 6 seconds.

Router information
- Default access address
- Default user name and password
- Security PIN
- Serial number
- MAC address

Note: If label on your router looks like the one in the following figure, then your router has no preset wireless security. You need to set the wireless security to protect your network.


USB
4 3 2 1
Ethernet
ADSL
Power On Off
Power 12V 1.0A
Prototype only, not for resale
LAN: GREEN = 100 Mbps BLINK = ACTIVITY
NETGEAR
Wireless-N 300 Modem Router DGN2200
Power LAN 1 2 3 4 USB ADSL Internet WiFi WPS
Restore Factory Settings
DEFAULT ACCESS
http://www.routerlogin.net
user name: admin
password: password
ReadyShare Access on Windows: Start -> RUN -> \\readyshare (Type \\readyshare)
Designed by NETGEAR in California
Tested To Comply With FCC Standards FOR HOME OR OFFICE USE
US LISTED I.T.E. E212778 SER
FCC ID: PY309200112
272-10856-01
SECURITY PIN
SERIAL
MAC
Made in China

Restore Factory Settings: Press for 6 seconds.

Router information
- Default access address
- Default user name and password
- Security PIN
- Serial number
- MAC address

The wireless modem router comes with preset security. This means that the WiFi network name (SSID), passphrase, and security option (encryption protocol) are preset in the factory. You can find the preset SSID and passphrase on the bottom of the unit.

- **WiFi network name (SSID)** identifies your network so devices can find it.
- **Passphrase** controls access to your network. Devices that know the SSID and the passphrase can find your wireless network and connect.

Note: The preset SSID and passphrase are uniquely generated for every device to protect and maximize your wireless security.

- **Security option** is the type of security protocol applied to your wireless network. The security protocol in force encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. The preset security option is WPA-PSK/WPA2-PSK mixed mode, described in *Wireless Security Options* on page 31.

The Wireless Settings screen lets you view and change the preset security settings. ***However, NETGEAR recommends that you not change your preset security settings***. If you do decide to change your preset security settings, make a note of the new settings and store it in a safe place where you can easily find it.

Security Basics

Unlike wired network data, wireless data transmissions extend beyond your walls and can be received by any device with a compatible wireless adapter (radio). For this reason, it is very important to maintain the preset security and understand the other security features available to you. Besides the preset security settings described in the previous section, your wireless modem router has the security features described here and in *Chapter 3, Protecting Your Network*.

- Turn off wireless connectivity
- Disable SSID broadcast
- Restrict access by MAC address
- Wireless security options

Turn Off Wireless Connectivity

You can turn off the wireless connectivity of the wireless modem router by pressing the **WiFi On/Off** button on its front panel ((•)). For example, if you use your laptop to wirelessly connect to your wireless modem router and you take a business trip, you can turn off the wireless portion of the wireless modem router while you are traveling. Other members of your household who use computers connected to the wireless modem router through Ethernet cables can still use the wireless modem router.

Disable SSID Broadcast

By default, the wireless modem router broadcasts its WiFi network name (SSID) so devices can find it. If you change this setting to not allow the broadcast, wireless devices will not find your wireless modem router unless they are configured with the same SSID. See *Wireless Access Point Settings* on page 37 for the procedure.

Note: Turning off SSID broadcast 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. If you allow the broadcast, be sure to keep wireless security enabled.

Restrict Access by MAC Address

You can enhance your network security by allowing access to only specific computers based on their Media Access Control (MAC) addresses. You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the wireless modem router. The wireless station MAC address filtering adds additional security protection to the wireless security option that you have in force. The access list determines which wireless hardware devices are allowed to connect to the wireless modem router by MAC address. See *Advanced Wireless Settings* on page 84 for the procedure.

Wireless Security Options

A security option is the type of security protocol applied to your wireless network. The security protocol encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. There are several types of encryption: Wi-Fi Protected Access II (WPA2), WPA, and Wired Equivalent Privacy (WEP). WPA2 is the latest and most secure, and is recommended if your equipment supports it. WPA has several options including pre-shared key (PSK) encryption and 802.1x encryption for enterprises. Note that it is also possible to disable wireless security. NETGEAR does *not* recommend this. You can view or change the wireless security options in the Wireless Settings screen. See *Wireless Settings Screen* on page 33.

Add Clients (Computers or Devices) to Your Network

Choose either the manual or the WPS method to add wireless computers or devices to your wireless network.

Manual Method

➢ **To add clients manually:**

1. Open the software that manages your wireless connections on the wireless device (laptop computer, gaming device, iPhone) that you want to connect to your wireless modem router. This software scans for all wireless networks in your area.
2. Look for your network and select it. If you did not change the name of your network during the setup process, look for the default WiFi network name (SSID) and select it. The default SSID is located on the product label on the bottom of the wireless modem router.
3. Enter the wireless modem router passphrase, and click **Connect**. The default wireless modem router passphrase is located on the product label on the bottom of the wireless modem router.
4. Repeat steps 1–3 to add other wireless devices.

Wi-Fi Protected Setup (WPS) Method

Wi-Fi Protected Setup (WPS) is a standard that lets you easily join a secure wireless network with WPA or WPA2 wireless security. The wireless modem router automatically sets security for each computer or device that uses WPS to join the wireless network. To use WPS, make sure that your wireless devices are Wi-Fi certified and support WPS. NETGEAR products that use WPS call it Push 'N' Connect.[1]

Note: If the SSID changes each time you add a WPS client, the Keep Existing Wireless Settings check box on the Advanced Wireless Settings screen has been cleared. See *Configure WPS Settings* on page 86 for more information about this setting.

You can use a WPS button or the wireless modem router interface method to add wireless computers and devices to your wireless network.

WPS Button Method

➢ **To add clients using the WPS button:**

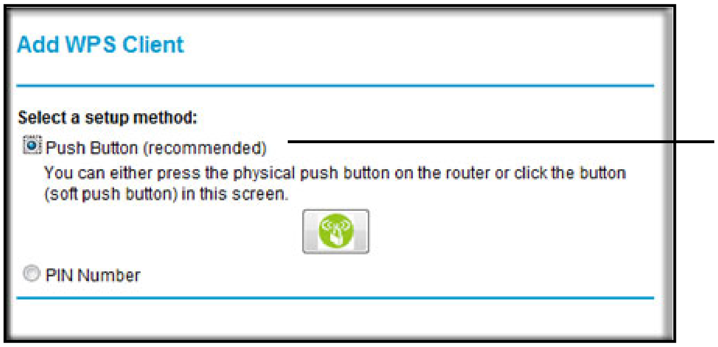
1. Press the **WPS** button on the wireless modem router front panel.
2. Within 2 minutes, press the **WPS** button on your wireless computer or device, or follow the WPS instructions that came with the computer. The device is now connected to your wireless modem router.
3. Repeat steps 1–2 to add other WPS wireless computers or devices.

[1] For a list of other Wi-Fi-certified products available from NETGEAR, go to http://www.wi-fi.org.

Wireless Modem Router Interface Method

➢ **To add clients using the wireless modem router interface:**

1. Select **Add WPS Client** at the top of the wireless modem router menus.
2. Click **Next**. The following screen lets you select the method for adding the WPS client.



Add WPS Client

Select a setup method:

● Push Button (recommended)

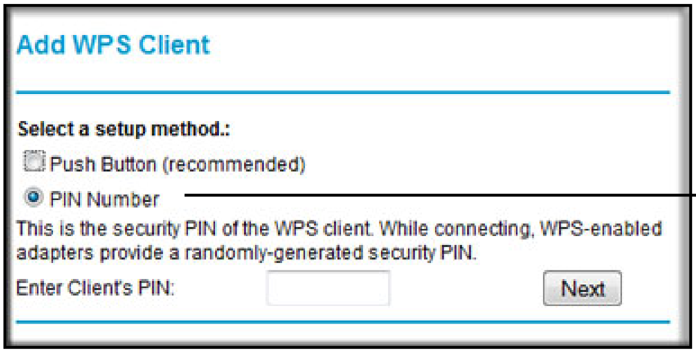
You can either press the physical push button on the router or click the button (soft push button) in this screen.

○ PIN Number

WPS Push button method

3. Select either **Push Button** or **PIN Number**. With either method, the wireless modem router tries to communicate with the computer or wireless device, set the wireless security for wireless device, and allow it to join the wireless network.

   The PIN method displays this screen so you can enter the client security PIN number:



Add WPS Client

Select a setup method.:

○ Push Button (recommended)

● PIN Number

This is the security PIN of the WPS client. While connecting, WPS-enabled adapters provide a randomly-generated security PIN.

Enter Client's PIN:

WPS PIN method

   While the wireless modem router attempts to connect, the WPS LED on the front of the wireless modem router blinks green. When the wireless modem router establishes a WPS connection, the LED is solid green, and the wireless modem router WPS screen displays a confirmation message.

4. Repeat to add another WPS client to your network.

Wireless Settings Screen

The Wireless Settings screen lets you view or change the wireless network settings. Note that your preset wireless modem router has a unique network name and password, located on the product label. NETGEAR recommends that you use these settings. If you decide to change them, note the new settings and save them in a secure location.

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

Consider Every Device on Your Network

Before you begin, check the following:

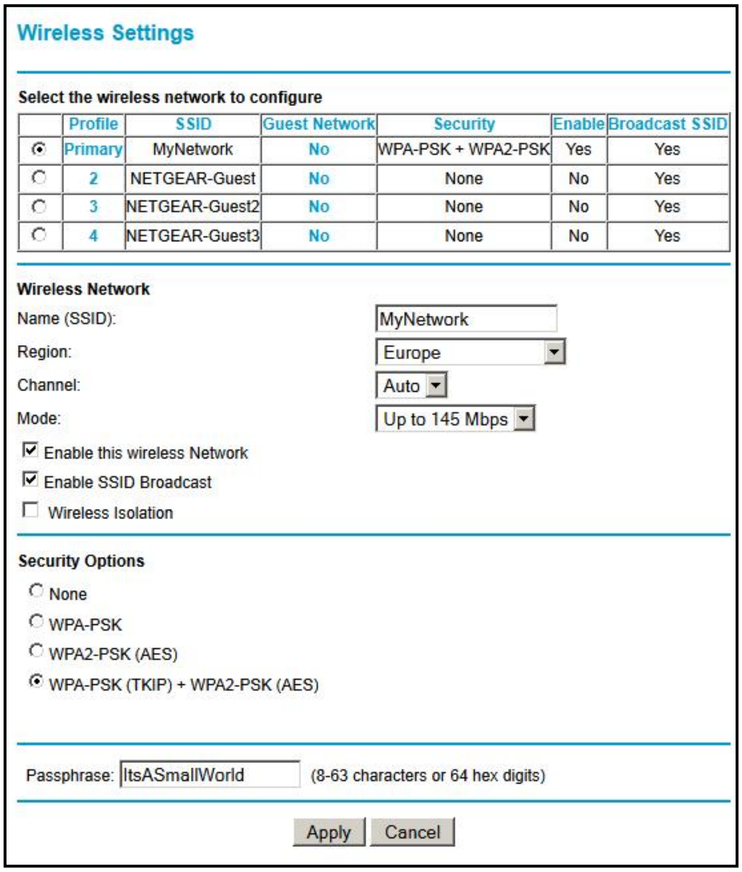
- Every wireless computer has to be able to obtain an IP address by DHCP from the wireless modem router.
- Each computer or wireless adapter in your network needs to have the same SSID and wireless mode (bandwidth and data rate) as the wireless modem router. Check that the wireless adapter on each computer can support the mode and security option you want to use.
- The security option on each wireless device in the network needs to match the wireless modem router. For example, if you select a security option that requires a passphrase, be sure to use same passphrase for each wireless computer in the network.

View or Change Wireless Settings

Your preset wireless modem router comes set up with a unique wireless network name (SSID) and network password. This information is printed on the label for your wireless modem router. You view or change these settings in the Wireless Settings screen. You can also use this screen to set up guest wireless networks.

➢ To view or change wireless settings:

1. Select **Setup > Wireless Settings** to display the following screen.



Wireless Settings

Select the wireless network to configure

	Profile	SSID	Guest Network	Security	Enable	Broadcast SSID
●	Primary	MyNetwork	No	WPA-PSK + WPA2-PSK	Yes	Yes
○	2	NETGEAR-Guest	No	None	No	Yes
○	3	NETGEAR-Guest2	No	None	No	Yes
○	4	NETGEAR-Guest3	No	None	No	Yes

Wireless Network

Name (SSID):	MyNetwork
Region:	Europe
Channel:	Auto
Mode:	Up to 145 Mbps

☑ Enable this wireless Network

☑ Enable SSID Broadcast

□ Wireless Isolation

Security Options

○ None

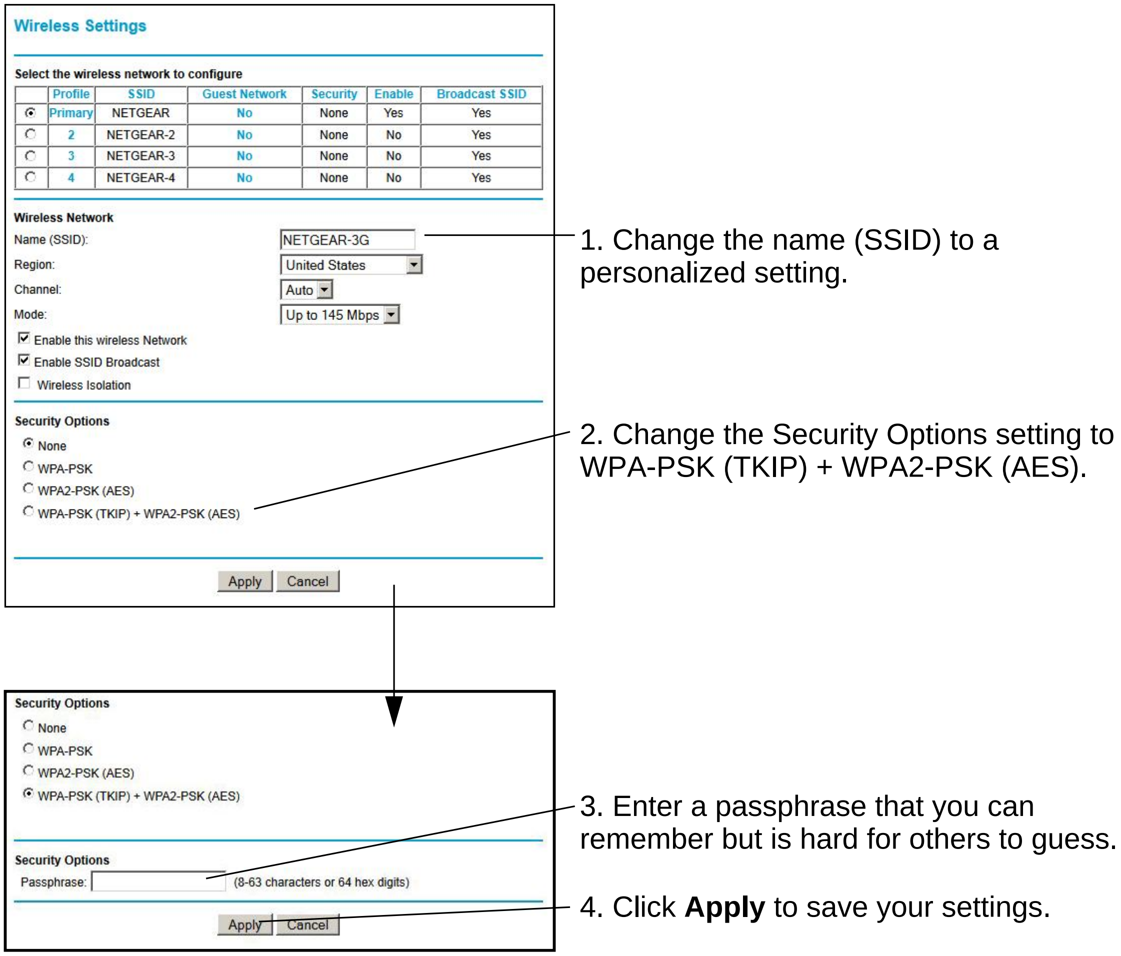
○ WPA-PSK

○ WPA2-PSK (AES)

● WPA-PSK (TKIP) + WPA2-PSK (AES)

Passphrase: ItsASmallWorld (8-63 characters or 64 hex digits)

Note: If your wireless security is not preset, the Wireless Settings screen looks like this:



Wireless Settings

Select the wireless network to configure

	Profile	SSID	Guest Network	Security	Enable	Broadcast SSID
●	Primary	NETGEAR	No	None	Yes	Yes
○	2	NETGEAR-2	No	None	No	Yes
○	3	NETGEAR-3	No	None	No	Yes
○	4	NETGEAR-4	No	None	No	Yes

Wireless Network

Name (SSID): NETGEAR-3G

Region: United States

Channel: Auto

Mode: Up to 145 Mbps

☑ Enable this wireless Network

☑ Enable SSID Broadcast

□ Wireless Isolation

Security Options

● None

○ WPA-PSK

○ WPA2-PSK (AES)

○ WPA-PSK (TKIP) + WPA2-PSK (AES)

Apply | Cancel

1. Change the name (SSID) to a personalized setting.

2. Change the Security Options setting to WPA-PSK (TKIP) + WPA2-PSK (AES).

Security Options

○ None

○ WPA-PSK

○ WPA2-PSK (AES)

● WPA-PSK (TKIP) + WPA2-PSK (AES)

Security Options

Passphrase: (8-63 characters or 64 hex digits)

Apply | Cancel

3. Enter a passphrase that you can remember but is hard for others to guess.

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

2. Select the wireless network that you want to configure.
3. Make any changes that are needed, and click **Apply** when done to save your settings.

Note: The screen sections, settings, and procedures are explained in the following sections.

4. Set up and test your computers for wireless connectivity:
   - **a.** Use your wireless computer or device to join your network. When prompted, enter the network password.
   - **b.** From the wirelessly connected computer, make sure that you can access the Internet.

Wireless Settings Screen Fields

Wireless Network

The primary network is the one that you usually use. You can set up guest networks too. You can customize access so that people who use their computers to access your guest network can use the Internet, but they do not have access to the rest of your home 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 for your primary network is randomly generated, and there is typically no need to change it. If you want to set up guest networks, NETGEAR does recommend that you customize the default guest network names (SSIDs).
- **Region**. The location where the wireless modem router is used. It might not be legal to operate the wireless modem router in a region other than the regions listed.
- **Channel**. The wireless channel used by the gateway: 1 through 13. Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which is the best.
- **Mode**. Up to 150 Mbps is the default and allows 802.11n and 802.11g wireless devices to join the network. g & b supports up to 54 Mbps. Up to 65 Mbps supports up to 65 Mbps.

Wireless Access Point Settings

- **Enable this wireless network**. When this check box is selected, the wireless modem router accepts wireless clients for the network. By default, this check box is selected for your primary network. If you clear this check box, the wireless modem router accepts wired clients only.
- **Allow Broadcast of Name (SSID)**. This setting allows the wireless modem router to broadcast its SSID so that a wireless station can display this wireless name (SSID) in its scanned network list. This check box is selected by default. To turn off the SSID broadcast, clear the **Allow Broadcast of Name (SSID)** check box and click **Apply**.
- **Wireless Isolation**. When this check box is selected, wireless stations cannot communicate with each other or with stations on the wired network. By default, this check box is not selected.

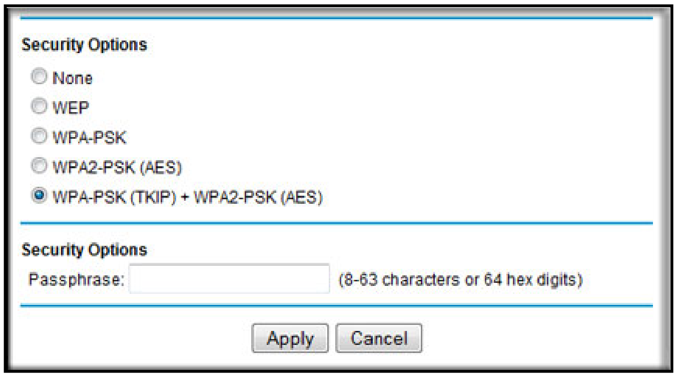
Security Options Settings

The Security Options section of the Wireless Settings screen lets you change the security option and passphrase. The primary network for your preset wireless modem router is already set up with WPA2 and WPA security. NETGEAR recommends that you set up wireless security for each guest network that you plan to use. For information about changing these settings, see the following section, *Change WPA Security Option and Passphrase*, and *Set WEP Encryption and Passphrase* on page 38.

Change WPA Security Option and Passphrase

➢ **To change the WPA security option and passphrase:**

1. In the Security Options section, select the WPA option that you want.



Security Options

○ None
○ WEP
○ WPA-PSK
○ WPA2-PSK (AES)
● WPA-PSK (TKIP) + WPA2-PSK (AES)

Security Options

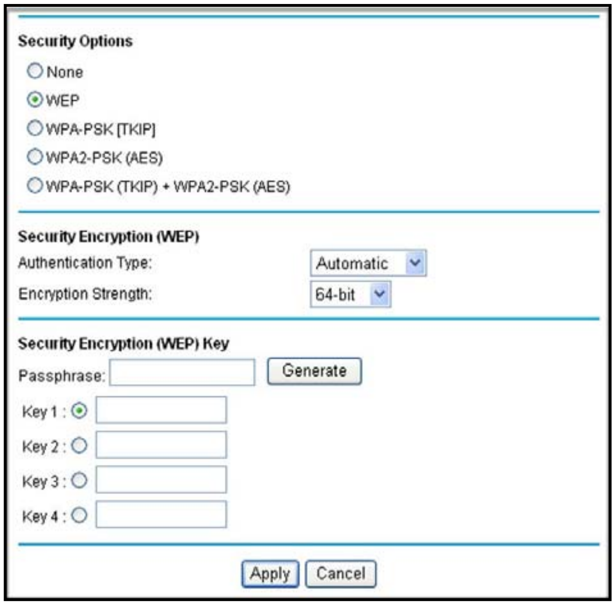
Passphrase: (8-63 characters or 64 hex digits)

2. Enter the passphrase that you want to use. It is a text string from 8 to 63 characters.
3. Click **Apply**.

Set WEP Encryption and Passphrase

➢ **To set WEP encryption and passphrase:**

1. In the Security Options section of the Wireless Settings screen, select **WEP**:



Security Options

○ None
● WEP
○ WPA-PSK [TKIP]
○ WPA2-PSK (AES)
○ WPA-PSK (TKIP) + WPA2-PSK (AES)

Security Encryption (WEP)

Authentication Type: Automatic

Encryption Strength: 64-bit

Security Encryption (WEP) Key

Passphrase:

Key 1 : ●
Key 2 : ○
Key 3 : ○
Key 4 : ○

2. Select the authentication type. The default is Automatic. Other choices are Open System (any client can authenticate itself to the network) and Shared Key (a passphrase and a four-way challenge are needed for authentication).
3. Select the encryption strength setting, either 64-bit or 128-bit.

4. Enter the four data encryption keys either manually or automatically. These values need to 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 fields are automatically populated with key values.
   - **Manual**. The number of hexadecimal digits that you 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).
5. Select the radio button for the key you want to make active.

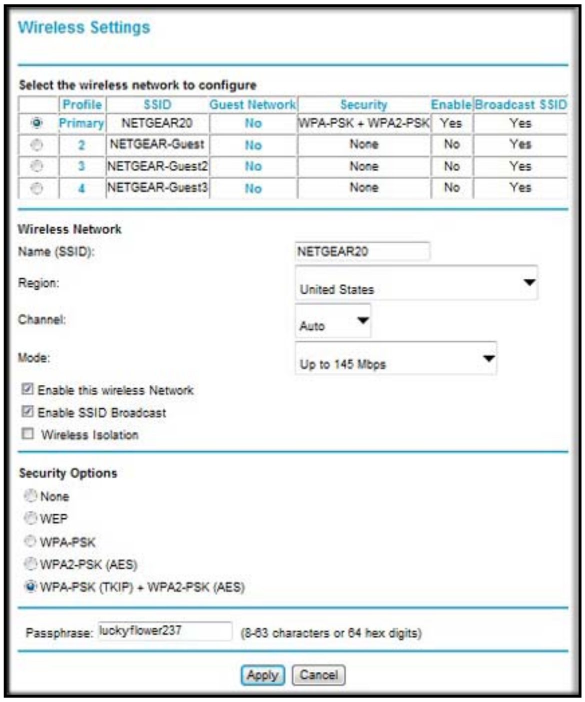
   Make sure that you understand how the WEP key settings are configured in your wireless adapter. Wireless adapter configuration utilities such as the one in Windows XP allow one key entry, which has to match the default key you set in the wireless modem router.
6. Click **Apply**.

Wireless Guest Networks

A wireless guest network allows you to provide guests access to your wireless network without prior authorization of each individual guest. You can configure wireless guest networks and specify the security options for each wireless guest network.

➢ **To set up a wireless guest network:**

1. Select **Setup > Wireless Settings**.



Wireless Settings

Select the wireless network to configure

	Profile	SSID	Guest Network	Security	Enable	Broadcast SSID
●	Primary	NETGEAR20	No	WPA-PSK + WPA2-PSK	Yes	Yes
○	2	NETGEAR-Guest	No	None	No	Yes
○	3	NETGEAR-Guest2	No	None	No	Yes
○	4	NETGEAR-Guest3	No	None	No	Yes

Wireless Network

Name (SSID): NETGEAR20

Region: United States

Channel: Auto

Mode: Up to 145 Mbps

☑ Enable this wireless Network

☑ Enable SSID Broadcast

☐ Wireless Isolation

Security Options

○ None

○ WEP

○ WPA-PSK

○ WPA2-PSK (AES)

● WPA-PSK (TKIP) + WPA2-PSK (AES)

Passphrase: luckyflower237 (8-63 characters or 64 hex digits)

2. Select the radio button for the network profile that you want to set up.
3. You can specify whether the SSID broadcast is enabled and whether you want to allow guests to access your local network. You can also change the SSID.
    - NETGEAR strongly recommends that you change the SSID to a different name. Note that the SSID is case-sensitive. For example, GuestNetwork is not the same as Guestnetwork.
    - For guest networks, wireless security is disabled by default. NETGEAR strongly recommends that you implement wireless security for the guest network.
4. Select a security option for the guest network, and specify the password.
5. When you have finished making changes, click **Apply**.

3. Protecting Your Network

3

This chapter describes how to use the basic firewall features of the wireless modem router to protect your network. The chapter includes:

- *Protect Access to Your Wireless-N Modem Router*
- *Block Keywords, Sites, and Services*
- *Set Times and Schedule Firewall Services*
- *Enable Security Event Email Notification*
- *Live Parental Controls*

Protect Access to Your Wireless-N Modem Router

For security reasons, the wireless modem router has its own user name and password. Also, after a period of inactivity for a set length of time, the login automatically disconnects. You can use the following procedures to change the wireless modem router's password and the period for the administrator's login time-out.

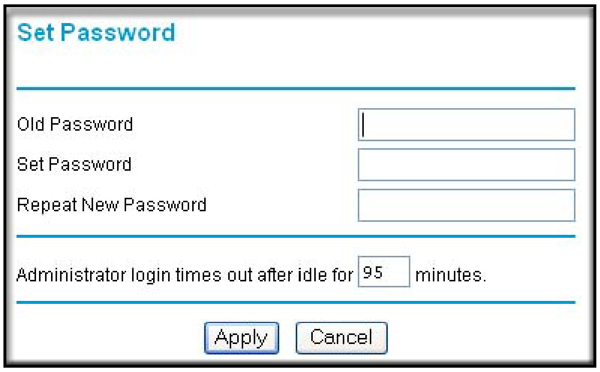
Note: The user name and password are not the same as any other user name or password your might use to log in to your Internet connection.

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

Change the Built-In Password

➢ **To change the build-in password:**

1. In the main menu, under Maintenance, select **Set Password**.



Set Password

Old Password

Set Password

Repeat New Password

Administrator login times out after idle for 95 minutes.

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

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

Change the Administrator Login Time-Out

For security, the administrator's login to the wireless modem router configuration times out after a period of inactivity.

➢ **To change the login time-out period:**

1. In the Set Password screen, type a number in the Administrator login times out field. The suggested default value is 5 minutes.
2. Click **Apply** to save your changes, or click **Cancel** to keep the current period.

Block Keywords, Sites, and Services

The wireless modem router provides a variety of options for blocking Internet-based content and communications services. With its content filtering feature, the wireless modem router prevents objectionable content from reaching your computers. The wireless modem router allows you to control access to Internet content by screening for keywords within web addresses. Key content filtering options include:

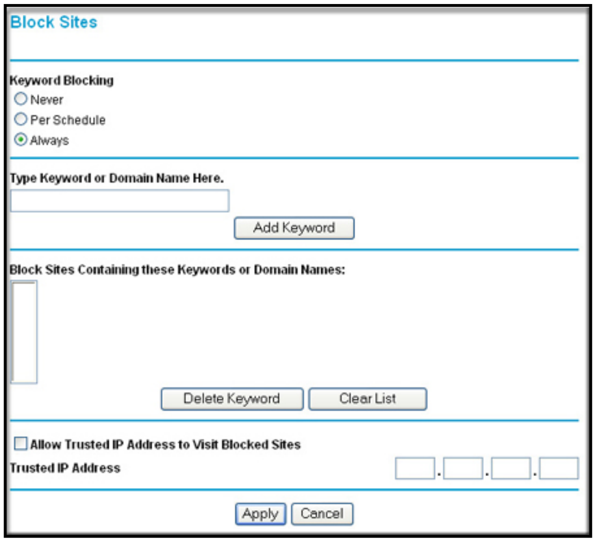
- Keyword blocking of HTTP traffic.

- Outbound service blocking. Limits access from your LAN to Internet locations or services that you specify as off-limits.
- Denial of service (DoS) protection. Automatically detects and thwarts denial of service (DoS) attacks such as Ping of Death, SYN flood, LAND Attack, and IP spoofing.
- Blocking unwanted traffic from the Internet to your LAN.

Block Sites

➢ **To block keywords and sites:**

1. In the main menu, under Content Filtering, select **Block Sites**:



Block Sites

Keyword Blocking

○ Never
○ Per Schedule
● Always

Type Keyword or Domain Name Here.

Block Sites Containing these Keywords or Domain Names:

□ Allow Trusted IP Address to Visit Blocked Sites

Trusted IP Address . . .

2. To enable keyword blocking, select one of the following:
   - **Per Schedule**. Turn on keyword blocking according to the settings in the Schedule screen.
   - **Always**. Turn on keyword blocking all the time, independent of the Schedule screen.
3. Enter a keyword or domain in the Keyword field, click **Add Keyword**, and then click **Apply**.

   Some examples of keyword application follow:

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

   Up to 32 entries are supported in the Keyword list.
4. To delete a keyword or domain, select it from the list, click **Delete Keyword**, and then click **Apply**.
5. To specify a trusted user, enter that computer’s IP address in the Trusted IP Address field, and click **Apply**.

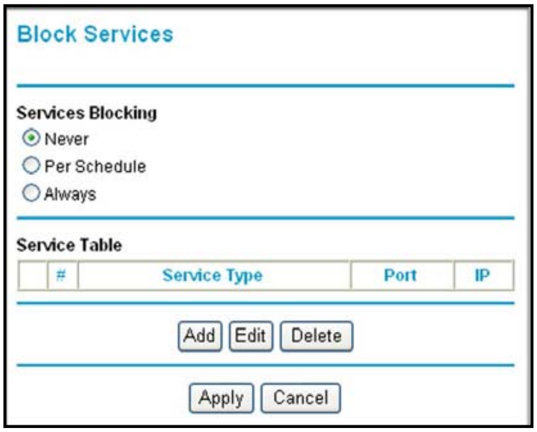
You can specify one trusted user, which is a computer that will be exempt from blocking and logging. Since the trusted user will be identified by an IP address, you should configure that computer with a fixed IP address.

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

Block Services

➢ **To block services:**

1. In the main menu, under Content Filtering, select **Block Services**.



Block Services

Services Blocking

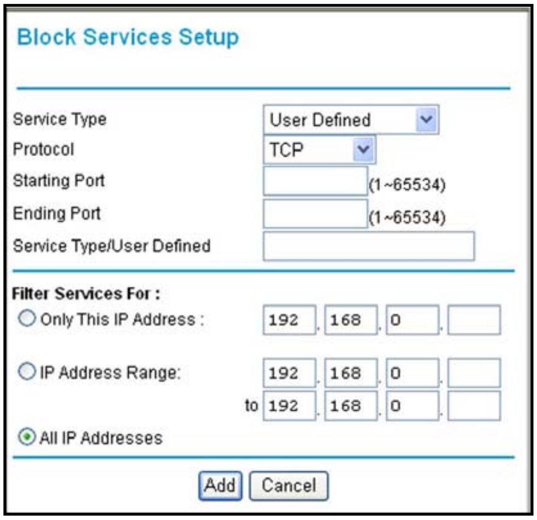
● Never
○ Per Schedule
○ Always

Service Table

	#	Service Type	Port	IP

2. Select one of the following:
   - **Per Schedule**. Turn on keyword blocking according to the settings in the Schedule screen.
   - **Always**. Turn on keyword blocking all the time, independent of the Schedule screen.

3. Click **Add**, and the following screen displays:



Block Services Setup

Service Type	User Defined
Protocol	TCP
Starting Port	(1~65534)
Ending Port	(1~65534)
Service Type/User Defined	

Filter Services For :

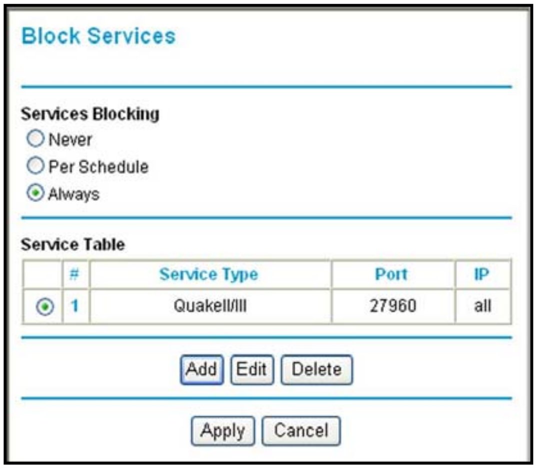
○ Only This IP Address : 192 . 168 . 0 .

○ IP Address Range: 192 . 168 . 0 .
to 192 . 168 . 0 .

● All IP Addresses

4. Either select a service from the Service Type drop-down list, or select **User Defined** to create a custom service.

5. Click **Add** to create the service, and the service is listed in the Service Table:



Block Services

Services Blocking

○ Never
○ Per Schedule
● Always

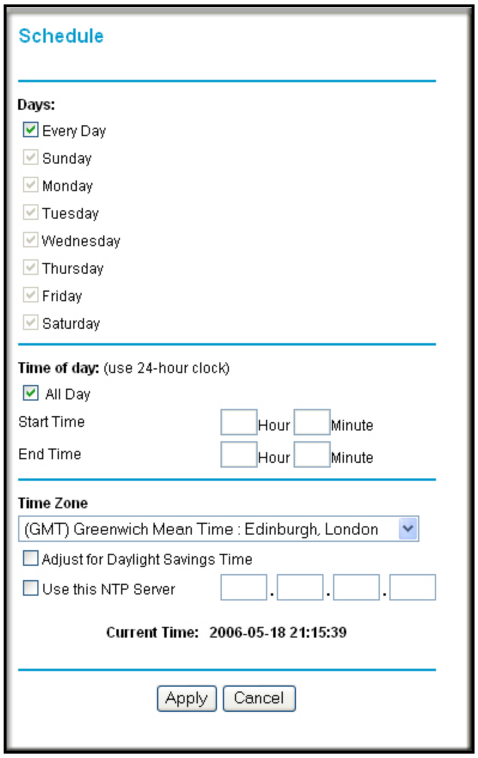
Service Table

	#	Service Type	Port	IP
●	1	QuakeII/III	27960	all

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

Set Times and Schedule Firewall Services

The wireless modem router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet. On the router menu, select **Schedule** under Security to display the Security screen:



Schedule

Days:

☑ Every Day
☑ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday

Time of day: (use 24-hour clock)

☑ All Day

Start Time □ Hour □ Minute

End Time □ Hour □ Minute

Time Zone

(GMT) Greenwich Mean Time : Edinburgh, London

□ Adjust for Daylight Savings Time

□ Use this NTP Server □ . □ . □ . □

Current Time: 2006-05-18 21:15:39

Set Your Time Zone

➢ **To localize the time for your log entries:**

1. In the Schedule screen, select your time zone.

   This setting is used for the blocking schedule according to your local time zone and for time-stamping log entries.

2. If your time zone is currently in daylight savings time, select the **Adjust for Daylight Savings Time** check box.

Note: If your region uses daylight savings time, you need to manually select **Adjust for Daylight Savings Time** on the first day of daylight savings time, and clear it at the end. Enabling daylight savings time causes 1 hour to be added to the standard time.

3. The wireless modem router has a list of NETGEAR NTP servers. If you would prefer to use a particular NTP server as the primary server, select the **Use this NTP Server** check box, and enter its IP address.
4. Click **Apply** to save your settings.

Schedule Firewall Services

If you enabled service blocking in the Block Services screen or port forwarding in the Port Forwarding/Port Triggering screen, you can set up a schedule for when blocking occurs or when access is not restricted.

➢ **To block Internet services based on a schedule:**

1. From the Schedule screen, select **Every Day**, or select one or more days.
2. If you want to limit access completely for the selected days, select **All Day**. Otherwise, to limit access during certain times for the selected days, or enter times in the Start Time and End Time fields.

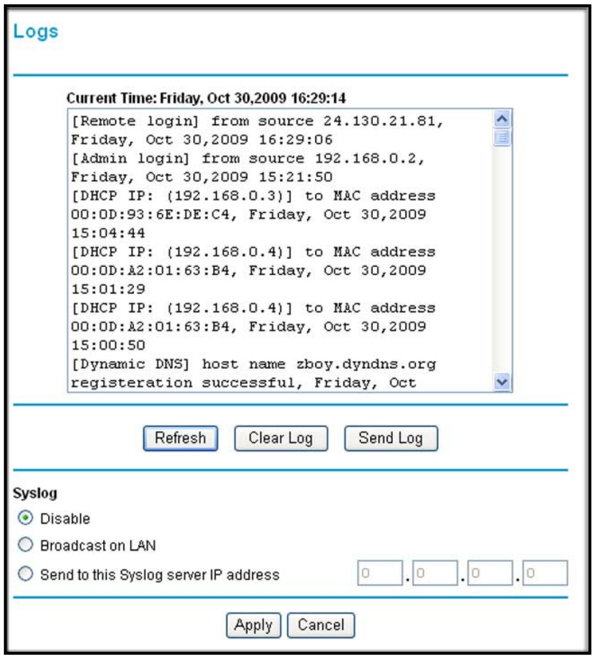
Note: Enter the values in 24-hour time format. For example, 10:30 a.m. would be 10 hours and 30 minutes, and 10:30 p.m. would be 22 hours and 30 minutes. If you set the start time after the end time, the schedule will be effective through midnight the next day.

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

View, Select, and Save Logged Information

The wireless modem router logs security-related events such as denied incoming service requests, hacker probes, and administrator logins. If you enable content filtering in the Block Sites screen, the Logs screen show you when someone on your network tries to access a blocked site. If you enable email notification, you will receive these logs in an email message.

To view the log, under Content Filtering, select **Logs**. A screen similar to the following displays:



Current Time: Friday, Oct 30,2009 16:29:14

```
[Remote login] from source 24.130.21.81,
Friday, Oct 30,2009 16:29:06
[Admin login] from source 192.168.0.2,
Friday, Oct 30,2009 15:21:50
[DHCP IP: (192.168.0.3)] to MAC address
00:0D:93:6E:DE:C4, Friday, Oct 30,2009
15:04:44
[DHCP IP: (192.168.0.4)] to MAC address
00:0D:A2:01:63:B4, Friday, Oct 30,2009
15:01:29
[DHCP IP: (192.168.0.4)] to MAC address
00:0D:A2:01:63:B4, Friday, Oct 30,2009
15:00:50
[Dynamic DNS] host name zboy.dyndns.org
registeration successful, Friday, Oct
```

● Disable
○ Broadcast on LAN
○ Send to this Syslog server IP address 0 . 0 . 0 . 0

You can write the logs to a computer running a syslog program. To activate this feature, select **Broadcast on LAN**, or enter the IP address of the server where the syslog file will be written.

Table 5. Security log entry descriptions

Field	Description
Date and time	The date and time the log entry was recorded.
Description or action	The type of event and what action was taken, if any.
Source IP	The IP address of the initiating device for this log entry.
Source port and interface	The service port number of the initiating device, and whether it originated from the LAN or WAN.
Destination	The name or IP address of the destination device or website.
Destination port and interface	The service port number of the destination device, and whether it is on the LAN or WAN.

Examples of Log Messages

Following are examples of log messages. In all cases, the log entry shows the time stamp as day, year-month-date hour:minute:second.

Activation and Administration

```
Tue, 2011-05-21 18:48:39 - NETGEAR activated
```

This entry indicates a power-up or reboot with initial time entry.

```
Tue, 2011-05-21 18:55:00 - Administrator login successful-IP:192.168.0.2
Thu, 2011-05-21 18:56:58 - Administrator logout - IP:192.168.0.2
```

This entry shows an administrator logging in to and out from IP address 192.168.0.2.

```
Tue, 2011-05-21 19:00:06 - Login screen timed out - IP:192.168.0.2
```

This entry shows a time-out of the administrator login.

```
Wed, 2011-05-22 22:00:19 - Log emailed
```

This entry shows when the log was emailed.

Dropped Packets

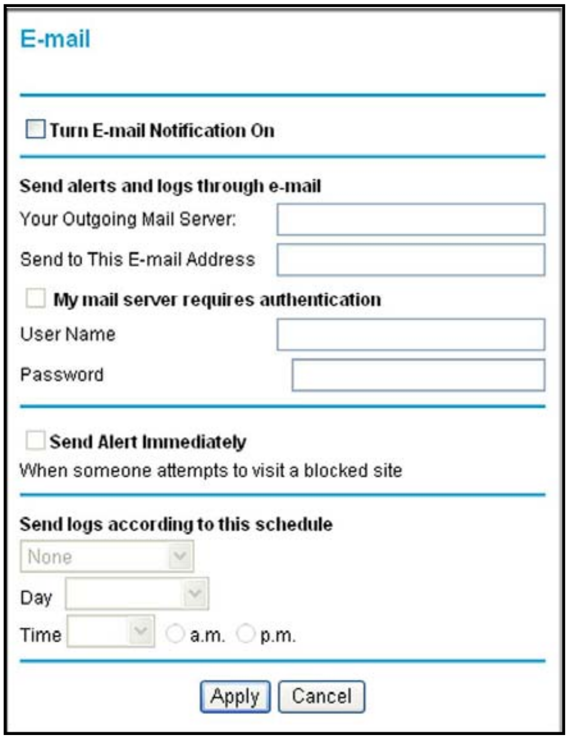
```
Wed, 2011-05-22 07:15:15 - TCP packet dropped - Source:64.12.47.28,4787,WAN -
Destination:134.177.0.11,21,LAN - [Inbound Default rule match]
Sun, 2011-05-22 12:50:33 - UDP packet dropped - Source:64.12.47.28,10714,WAN -
Destination:134.177.0.11,6970,LAN - [Inbound Default rule match]
Sun, 2011-05-22 21:02:53 - ICMP packet dropped -
Source:64.12.47.28,0,WAN - Destination:134.177.0.11,0,LAN - [Inbound Default
rule match]
```

These entries show an inbound FTP (port 21) packet, a User Datagram Protocol (UDP) packet (port 6970), and an Internet Control Message Protocol (ICMP) packet (port 0) being dropped as a result of the default inbound rule, which states that all inbound packets are denied.

Enable Security Event Email Notification

To receive logs and alerts by email, you need to provide your email information in the E-mail screen and specify which alerts you would like to receive and how often.

In the main menu, under Security, select **E-mail**. The E-mail screen displays.



E-mail

☐ Turn E-mail Notification On

Send alerts and logs through e-mail

Your Outgoing Mail Server:

Send to This E-mail Address

☐ My mail server requires authentication

User Name

Password

☐ Send Alert Immediately

When someone attempts to visit a blocked site

Send logs according to this schedule

None

Day

Time ○ a.m. ○ p.m.

You can make the following selections:

- **Turn E-mail Notification On**. Select this check box if you want to receive email logs and alerts from the wireless modem router.
- **Your Outgoing Mail Server**. Enter the name or IP address of your ISP’s outgoing (SMTP) mail server (such as mail.myISP.com). You might be able to find this information in the configuration settings of your email program.
- **Send to This E-mail Address**. Enter the email address to which logs and alerts are sent. This email address is also used as the From address. If you leave this field blank, log and alert messages are not sent through email.
- **My mail server requires authentication**. If you use an outgoing mail server provided by your current ISP, you do not need to select this check box. If you use an email account that is not provided by your ISP, select this check box, and enter the required user name and password information.
- **Send Alert immediately**. Select this check box if you would like immediate notification of a significant security event, such as a known attack, port scan, or attempted access to a blocked site.
- **Send logs according to this schedule**. Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.

- Day for sending log
  Specifies which day of the week to send the log. Relevant when the log is sent weekly.
- Time for sending log
  Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

If the Weekly, Daily, or Hourly option is selected and the log fills up before the specified period, the log is automatically emailed to the specified email address. After the log is sent, it is cleared from the wireless modem router's memory. If the wireless modem router cannot email the log file, the log buffer might fill up. In this case, the wireless modem router overwrites the log and discards its contents.

Live Parental Controls

NETGEAR Live Parental Controls, powered by OpenDNS, is a router-based web filtering solution available on NETGEAR Wireless-N router and gateway products. Designed to protect you from identity theft and scams, Live Parental Control blocks up to 50 categories of Internet content.

Live Parental Controls helps keep your family safe online, but like all web filtering tools, it is not perfect. NETGEAR reminds you there is no substitute for keeping the family computer in a common area and in plain sight where you can monitor the websites your kids are visiting, and taking caution when visiting websites requesting personal or financial information.

Download Live Parental Controls from this website: *http://www.netgear.com/lpc*

Web-Based Access

Live Parental Controls is the first to allow parents or network administrators to manage settings while away from home or office. This is particularly convenient when access exceptions need to be made. And since settings are stored on the web, using a browser interface to manage them is not difficult at all.

Total Home Protection

Live Parental Controls protects all Internet-connected devices through the router. It protects not only computers, but also set-top boxes, iPhones, iPods, and gaming consoles that are attached to your network. You no longer need to worry about phones and gaming consoles not being protected when kids use them in their own rooms. Even guest computers accessing the Internet through your network are protected.

Flexible Settings

You might have your own computer, or you might be sharing a computer with other members in the family. Default and settings for individual users allow you to customize configuration for different computing arrangements and personalize the settings for each person. Setting according to time allow Internet access during scheduled time slots to help manage the balance between work and play.

Minimal Software Installation

Installation requires a one-time installation of a management utility program. Once Live Parental Controls is set up, the software runs in the background and does not interfere with normal Internet usage.

Managing Your Network

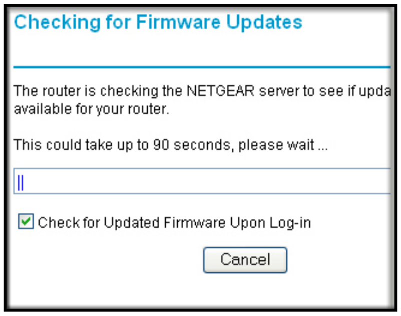
4

This chapter describes how to perform network management tasks with your wireless modem router. This chapter includes these sections:

- *Upgrade the Firmware*
- *Back Up, Restore, and Erase Your Settings*
- *Router Status and Usage Statistics*
- *View Attached Devices*
- *Run Diagnostics and Reboot*
- *Configure Remote Management* on page 62

Upgrade the Firmware

The wireless modem router's firmware (routing software) is stored in flash memory. By default, when you log in to your wireless modem router, it automatically checks the NETGEAR website for new firmware and alerts you if there is a newer version.



Checking for Firmware Updates

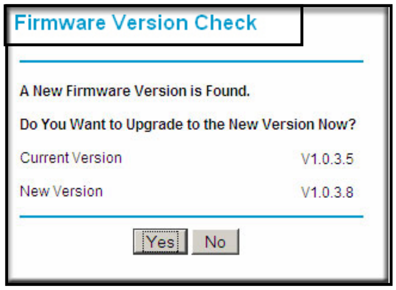
The router is checking the NETGEAR server to see if upda available for your router.

This could take up to 90 seconds, please wait ...

☑ Check for Updated Firmware Upon Log-in

Note: To turn off the automatic firmware check at login, clear the **Check for Updated Firmware Upon Log-in** check box on the Router Upgrade screen.

If the wireless modem router discovers a newer version of firmware, the message on the left displays. If no new firmware is available, the message on the right displays.

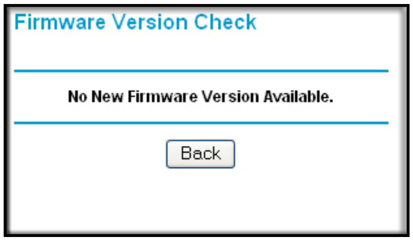

Firmware Version Check

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


Firmware Version Check

No New Firmware Version Available.

To upgrade, click **Yes** to allow the wireless modem router to download and install the new firmware.

WARNING:

When uploading firmware to the wireless modem 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.

When the upload is complete, your wireless modem router automatically restarts. The upgrade process could take a few minutes. Read the new firmware release notes to determine whether you need to reconfigure the wireless modem router after upgrading.

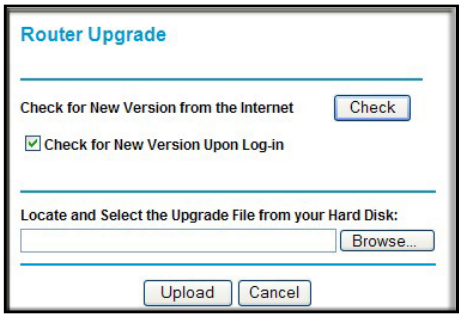
Manually Check for Firmware Upgrades

You can use the Router Upgrade screen to manually check the NETGEAR website for newer versions of firmware for your product.

➢ **To manually check for new firmware and install it on your wireless modem router:**

1. On the main menu, under Maintenance, select **Router Status**. Note the version number of your wireless modem router firmware.
2. Go to the DGN2200M Mobile Edition support page on the NETGEAR website at *http://www.netgear.com/support*.
3. If the firmware version on the NETGEAR website is newer than the firmware on your wireless modem router, download the file to your computer.

4. On the main menu, under Maintenance, select **Router Upgrade**.



Router Upgrade

Check for New Version from the Internet

☑ Check for New Version Upon Log-in

Locate and Select the Upgrade File from your Hard Disk:

5. Click **Browse**, and locate the firmware you downloaded (the file ends in .img or .chk).
6. Click **Upload** to send the firmware to the wireless modem router.

WARNING:

When uploading firmware to the wireless modem 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.

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

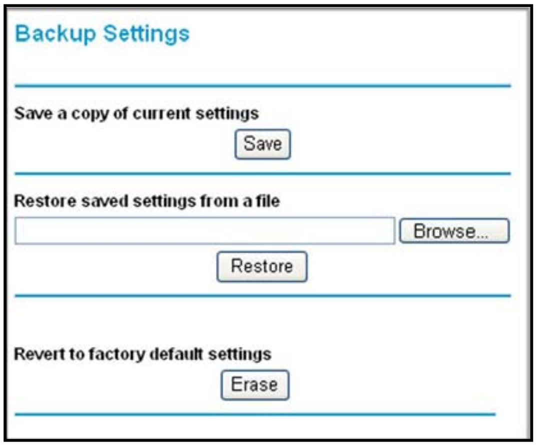
Back Up, Restore, and Erase Your Settings

The configuration settings of the wireless modem router are stored in a configuration file. This file can be backed up to your computer, restored, or reverted to factory default settings.

Back Up the Configuration to a File

➢ **To back up the configuration to a file:**

1. From the main menu, under Maintenance, select **Backup Settings** to display this screen:



Backup Settings

Save a copy of current settings

Restore saved settings from a file

Revert to factory default settings

2. Click **Save** to save a copy of the current settings.
3. Store the .cfg file on a computer on your network.

Restore the Configuration from a File

➢ **To restore the configuration from a file:**

1. In the main menu, under Maintenance, select **Backup Settings**.
2. Enter the full path to the file on your network, or click the **Browse** button to locate the file.
3. When you have located the .cfg file, click the **Restore** button to upload the file to the wireless modem router.
4. The wireless modem router then reboots automatically.

Erase the Configuration

Sometimes you might want to restore the wireless modem router to the factory default settings. You can do this by using the erase function.

➢ **To erase the configuration:**

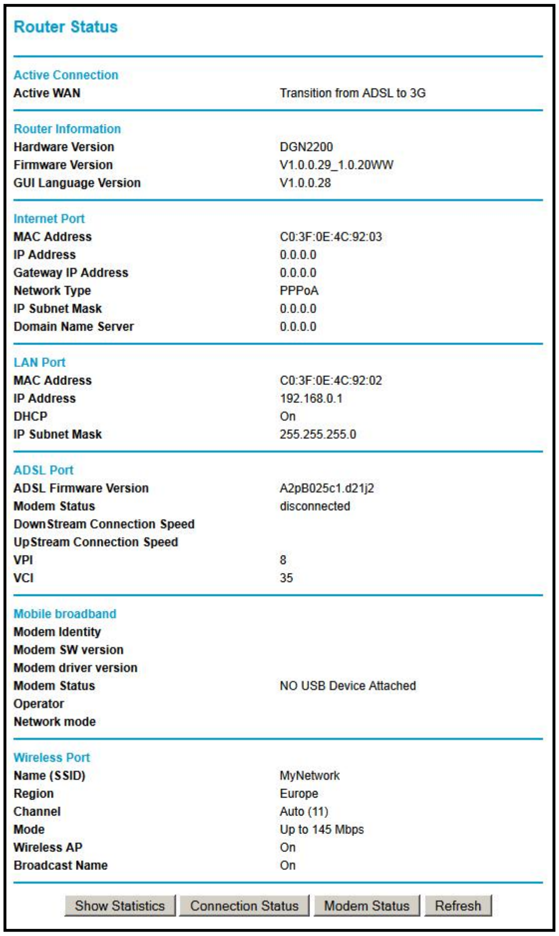
1. In the main menu, under Maintenance, select **Backup Settings**, and click the **Erase** button.
2. The wireless modem router then reboots automatically.

   After an erase, the wireless modem router’s password is **password**, the LAN IP address is **192.168.0.1**, and the wireless modem router’s DHCP client is enabled.

Note: To restore the factory default configuration settings when you do not know the login password or IP address, press the **Restore Factory Settings** button on the bottom of the wireless modem router for 6 seconds.

Router Status and Usage Statistics

In the main menu, under Maintenance, select **Router Status**.



Router Status

Active Connection	
Active WAN	Transition from ADSL to 3G
Router Information	
Hardware Version	DGN2200
Firmware Version	V1.0.0.29_1.0.20WW
GUI Language Version	V1.0.0.28
Internet Port	
MAC Address	C0:3F:0E:4C:92:03
IP Address	0.0.0.0
Gateway IP Address	0.0.0.0
Network Type	PPPoA
IP Subnet Mask	0.0.0.0
Domain Name Server	0.0.0.0
LAN Port	
MAC Address	C0:3F:0E:4C:92:02
IP Address	192.168.0.1
DHCP	On
IP Subnet Mask	255.255.255.0
ADSL Port	
ADSL Firmware Version	A2pB025c1.d21j2
Modem Status	disconnected
DownStream Connection Speed	
UpStream Connection Speed	
VPI	8
VCI	35
Mobile broadband	
Modem Identity	
Modem SW version	
Modem driver version	
Modem Status	NO USB Device Attached
Operator	
Network mode	
Wireless Port	
Name (SSID)	MyNetwork
Region	Europe
Channel	Auto (11)
Mode	Up to 145 Mbps
Wireless AP	On
Broadcast Name	On

Table 6. Router Status fields

Field	Description
Account Name	The host name assigned to the router in the Basic Settings screen.
Firmware Version	The wireless modem router firmware version.

Table 6. Router Status fields (continued)

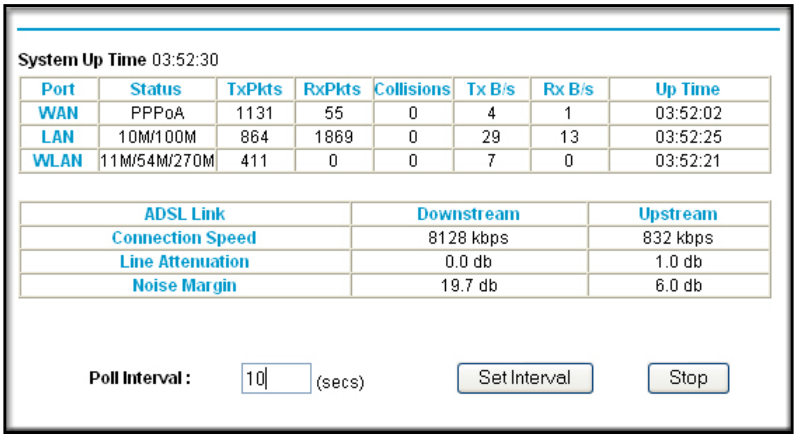
Field		Description
ADSL Port	MAC Address	The Ethernet MAC address being used by the Internet (ADSL) port.
	IP Address	The IP address used by the Internet (ADSL) port. If no address is shown, the wireless modem router cannot connect to the Internet.
	Network Type	The network type depends upon your ISP.
	IP Subnet Mask	The IP subnet mask used by the Internet (ADSL) port.
	Gateway IP Address	IP address used as a gateway to the Internet for computers configured to use DHCP.
	Domain Name Server	The DNS server IP addresses used by the wireless modem router. These addresses are usually obtained dynamically from the ISP.
LAN Port	MAC Address	This field displays the Ethernet MAC address being used by the local (LAN) port of the wireless modem router.
	IP Address	This field displays the IP address being used by the local (LAN) port of the wireless modem router. The default is 192.168.0.1.
	DHCP	If Off, the wireless modem router does not assign IP addresses to computers on the LAN. If On, the wireless modem router does assign IP addresses to computers on the LAN.
	IP Subnet Mask	This field displays the IP subnet mask being used by the local (LAN) port of the wireless modem router. The default is 255.255.255.0.
Modem	ADSL Firmware Version	The version of the firmware.
	Modem Status	The connection status of the modem.
	DownStream Connection Speed	The speed at which the modem is receiving data from the ADSL line.
	UpStream Connection Speed	The speed at which the modem is transmitting data to the ADSL line.
	VPI	The Virtual Path Identifier setting.
	VCI	The Virtual Channel Identifier setting.

Table 6. Router Status fields (continued)

Field		Description
Wireless Port	Name (SSID)	The service set ID, also known as the wireless network name for WLAN.
	Region	The country where the unit is set up for use.
	Channel	The current channel, which determines the operating frequency.
	Wireless AP	Indicates if the access point feature is enabled for WLAN. If disabled, the WiFi LED on the front panel is off.
	Broadcast Name	Indicates if the wireless modem router is configured to broadcast its SSID for WLAN.

View Statistics

On the Router Status screen, click the **Show Statistics** button to display wireless modem router usage statistics.



System Up Time 03:52:30

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	PPPoA	1131	55	0	4	1	03:52:02
LAN	10M/100M	864	1869	0	29	13	03:52:25
WLAN	11M/54M/270M	411	0	0	7	0	03:52:21

ADSL Link	Downstream	Upstream
Connection Speed	8128 kbps	832 kbps
Line Attenuation	0.0 db	1.0 db
Noise Margin	19.7 db	6.0 db

Poll Interval : 10 (secs)

The Show Statistics screen displays the following statistics:

Table 7. Router Statistics fields

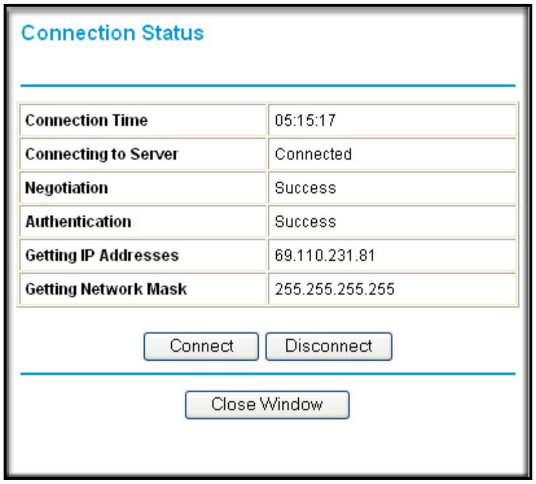
Field	Description
WAN, LAN, or WLAN	The statistics for the WAN (Internet), LAN (local), and wireless LAN (WLAN) ports. For each port, the screen displays the following:
Status	The link status of the port.
TxPkts	The number of packets transmitted on this port since reset or manual clear.
RxPkts	The number 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 line utilization—percentage of current bandwidth used on this port.

Table 7. Router Statistics fields (continued)

Field	Description
Rx B/s	The average line utilization for this port.
Up Time	The time elapsed since the last power cycle or reset.
ADSL Link Downstream or Upstream	The statistics for the upstream and downstream ADSL link. These statistics will be of interest to your technical support representative if you are having problems obtaining or maintaining a connection.
Connection Speed	Typically, the downstream speed is faster than the upstream speed.
Line Attenuation	The line attenuation increases the farther you are physically from your ISP's facilities.
WAN, LAN, or WLAN	The statistics for the WAN (Internet), LAN (local), and wireless LAN (WLAN) ports. For each port, the screen displays the following:
Status	The link status of the port.

View the Connection Status

On the Router Status screen, click the **Connection Status** button to display wireless modem router connection status.



Connection Status

Connection Time	05:15:17
Connecting to Server	Connected
Negotiation	Success
Authentication	Success
Getting IP Addresses	69.110.231.81
Getting Network Mask	255.255.255.255

This screen shows the following statistics:

Table 8. Connection Status fields (PPPoE network type example)

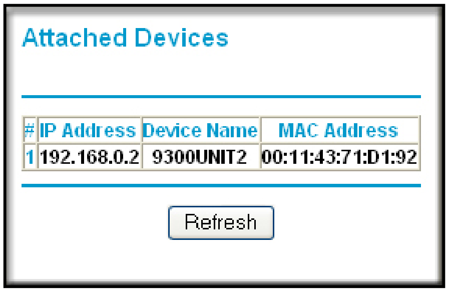
Field	Description
Connection Time	The time elapsed since the last connection to the Internet through the ADSL port.
Connecting to sender	The connection status.
Negotiation	Success or Failed.

Table 8. Connection Status fields (PPPoE network type example) (continued)

Field	Description
Authentication	Success or Failed.
Obtaining IP Address	The IP address assigned to the WAN port by the ADSL Internet service provider.
Obtaining Network Mask	The network mask assigned to the WAN port by the ADSL Internet service provider.

View Attached Devices

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



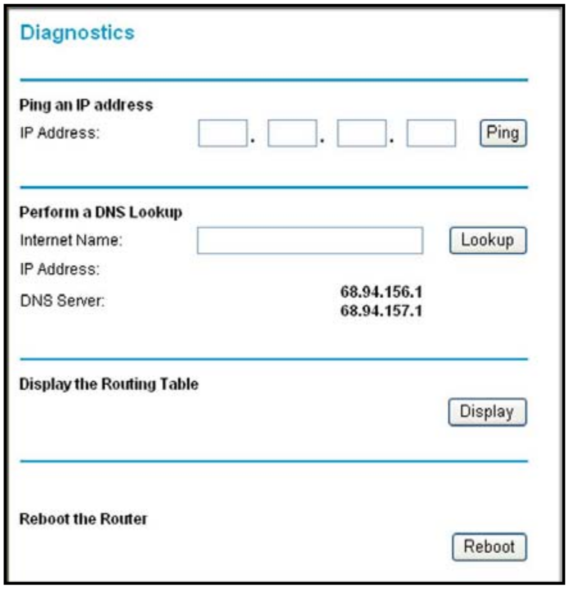
Attached Devices

#	IP Address	Device Name	MAC Address
1	192.168.0.2	9300UNIT2	00:11:43:71:D1:92

For each device, the table shows the IP address, device name if available, and the Ethernet MAC address. Note that if the wireless modem router is rebooted, the table data is lost until the wireless modem router rediscovers the devices. To force the wireless modem router to look for attached devices, click the **Refresh** button.

Run Diagnostics and Reboot

In the main menu, under Maintenance, select **Diagnostics**.



DNS Server: 68.94.156.1
68.94.157.1

The wireless modem router has a diagnostics feature. You can use the Diagnostics screen to perform the following functions from the wireless modem router:

- Ping an IP address to test connectivity to see if you can reach a remote host.
- Perform a DNS lookup to test if an Internet name resolves to an IP address to verify that the DNS server configuration is working.
- Display the Routing table to identify what other wireless modem routers the wireless modem router is communicating with.
- Reboot the wireless modem router to enable new network configurations to take effect or to clear problems with the wireless modem router’s network connection.

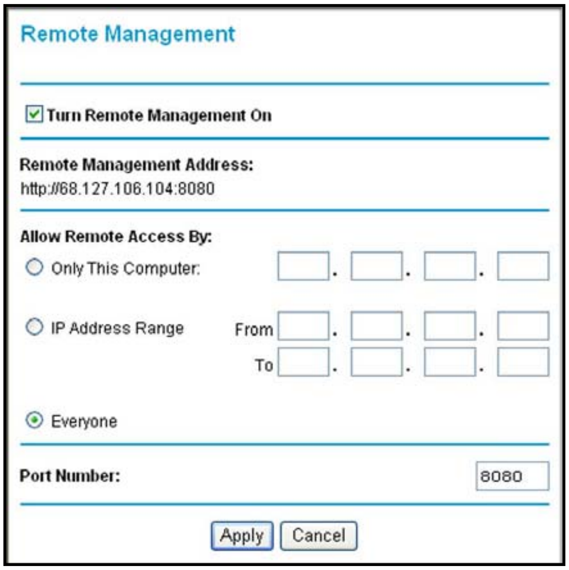
Configure Remote Management

Using the Remote Management screen, you can allow a user or users on the Internet to configure, upgrade, and check the status of your wireless modem router.

Note: Be sure to change the wireless modem router's default 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 remote management:**

1. Under Advanced in the main menu, select **Remote Management**.



Remote Management

☑ Turn Remote Management On

Remote Management Address:
http://68.127.106.104:8080

Allow Remote Access By:

○ Only This Computer: ___ . ___ . ___ . ___

○ IP Address Range From ___ . ___ . ___ . ___
To ___ . ___ . ___ . ___

● Everyone

Port Number: 8080

2. Select the **Turn Remote Management On** check box.
3. Specify the external addresses allowed to access the router remotely. For security, restrict access to as few as practical:
   - To allow access from any IP address on the Internet, select **Everyone**.
   - To allow access from a range of IP addresses, select **IP address Range**. Then 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.
4. Specify the port number that will be used for accessing the router menu.

   Web browser access usually uses the standard HTTP service port 80. For greater security, you can specify a custom port by entering that number in the field provided.

Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

5. Click **Apply** to have your changes take effect.

   To access the router from the Internet, type the router’s WAN IP address in the browser’s Address field, followed by a colon (:) and the port number. For example, if your external address is 134.177.0.123 and you use port 8080, enter the following in your browser:

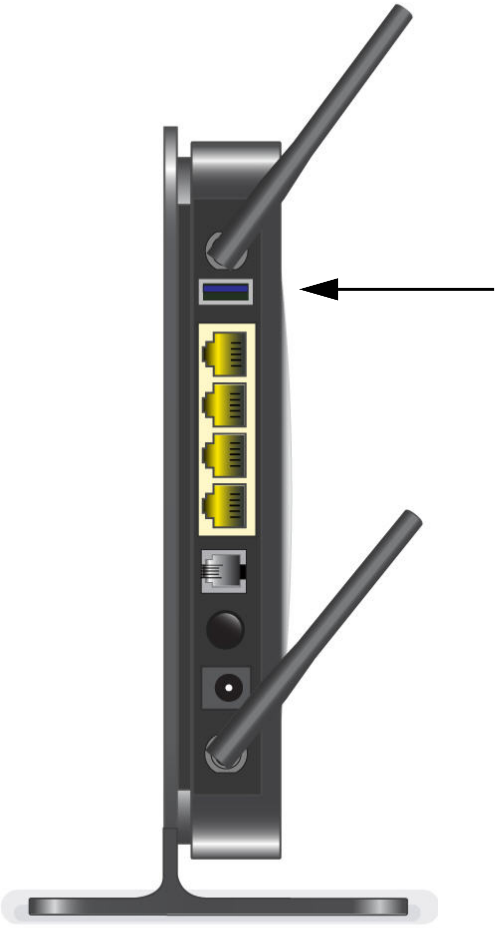
   http://134.177.0.123:8080

   In this case, the http:// needs to be included in the address.

5. USB Storage

5

This chapter describes how to access and configure a USB storage drive attached to your wireless modem router.



Note: The USB port on the wireless modem router can be used only to connect USB storage devices like flash drives or hard drives. Do not connect computers, USB modems, printers, CD drives, or DVD drives to the USB port.

Note: Because the USB port on the wireless modem router is used for connecting the broadband mobile modem cable, you are not able to use the USB port for both a ReadyShare storage and a broadband mobile Internet connection at the same time even when using a USB hub to fan out the USB port.

This chapter includes the following sections:

- *USB Drive Requirements*
- *File-Sharing Scenarios*
- *USB Storage Basic Settings*
- *Configure USB Storage Advanced Settings*
- *Unmount a USB Drive*
- *Specify Approved USB Devices*
- *Connect to the USB Drive from a Remote Computer*
- *Connect to the USB Drive with Microsoft Network Settings*

USB Drive Requirements

The wireless modem router works with 1.0 and 1.1 (USB full speed) and 2.0 (USB high speed) standards. The approximate USB bus speeds are shown in the following table.

Bus	Speed/Second
USB 1.1	12 Mbits
USB 2.0	480 Mbits

Actual bus speeds can vary, depending on the CPU speed, memory, speed of the network, and other variables. The wireless modem router should work with USB 2.0-compliant or 1.1-compliant external flash and hard drives. For the most up-to-date list of USB drives supported by the wireless modem router, go to *http://kb.netgear.com/app/answers/detail/a_id/12345*.

When selecting a USB device, bear in mind the following:

- The USB port on the wireless modem router can be used with one USB hard drive at a time. Do not attempt to use a USB hub attached to the USB port.
- According to the USB 2.0 specification, the maximum available power is 5V at 0.5A. Some USB devices might exceed this requirement, in which case the device might not function or might function erratically. Check the documentation for your USB device to be sure.
- The wireless modem router supports FAT, FAT32, NTFS (read-only), and Linux file systems.

File-Sharing Scenarios

You can share files on the USB drive for a wide variety of business and recreational purposes. The files can be any Windows, Mac, or Linux file type including text files, Word, PowerPoint, Excel, MP3, pictures, and multimedia. USB drive applications include:

- Sharing multimedia with friends and family. You can share MP3 files, pictures, and other multimedia with local and remote users.
- Sharing resources on your network. Store files in a central location so that you do not have to power up a computer to perform local sharing. In addition, you can share files between Macintosh, Linux, and Windows computers by using the USB drive as a go-between.
- Sharing files with offsite coworkers. Share files such as Word documents, PowerPoint presentations, and text files with remote users.

A few common uses are described in the following sections.

Share Photos with Friends and Family

You can create your own central storage location for photos and multimedia. This eliminates the need to log in to (and pay for) an external photo-sharing site.

➢ **To share files with your friends and family:**

1. Insert your USB drive into the USB port on the wireless modem router either directly or with a USB cable.

   Computers on your local area network (LAN) can access this USB drive using a web browser or Microsoft Networking.

2. If you want to specify read-only access, or to allow access from the Internet, see *Configure USB Storage Advanced Settings* on page 70.

Store Files in a Central Location for Printing

This scenario is for a family that has one high-quality color printer directly attached to a computer, but not shared on the local area network (LAN). This family does not have a print server:

- The family’s color printer is directly attached to the mother’s computer.
- The daughter has some photos on her Macintosh computer that she wants to print.
- Their computers are not visible to each other on the network.

➢ **To print her photos on the color printer:**

1. The daughter types **\\readyshare** in the address field of her web browser.

   This gives her access to the USB drive in the router.
2. She copies the photos from the Mac to the router USB drive.
3. The mother uses a her web browser or Microsoft Networking to transfer the files from the USB drive to her computer. Then she prints the files.

Share Large Files with Colleagues

Sending files larger than 5 MB can pose a problem for many email systems. The router allows you to share very large files such as PowerPoint presentations or .zip files with colleagues at another site. Rather than tying up their mail systems will large files, your colleagues can use FTP to easily download shared files from the wireless modem router.

➢ **To share files with a remote colleague:**

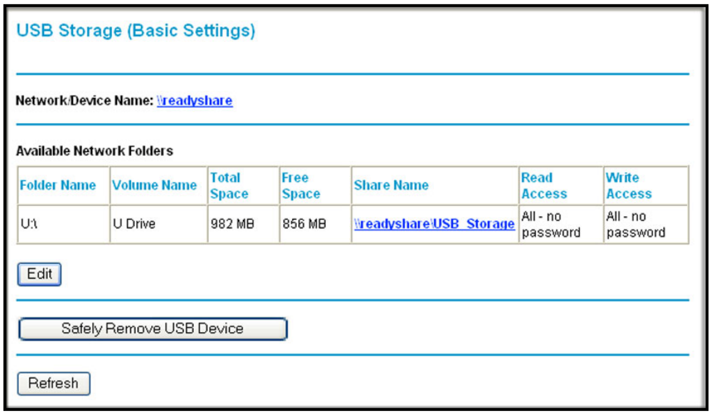
1. To protect your network, set up security. Create a user name and password for the colleague with appropriate access.
2. If you want to limit USB drive access to read-only access, from the wireless modem router USB Storage (Basic Settings) screen, click **Edit a Network folder**. In the Write Access field, select **admin**, and then click **Apply**.

   Note: The password for admin is the same one that you use to access the wireless modem router. By default it is **password**.

3. Enable FTP via Internet in the USB Storage (Advanced Settings) screen. See *Configure USB Storage Advanced Settings* on page 70.

USB Storage Basic Settings

You can view or edit basic settings for the USB storage device attached to your wireless modem router. On the wireless modem router main menu under USB, select **Basic Settings**. The following screen displays:



USB Storage (Basic Settings)

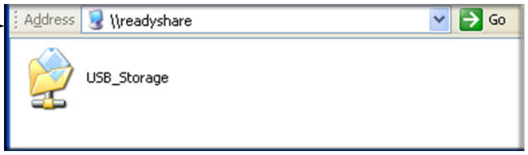
Network/Device Name: \\readyshare

Available Network Folders

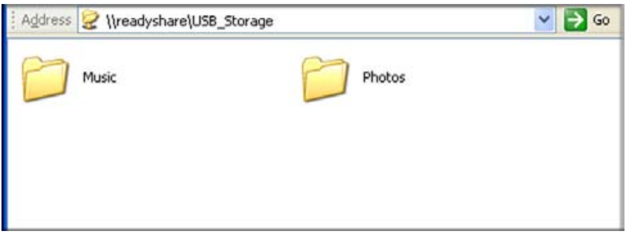
Folder Name	Volume Name	Total Space	Free Space	Share Name	Read Access	Write Access
U:\	U Drive	982 MB	856 MB	\\readyshare\USB_Storage	All - no password	All - no password

By default, the USB storage device is available to all computers on your local area network (LAN). To access your USB device from this screen, you can click the network or device name or the share name.

Network or device name: **\\readyshare**



Share name: **\\readyshare\USB_Storage**



You can also type **\\readyshare** in the address field of your web browser. If you logged in to the wireless modem router before you connected your USB device, you might not see your USB device in the wireless modem router screens until you log out and then log in again.

Table 9. USB Storage (Basic Settings)

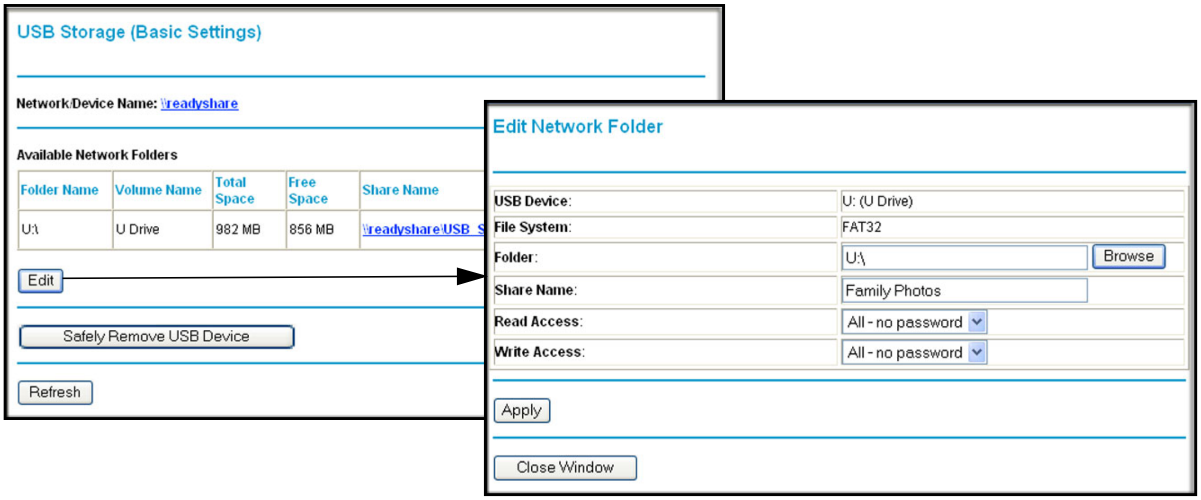
Fields and buttons	Description
Network Device Name	The default is \\readyshare. This is the name used to access the USB device connected to the wireless modem router.

Table 9. USB Storage (Basic Settings) (continued)

Fields and buttons		Description
Available Network Folders	Folder Name	Full path of the used by the network folder.
	Volume name	Volume name from the storage device (either USB drive or HDD).
	Total/Free Space	Shows the current utilization of the storage device.
	Share Name	• You can click the name shown, or you can type it in the address field of your web browser. • If Not Shared is shown, then the default share has been deleted, and no other share for the root folder exists. Click the link to change this setting.
	Read and Write Access	Shows the network folder permissions and access controls. • **All-no password** allows all users to access the network folder. • **admin** uses the same password that you use to log in to the wireless modem router main menu.
Edit button		You can click the **Edit** button to edit the Available Network Folders settings. See *Edit a Network Folder* on page 69.
Safely Remove USB Device button		Click to safely remove the USB device attached to your wireless modem router. See *Unmount a USB Drive* on page 72.

Edit a Network Folder

This process is the same from either the USB Storage (Basic Settings) screen or the USB Storage (Advanced Settings) screen. Click the **Edit** button to open the Edit Network Folder screen:



USB Storage (Basic Settings)

Network/Device Name: \\readyshare

Available Network Folders

Folder Name	Volume Name	Total Space	Free Space	Share Name
U:\	U Drive	982 MB	856 MB	\\readyshare\USB_S

Edit Network Folder

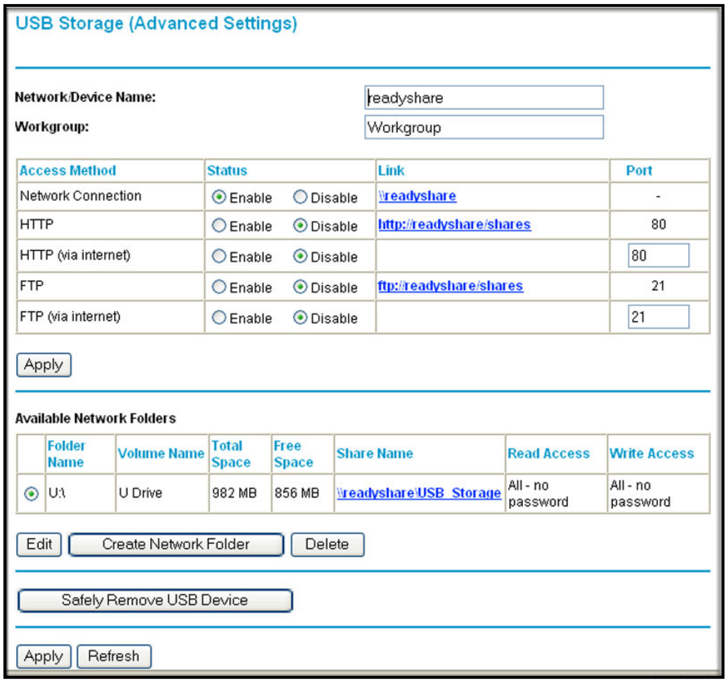
USB Device:	U: (U Drive)
File System:	FAT32
Folder:	U:\
Share Name:	Family Photos
Read Access:	All - no password
Write Access:	All - no password

You can use this screen to select a folder, to change the share name, or to change read access or write access from All-no password to admin. The password for admin is the same one that is used to log in to the router main menu. By default it is **password**.

Note: You need to click **Apply** for your changes to take effect.

Configure USB Storage Advanced Settings

To configure advanced USB settings, from the router menu, under USB, select **Advanced Settings**. The USB Storage (Advanced Settings) screen displays:



USB Storage (Advanced Settings)

Network/Device Name: readyshare

Workgroup: Workgroup

Access Method	Status	Link	Port
Network Connection	● Enable ○ Disable	\\readyshare	-
HTTP	○ Enable ● Disable	http://readyshare/shares	80
HTTP (via internet)	○ Enable ● Disable		80
FTP	○ Enable ● Disable	ftp://readyshare/shares	21
FTP (via internet)	○ Enable ● Disable		21

Available Network Folders

	Folder Name	Volume Name	Total Space	Free Space	Share Name	Read Access	Write Access
●	U:\	U Drive	982 MB	856 MB	\\readyshare\USB_Storage	All - no password	All - no password

You can use this screen to specify access to the USB storage device. The following table explains the fields and buttons in the USB Storage (Advanced Settings) screen.

Table 10. USB Storage (Advanced Settings)

Fields	Description
Network Device Name	The default is readyshare. This is the name used to access the USB device connected to the wireless modem router from your computer.
Workgroup	If you are using a Windows workgroup rather than a domain, the workgroup name is displayed here.

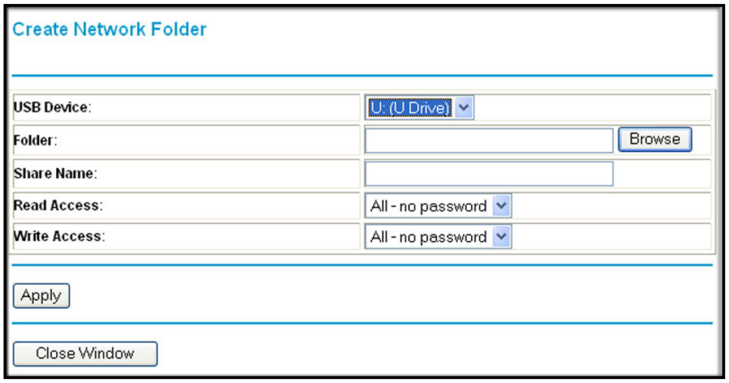
Table 10. USB Storage (Advanced Settings) (continued)

Fields		Description
Access Method	Network Connection	Enabled by default, this allows all users on the LAN to have access to the USB drive.
	HTTP	Disabled by default. If you enable this setting, you can type **http://readyshare** to access the USB drive.
	HTTP (via Internet)	Disabled by default. If you enable this setting, remote users can type **http://readyshare** to access the USB drive over the Internet.
	FTP	Disabled by default.
	FTP (via Internet)	Disabled by default. If you enable this setting, remote users can access the USB drive through FTP over the Internet.
Available Network Folders	Folder Name	Full path of the used by the network folder.
	Volume name	Volume name from the storage device (either USB drive or HDD).
	Total/Free Space	The current utilization of the storage device.
	Share Name	• You can click the name shown, or you can type it into the address field of your web browser. • If Not Shared is shown, then the default share has been deleted, and no other share for the root folder exists. Click the link to change this setting.
	Read and Write Access	Shows the permissions and access controls on the network folder. • **All-no password** allows all users to access the network folder. • **admin** prompts you to enter the same password that you use to log in to the wireless modem router main menu.

Create a Network Folder

➢ To create a network folder:

1. From the USB Storage (Advanced Settings) screen, click the **Create a Network Folder** button to open the Create a Network Folder screen:



Create Network Folder

USB Device:	U: (U Drive)
Folder:	
Share Name:	
Read Access:	All - no password
Write Access:	All - no password

2. Create a folder.
   - You can specify the folder’s share name read access and write access from All-no password to admin.
   - The password for admin is the same one that is used to log in to the wireless modem router main menu. By default it is **password**.
3. Click **Apply** so that your changes take effect.

Unmount a USB Drive

WARNING:

Unmount the USB drive first before physically unplugging it from the wireless modem router. If the USB disk is removed or a cable is pulled while data is being written to the disk, it could result in file or disk corruption.

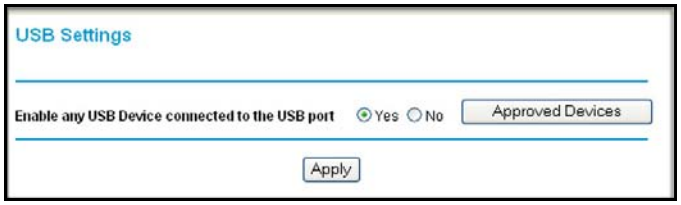
To unmount a USB disk drive so that no users can access it, from the USB Settings screen, click the **Safely Remove USB** button. This takes the drive offline.

Specify Approved USB Devices

You can specify which USB devices are approved for use when connected to the router.

➢ **To specify approved USB devices:**

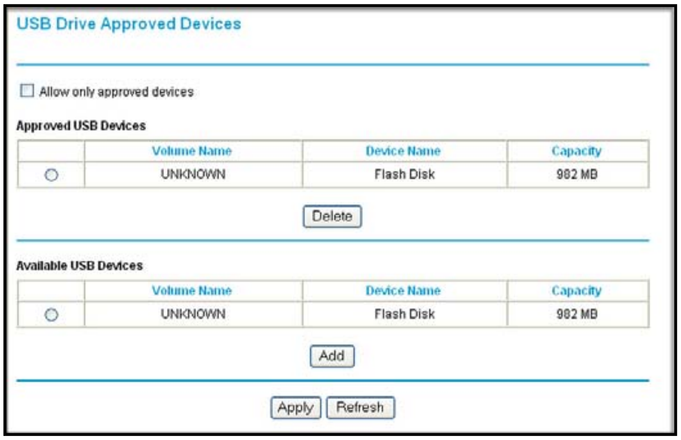
1. On the router main menu, under Advanced, select **USB Settings**.



USB Settings

Enable any USB Device connected to the USB port ● Yes ○ No

2. Click **Approved Devices**.



USB Drive Approved Devices

□ Allow only approved devices

Approved USB Devices

	Volume Name	Device Name	Capacity
○	UNKNOWN	Flash Disk	982 MB

Available USB Devices

	Volume Name	Device Name	Capacity
○	UNKNOWN	Flash Disk	982 MB

3. On the USB Drive Approved Devices screen, select the USB device from the Available USB Devices list.
4. Click **Add**.
5. Select the **Allow only approved devices** check box.
6. Click **Apply** so that your change takes effect.

If you want to approve another USB device, you need to first click the **Safely Remove USB Device** button to unmount the currently connected USB device. Connect the other USB device, and then repeat this process.

Connect to the USB Drive from a Remote Computer

To connect to the USB drive from remote computers using a web browser, you need to use the router’s Internet port IP address.

Locate the Internet Port IP Address

➢ **To view the Internet port IP address:**

1. Log in to the wireless modem router.
2. In the main menu, under Maintenance, select **Router Status**.
3. Record the IP address that is listed for the Internet port. This is the IP address you can use to connect to the router remotely.

Access the Router’s USB Drive Remotely Using FTP

➢ **To connect to the router’s USB drive using a web browser:**

1. Connect to the router by typing **ftp://** and the Internet port IP address in the address field of Internet Explorer or Netscape Navigator, for example, **ftp://10.1.65.4**. If you are using Dynamic DNS, you can type the DNS name rather than the IP address.
2. Type the account name and password that provide access rights to the USB drive.

3. The directories of the USB drive that your account has access to display, for example, share/partition1/directory1. You can now read and copy files from the USB directory.

Connect to the USB Drive with Microsoft Network Settings

You can access the USB drive from local computers on your home or office network using Microsoft network settings. You need to be running Microsoft Windows 2000, XP, or older versions of Windows with Microsoft Networking enabled. You can use normal Explorer operations such as dragging and dropping, opening files, or cutting and pasting files from:

- Microsoft Windows Start menu, Run option
- Windows Explorer
- Network Neighborhood or My Network Place

Enable File and Printer Sharing

Each computer’s network properties need to be set to enable network communication with the USB drive. File and Printer Sharing for Microsoft Networking needs to be enabled, as described in the following sections.

Note: In Windows 2000 and Windows XP, File and Printer Sharing is enabled by default.

Configure Windows 98SE and Windows ME

The easiest way to get to your network properties is to go to your desktop, right-click **Network Neighborhood**, and then select **Properties**. File and Printer Sharing for Microsoft Windows should be listed. If it is not, click **Add**, and follow the installation prompts.

Note: If you have any questions about File and Printer Sharing, contact Microsoft for assistance.

Configure Windows 2000 and Windows XP

Right-click the network connection for your local area network. File and Printer Sharing for Microsoft Windows should be listed. If it is not, click **Install**, and follow the installation prompts.

Advanced Configuration

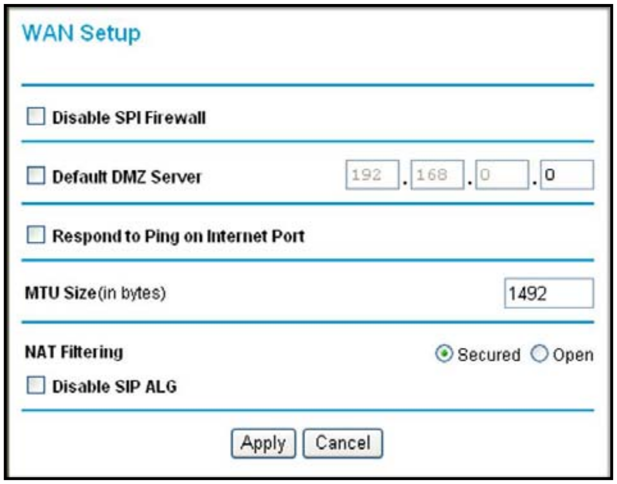
6

This chapter describes how to configure the advanced features of your wireless modem router. For information about remote management, see *Configure Remote Management* on page 62. The following features are discussed in this chapter:

- *Configure WAN Settings*
- *Configure Dynamic DNS*
- *Configure LAN Settings*
- *Set Up Quality of Service (QoS)*
- *Advanced Wireless Settings*
- *Use Static Routes*
- *Configure Universal Plug and Play*
- *Build Wireless Bridging and Repeating Networks*
- *Port Forwarding and Port Triggering*
- *Advanced USB Settings*
- *Traffic Meter*

Configure WAN Settings

In the main menu, under Advanced, select **WAN Setup** to display the following screen.



WAN Setup

□ Disable SPI Firewall

□ Default DMZ Server 192 . 168 . 0 . 0

□ Respond to Ping on Internet Port

MTU Size(in bytes) 1492

NAT Filtering ● Secured ○ Open

□ Disable SIP ALG

Table 11. WAN settings

Setting	Description
Disable SPI Firewall	The SPI (stateful packet inspection) firewall protects your LAN against denial of service attacks. This should be disabled only in special circumstances.
Default DMZ Server	See *Set Up a Default DMZ Server* on page 77.
Respond to a Ping on an Internet WAN Port	If you want the wireless modem 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 wireless modem router to be discovered. Do not select this check box unless you have a specific reason to do so.
MTU Size	The normal MTU (maximum transmit unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs you might need to reduce the MTU. But this is rarely required and should not be done unless you are sure it is necessary for your ISP connection.
NAT Filtering	This option determines how the router deals with inbound traffic. The Secured option provides a secured firewall to protect the computers on LAN from attacks from the Internet, but it might cause some Internet games, point-to-point applications, or multimedia applications not to work. The Open option, on the other hand, provides a much less secured firewall, while it allows almost all Internet applications to work.
Disabling the SIP ALG	The Session Initiation Protocol (SIP) Application Level Gateway (ALG) is enabled by default to optimize VoIP phone calls that use the SIP. The **Disable SIP ALG** check box allows you to disable the SIP ALG. Disabling the SIP ALG might be useful when running certain applications.

Set Up a Default DMZ Server

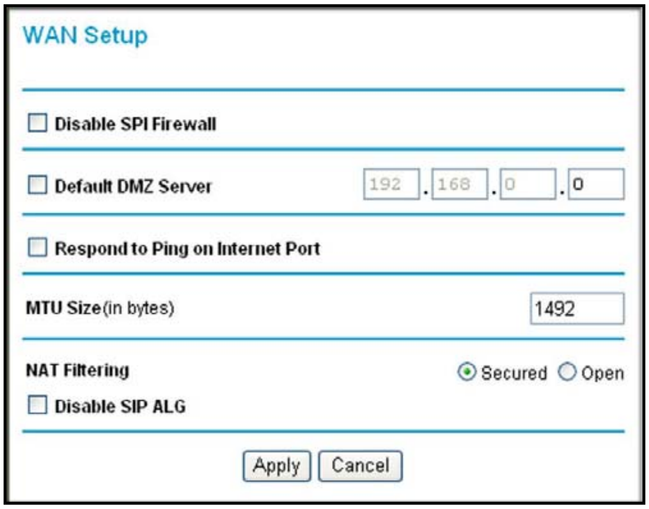
The default demilitarized zone (DMZ) server feature is helpful when you use some online games and videoconferencing applications that are incompatible with NAT. The wireless modem router is programmed to recognize some of these applications and to work correctly with them, but there are other applications 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.

> ***Note:*** For security reasons, you should avoid using the default DMZ server feature. When a computer is designated as the default DMZ server, it loses much of the protection of the firewall, and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

Incoming traffic from the Internet is usually discarded by the wireless modem 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.

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

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



WAN Setup

□ Disable SPI Firewall

□ Default DMZ Server 192 . 168 . 0 . 0

□ Respond to Ping on Internet Port

MTU Size(in bytes) 1492

NAT Filtering ● Secured ○ Open

□ Disable SIP ALG

2. Select the **Default DMZ Server** check box.
3. Type the IP address for that server.
4. Click **Apply** to save your changes.

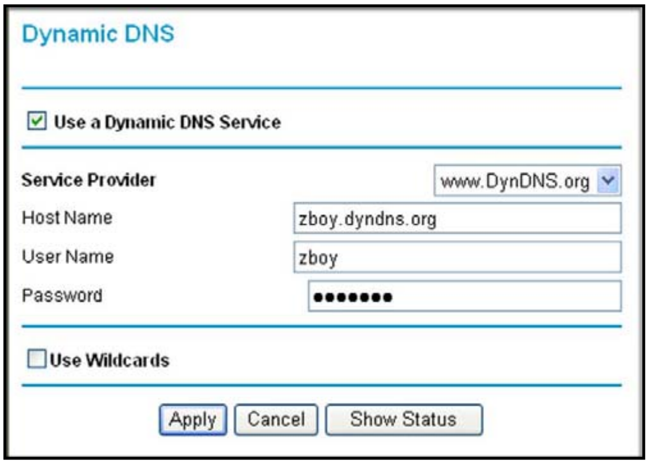
Configure Dynamic DNS

If your network has 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 will 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 that will allow you to register your domain to their IP address and will forward traffic directed at your domain to your frequently changing IP address.

The router contains a client that can connect to a Dynamic DNS service provider. To use this feature, you need to select a service provider and obtain an account with them. After you have configured your account information in the router, whenever your ISP-assigned IP address changes, your router automatically contacts your Dynamic DNS service provider, logs in to your account, and registers your new IP address.

➢ **To configure Dynamic DNS:**

1. In the main menu, under Advanced, select **Dynamic DNS**.



Dynamic DNS

☑ Use a Dynamic DNS Service

Service Provider: www.DynDNS.org
Host Name: zboy.dyndns.org
User Name: zboy
Password: •••••••

□ Use Wildcards

2. Access the website of one of the Dynamic DNS service providers whose names appear in the Service Provider drop-down list, and register for an account. For example, for dyndns.org, go to www.dyndns.org.
3. Select the **Use a Dynamic DNS Service** check box.
4. Select the name of your Dynamic DNS service provider.
5. Type the host name that your Dynamic DNS service provider gave you. The Dynamic DNS service provider might call this the domain name. If your URL is myName.dyndns.org, then your host name is myName.
6. Type the user name for your Dynamic DNS account.
7. Type the password (or key) for your Dynamic DNS account.
8. 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.

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

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.

Configure LAN Settings

The LAN Setup screen allows configuration of LAN IP services such as DHCP.

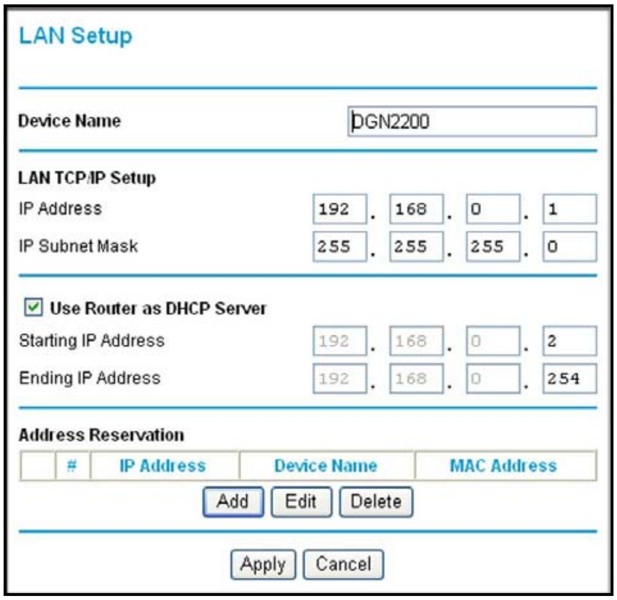
Note: If you change the LAN IP address of the wireless modem router while connected through the browser, you will be disconnected. You need to then open a new connection to the new IP address and log in again.

The wireless modem router is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server. The wireless modem router's default LAN IP configuration is as follows:

- **LAN IP address**. 192.168.0.1
- **Subnet mask**. 255.255.255.0

These addresses are part of the Internet Engineering Task Force (IETF)–designated private address range for use in private networks and should be suitable in most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes by opening the LAN Setup screen.

Under Advanced in the main menu, select **LAN Setup**.



LAN Setup

Device Name: DGN2200

LAN TCP/IP Setup

IP Address: 192 . 168 . 0 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

☑ Use Router as DHCP Server

Starting IP Address: 192 . 168 . 0 . 2

Ending IP Address: 192 . 168 . 0 . 254

Address Reservation

	#	IP Address	Device Name	MAC Address

Table 12. LAN Setup

Setting	Description
Device Name	This is a user-friendly name of the router. You can see this name for the router in Network Explorer on Windows systems.
IP Address	This is the LAN IP address of the wireless modem router.
IP Subnet Mask	This is the LAN subnet mask of the wireless modem router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which need to be reached through a gateway or wireless modem router.
Use Router as DHCP Server	See the following section, *Configure DHCP*.
Address Reservation	See *Configure Reserved IP Addresses* on page 81.

Configure DHCP

By default, the wireless modem router functions as a Dynamic Host Configuration Protocol (DHCP) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the wireless modem router’s LAN. The assigned default gateway address is the LAN address of the router. IP addresses are assigned 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.

Use Router as DHCP Server

If another device on your network will be the DHCP server, or if you will manually configure the network settings of all of your computers, clear the **Use Router as DHCP Server** check box. Otherwise, leave it selected.

Specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the router's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.0.2 and 192.168.0.254, although you might want to save part of the range for devices with fixed addresses.

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

- An IP address from the range you have defined
- Subnet mask
- Gateway IP address, which is 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
- WINS server, short for Windows Internet Naming Service Server, determines the IP address associated with a particular Windows computer. A WINS server records and reports a list of names and IP addresses of Windows computers on its local network. If you connect to a remote network that contains a WINS server, enter the server's IP address here. This allows your computers to browse the network using the Network Neighborhood feature of Windows.

Configure Reserved IP Addresses

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

➢ **To reserve an IP address:**

1. In the LAN Setup screen, click the **Add** button.
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 192.168.0.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 will not be 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. Select the radio button next to the reserved address that you want to edit or delete.
2. Click **Edit** or **Delete**.

Set Up Quality of Service (QoS)

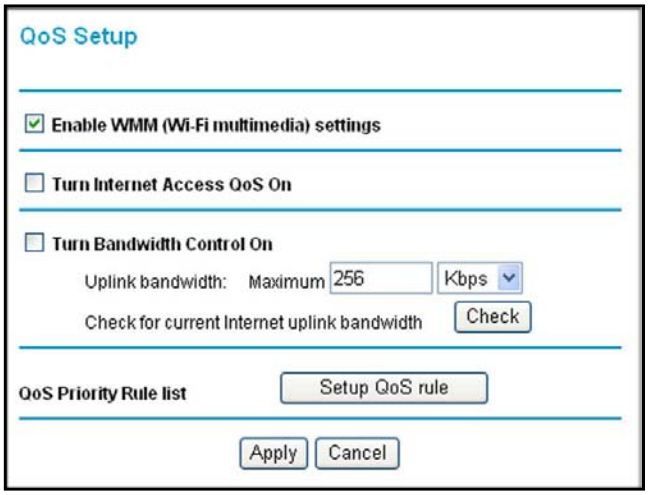
Quality of Service (QoS) is an advanced feature that can be used to prioritize some types of traffic ahead of others. The modem router can provide QoS prioritization over the wireless link and on the Internet connection.

The modem router supports WiFi 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 need to 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.

Configure QoS for Internet Access

➢ **To add or create a policy to prioritize traffic:**

1. From the main menu, under Advanced, select **QoS Setup**.



QoS Setup

☑ Enable WMM (Wi-Fi multimedia) settings

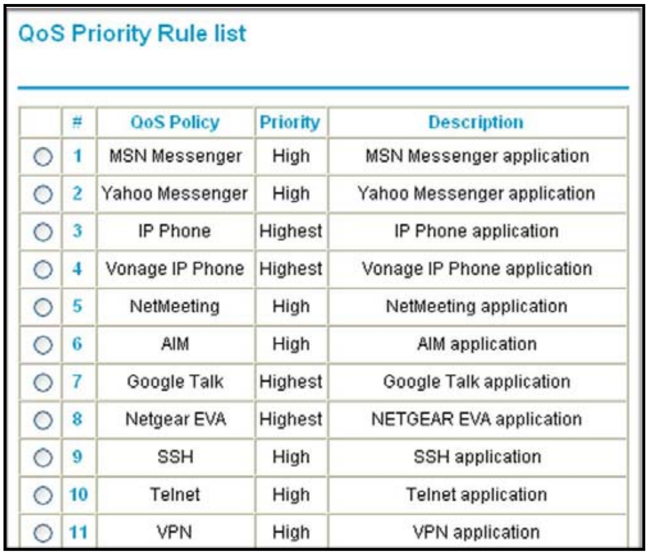
☐ Turn Internet Access QoS On

☐ Turn Bandwidth Control On

Uplink bandwidth: Maximum 256 Kbps

Check for current Internet uplink bandwidth

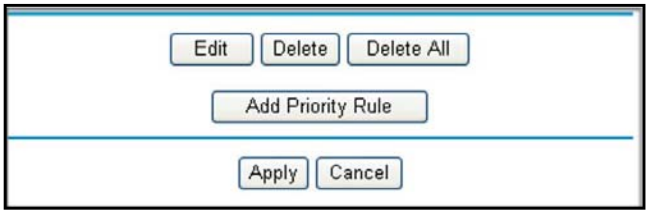
2. Click **Setup QoS rule**. The QoS Priority Rule list displays:



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	Telnet	High	Telnet application
○	11	VPN	High	VPN application

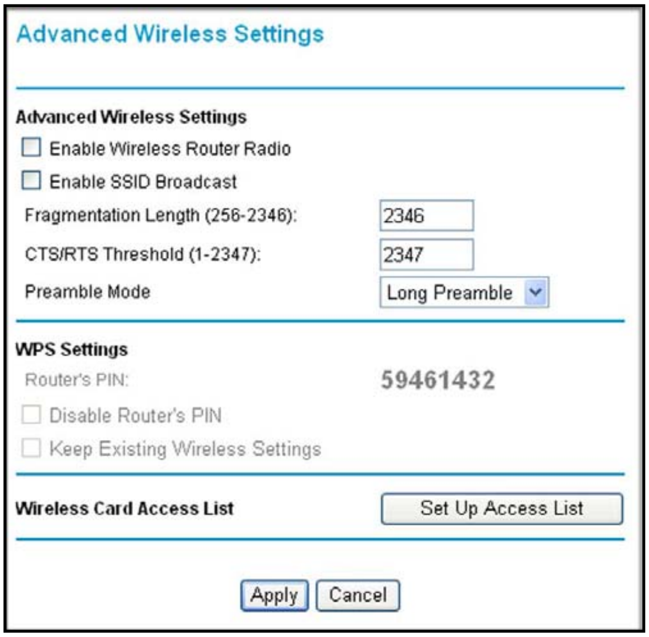
3. To change a rule, select its radio button, and scroll down to the bottom of the screen:



4. To edit a rule, click **Edit**. To add a custom rule, click **Add Priority Rule**, and enter the requested information on the screen that displays.
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, click **Apply**.

Advanced Wireless Settings

From the main menu, under the Advanced heading, select **Wireless Settings**:



Advanced Wireless Settings

Advanced Wireless Settings

☐ Enable Wireless Router Radio

☐ Enable SSID Broadcast

Fragmentation Length (256-2346): 2346

CTS/RTS Threshold (1-2347): 2347

Preamble Mode: Long Preamble

WPS Settings

Router's PIN: 59461432

☐ Disable Router's PIN

☐ Keep Existing Wireless Settings

Wireless Card Access List

Restrict Wireless Access to Your Network

By default, any wireless computer that is configured with the correct SSID can access your wireless network. For increased security, the wireless 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.

Turn Off Wireless Connectivity Completely

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

Hide Your Wireless Network Name (SSID)

By default, the wireless 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 wireless modem router. You need to configure your wireless devices to match the SSID of the wireless modem router.

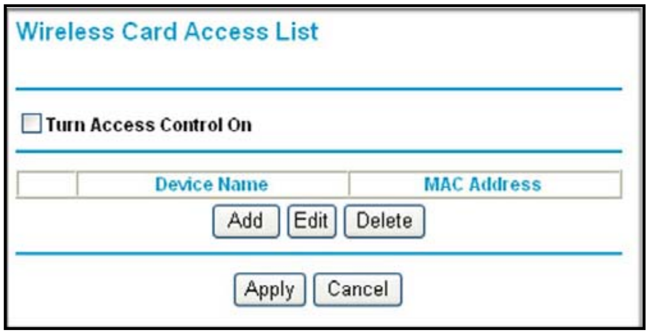
> ***Note:*** The SSID of any wireless access adapters need to match the SSID you specify in the wireless modem router. If the SSIDs do not match, you will not get a wireless connection to the wireless modem router.

Restrict Access by MAC Address

For increased security, you can restrict access to the wireless network to allow only specific computers based on their MAC addresses. You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the wireless modem 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 Card Access List determines which wireless hardware devices will be allowed to connect to the wireless modem router.

➢ **To restrict access based on MAC addresses:**

1. In the Wireless Settings screen, click the **Set Up Access List** button to display the list.



Wireless Card Access List

☐ Turn Access Control On

	Device Name	MAC Address

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

> ***Note:*** If you are using a wireless connection, do not click **Apply** until you have added your computer’s MAC address in this screen.

3. Click the **Add** button to add wireless stations so that they will have access.
   - You can select currently connected wireless computers from the Available Wireless Cards List.

- You can type in the MAC address for the wireless computer or device. The MAC address is usually printed on the wireless card, or on the label of a wireless device. It might appear in the wireless modem router’s DHCP table. The MAC address is 12 hexadecimal digits.
- You can copy and paste the MAC addresses from the wireless 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 wireless modem router. The computer should then appear in the Attached Devices screen.

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

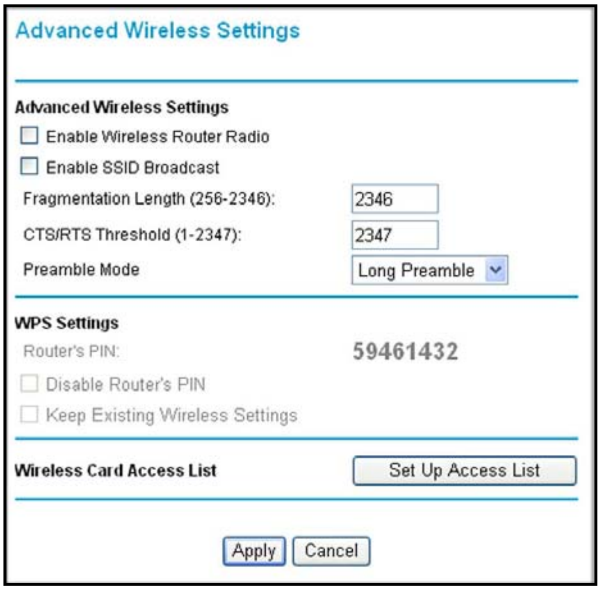
Now, only computers and devices on this list can wirelessly connect to the wireless modem router. This prevents unauthorized access to your network.

Configure WPS Settings

The advanced WPS settings cannot be displayed if you have selected WEP as the security option.

➢ **To display and specify advanced WPS settings:**

1. Log in to the wireless modem router as described in *Log In to Your Wireless-N Modem Router* on page 17.
2. In the main menu, under Advanced, select **Wireless Settings** to display the Advanced Wireless Settings screen:



Advanced Wireless Settings

Advanced Wireless Settings

□ Enable Wireless Router Radio

□ Enable SSID Broadcast

Fragmentation Length (256-2346): 2346

CTS/RTS Threshold (1-2347): 2347

Preamble Mode: Long Preamble

WPS Settings

Router's PIN: 59461432

□ Disable Router's PIN

□ Keep Existing Wireless Settings

Wireless Card Access List

By default the Enable WPS check box is selected. If you clear this check box and click **Apply**, you will not be able to use WPS.

3. Under WPS Settings, you can configure the following settings:

- **Disable Router’s PIN**. Only when the wireless modem router’s PIN is enabled can you configure the wireless modem router’s wireless settings or add a wireless client through WPS with the wireless modem router’s PIN number. If the wireless modem router detects suspicious attempts to access the network with a PIN, the PIN function might be disabled temporarily. You can manually enable the PIN function by clearing the **Disable Router’s PIN** check box.
- **Keep Existing Wireless Settings**. By default, the Keep Existing Wireless Settings check box is cleared. This allows the modem router to automatically generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the modem router automatically selects this check box so that your SSID and wireless security settings remain the same if other WPS-enabled devices are added later.

If you configure your wireless router settings and security manually, the Keep Existing Wireless Settings check box will also be selected. This allows you to use WPS (Push 'N' Connect) to connect additional WPS-capable devices to your wireless network using the existing settings.

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

Use Static Routes

Static routes provide additional routing information to your router. Under normal 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 need to configure static routes only for unusual cases such as multiple routers or multiple IP subnets located on your network.

Static Route Example

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 192.168.0.100.
- 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 to the wireless modem router, and a second static route was created to your local network for all 192.168.0.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 need to define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100.

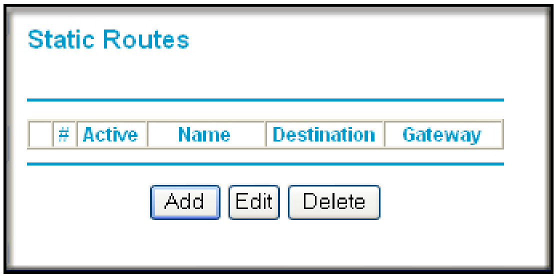
In this example:

- 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 192.168.0.100.
- The value in the Metric field represents the number of routers between your network and the destination. This is a direct connection, so it can be set to the minimum value of 2.
- The Private check box is selected only as a precautionary security measure in case RIP is activated.

Configure Static Routes

➢ **To add a static route:**

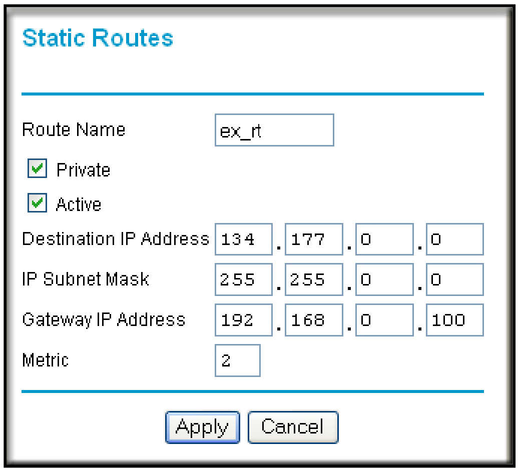
1. In the main menu, under Advanced, select **Static Routes**.



Static Routes

	#	Active	Name	Destination	Gateway

2. Click **Add** to open the Static Routes screen.



Static Routes

Route Name: ex_rt

☑ Private

☑ Active

Destination IP Address: 134 . 177 . 0 . 0

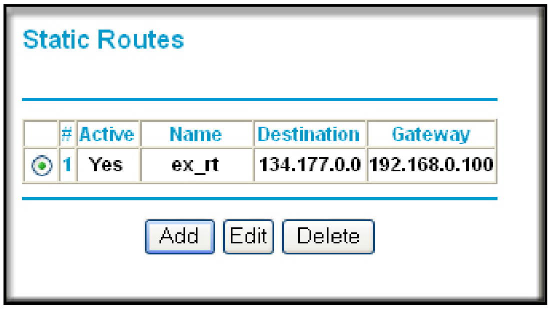
IP Subnet Mask: 255 . 255 . 0 . 0

Gateway IP Address: 192 . 168 . 0 . 100

Metric: 2

3. Enter a route name for this static route in the Route Name field. This name is for identification purpose only.
4. Select **Private** if you want to limit access to the LAN only. The static route will not be reported in RIP.
5. Select **Active** to make this route effective.
6. Enter the IP address of the final destination.

7. Enter the IP subnet mask for this destination. If the destination is a single host, type **255.255.255.255**.
8. Enter the gateway IP address, which needs to be a router on the same LAN segment as the router.
9. Enter a number between 2 and 15 in the Metric field. This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works.
10. Click **Apply**. The Static Routes table is updated to show the new entry.



Static Routes

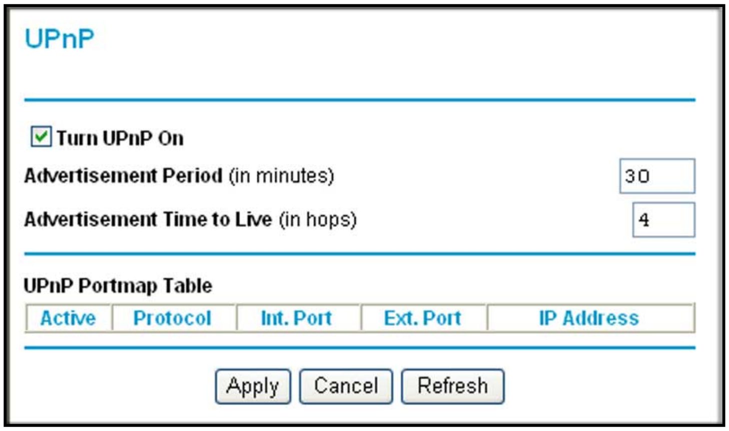
	#	Active	Name	Destination	Gateway
◉	1	Yes	ex_rt	134.177.0.0	192.168.0.100

Configure Universal Plug and Play

Universal Plug and Play (UPnP) helps devices such as Internet appliances and computers 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.

➢ **To configure Universal Plug and Play:**

1. On the main menu, select **UPnP**:



UPnP

☑ Turn UPnP On

Advertisement Period (in minutes) 30

Advertisement Time to Live (in hops) 4

UPnP Portmap Table

Active	Protocol	Int. Port	Ext. Port	IP Address

2. Fill in the settings on the UPnP screen:
   - **Turn UPnP On**. UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If UPnP is disabled, the wireless modem router does not allow any device to automatically control the resources, such as port forwarding (mapping), of the wireless modem router.
   - **Advertisement Period**. The advertisement period is how often the wireless modem router advertises (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. Hops are the steps 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 a little.
- **UPnP Portmap Table**. The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the wireless modem router and which ports (internal and external) that device has opened. The UPnP Portmap Table also displays what type of port is opened and if that port is still active for each IP address.

3. Save, cancel your changes, or refresh the table:
   - Click **Apply** to save the new settings to the wireless modem router.
   - Click **Cancel** to disregard any unsaved changes.
   - Click **Refresh** to update the portmap table and to show the active ports that are currently opened by UPnP devices.

Build Wireless Bridging and Repeating Networks

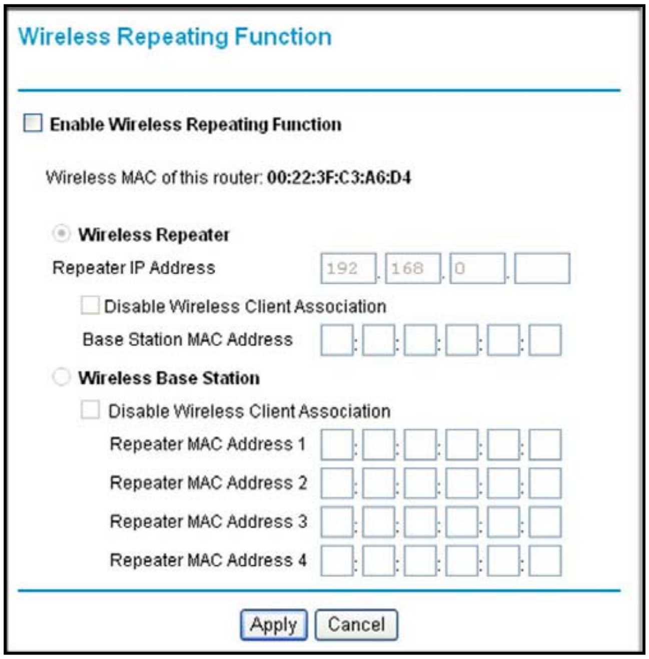
With the DGN2200M Mobile Edition wireless modem router, you can build large bridged wireless networks that form an IEEE 802.11n Wireless Distribution System (WDS). Using the modem router with other access points (APs) and wireless devices, you can connect clients by using their MAC addresses rather than by specifying IP addresses.

Here are some examples of wireless bridged configurations:

- **Point-to-point bridge**. The wireless modem router communicates with another bridge-mode wireless station. See *Point-to-Point Bridge Configuration* on page 92.
- **Multi-point bridge**. The wireless modem router is the “master” for a group of bridge-mode wireless stations. Then all traffic is sent to this master, rather than to other access points. See *Multi-Point Bridge* on page 93.
- **Repeater with wireless client association**. Sends all traffic to the remote access point. See *Repeater with Wireless Client Association* on page 94.

Note: The wireless bridging and repeating feature uses the default security profile to send and receive traffic.

To view or change these configurations, from the main menu, select **Wireless Repeating Function**:



Wireless Repeating Function

□ Enable Wireless Repeating Function

Wireless MAC of this router: **00:22:3F:C3:A6:D4**

● **Wireless Repeater**

Repeater IP Address 192 . 168 . 0 .

□ Disable Wireless Client Association

Base Station MAC Address : : : : :

○ **Wireless Base Station**

□ Disable Wireless Client Association

Repeater MAC Address 1 : : : : :

Repeater MAC Address 2 : : : : :

Repeater MAC Address 3 : : : : :

Repeater MAC Address 4 : : : : :

Point-to-Point Bridge Configuration

In point-to-point bridge mode, the wireless modem router communicates as an access point with another bridge-mode wireless station. When used as a bridge, wireless client associations are disabled—only wired clients can be connected. You need to enter the MAC address of the other bridge-mode wireless station in the field provided. Use wireless security to protect this communication. The following figure shows an example of point-to-point bridge mode.

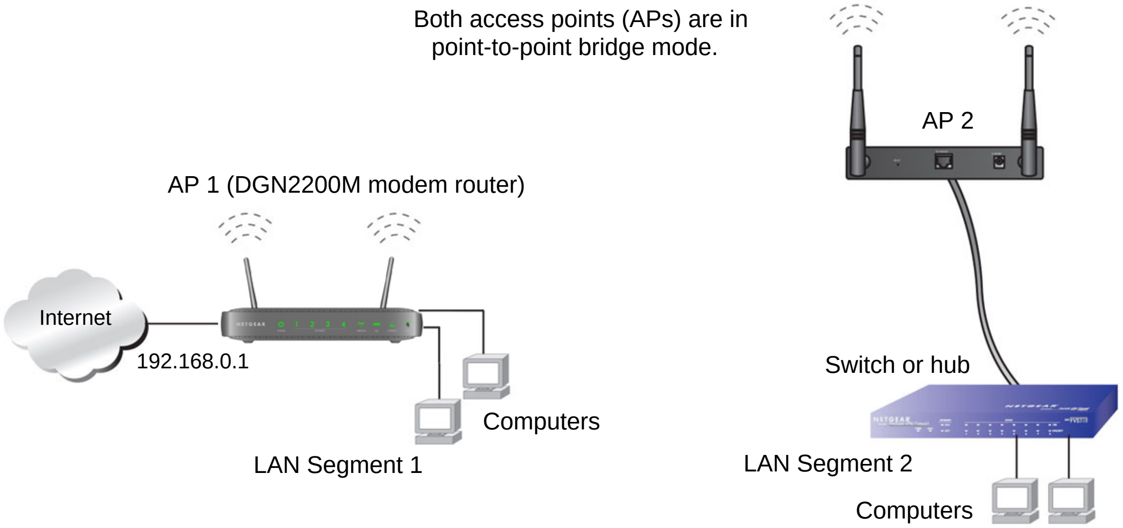

Both access points (APs) are in point-to-point bridge mode.
AP 2
AP 1 (DGN2200M modem router)
Internet
192.168.0.1
Computers
LAN Segment 1
Switch or hub
LAN Segment 2
Computers

Figure 1. Point-to-point bridge mode

- **To set up a point-to-point bridge configuration:**

1. Configure the DGN2200M Mobile Edition wireless modem router (AP 1) on LAN Segment 1 in point-to-point bridge mode.
2. Configure the other access point (AP 2) on LAN Segment 2 in point-to-point bridge mode.

   The DGN2200M Mobile Edition wireless modem router needs to have AP 2’s MAC address in its Remote MAC Address field, and AP 2 needs to have the DGN2200M Mobile Edition’s MAC address in its Remote MAC Address field.
3. Configure both APs, and verify that both APs are using the same SSID, channel, authentication mode, if any, and security settings if security is in use.
4. Disable the DHCP server on AP 2. AP 1 will then be the DHCP server.
5. Verify connectivity across LAN Segment 1 and LAN Segment 2. A computer on either LAN segment should be able to connect to the Internet or share files and printers of any other computers or servers connected to LAN Segment 1 or LAN Segment 2.

Multi-Point Bridge

Multi-point bridge mode allows a router to bridge to multiple peer access points simultaneously. Wireless client associations are disabled. Only wired clients can be connected. Multi-point bridge mode configuration includes the following steps:

1. Enter the MAC addresses of the other access points in the fields provided.
2. Set the other bridge-mode access points to point-to-point bridge mode, using the MAC address of this DGN2200M Mobile Edition as the remote MAC address.
3. Use wireless security to protect this traffic.

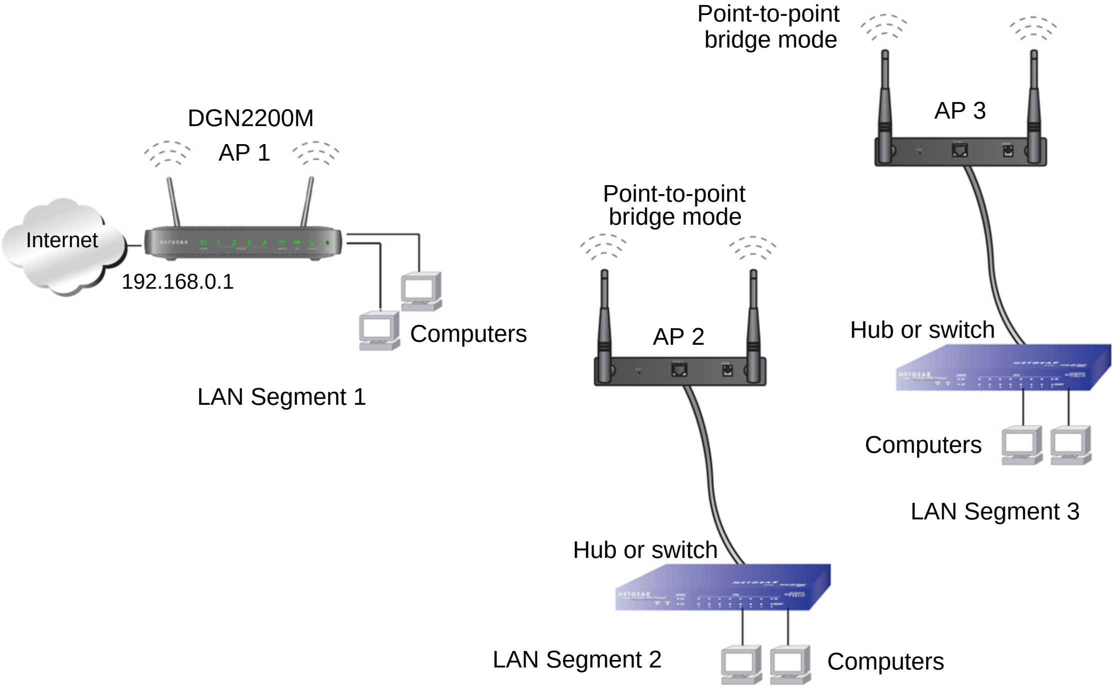


Figure 2. Multi-point bridge mode

➢ To set up the multi-point bridge configuration:

1. Configure the operating mode of the wireless modem routers.
   - Because it is in a central location, configure the DGN2200M Mobile Edition wireless modem router (AP 1) on LAN segment 1 in point-to-multi-point bridge mode, and enter the MAC addresses of AP 2 and AP 3 in the Remote MAC Address 1 and Remote MAC Address 2 fields.
   - Configure the access point (AP 2) on LAN segment 2 in point-to-point bridge mode with the remote MAC address of the DGN2200M Mobile Edition wireless modem router.
   - Configure the access point (AP 3) on LAN segment 3 in point-to-point bridge mode with the remote MAC address of the DGN2200M Mobile Edition wireless modem router.
2. Disable the DHCP server on AP 2 and AP 3. AP 1 will then be the DHCP server.
3. Verify the following for all access points:

- The LAN networks of the wireless modem router and other access points are configured to operate in the same LAN network address range as the LAN devices.
- Only one access point, the DGN2200M Mobile Edition wireless modem router in *Figure 2, Multi-point bridge mode*, is configured in point-to-multi-point bridge mode; all the others are in point-to-point bridge mode.
- All APs, including the DGN2200M Mobile Edition wireless modem router, need to be on the same LAN. That is, all the access point LAN IP addresses need to be in the same network.
- If you are using DHCP, for all access points, in the Internet IP Address section of the Basic Settings screen, the **Get Dynamically from ISP** check box should be selected.
- All APs, including the DGN2200M Mobile Edition wireless modem router, need to use the same SSID, channel, authentication mode, if any, and WEP security settings if security is in use.
- All point-to-point APs need to have the MAC address of AP 1 (the DGN2200M Mobile Edition wireless modem router in the previous figure) in the Remote AP MAC address field.

4. Verify connectivity across the LANs. A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other computers or servers connected to any of the three LAN segments.

Note: Wireless stations configured as they are in *Figure 1* on page 92 will not be able to connect to the wireless modem router or access points. If you require wireless stations to access any LAN segment, you can use additional access points configured in wireless access point mode in any LAN segment.

Repeater with Wireless Client Association

In the repeater mode with wireless client association, the DGN2200M Mobile Edition wireless modem router sends all traffic to a remote access point. For the repeater mode, you need to enter the MAC address of the remote “parent” access point. Alternatively, you can configure the DGN2200M Mobile Edition wireless modem router as the parent by entering the address of a “child” access point. Note that the following restrictions apply:

- You *do not* have the option of disabling client associations with this DGN2200M Mobile Edition wireless modem router.
- You cannot configure a sequence of parent-child APs. You are limited to only one parent access point, although if the DGN2200M Mobile Edition wireless modem router is the parent access point, it can connect with up to four child APs.

The following figure shows an example of a repeater mode configuration.

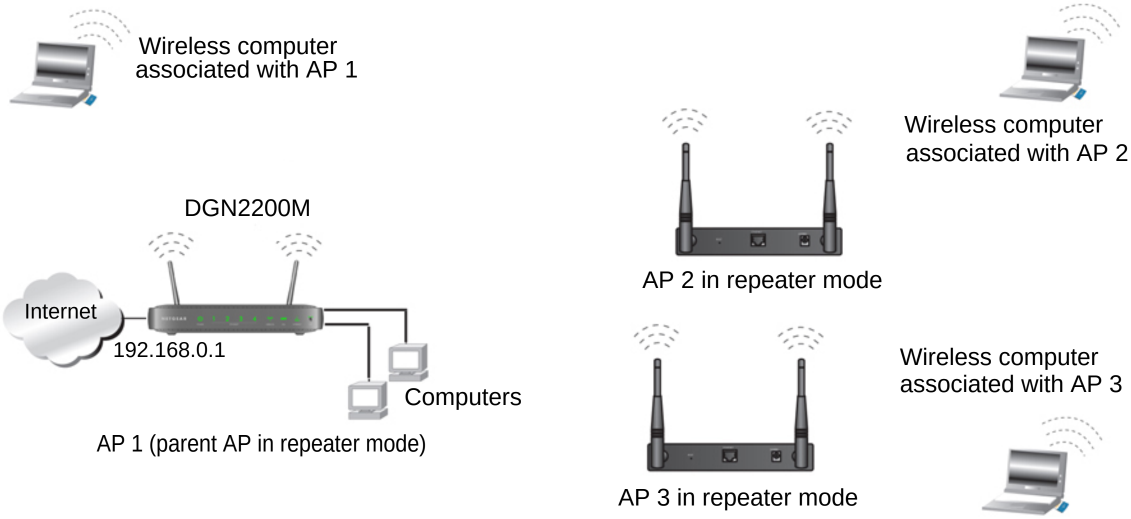

Wireless computer associated with AP 1
DGN2200M
Internet
192.168.0.1
Computers
AP 1 (parent AP in repeater mode)
Wireless computer associated with AP 2
AP 2 in repeater mode
Wireless computer associated with AP 3
AP 3 in repeater mode

Figure 3. Repeater mode

➢ **To set up a repeater with wireless client association:**

1. Configure the operating mode of the devices.
   - Configure AP 1 (the DGN2200M Mobile Edition wireless modem router in *Figure 3, Repeater mode*) with the MAC address of AP 2 and AP 3 in the first two Remote MAC Address fields.
   - Configure AP 2 with the MAC address of AP 1 in the Remote MAC Address field.
   - Configure AP 3 with the MAC address of AP 1 in the Remote MAC Address field.
2. Verify the following for both access points:
   - The LAN network configuration of each access point is configured to operate in the same LAN network address range as the LAN devices.
   - The access points need to be on the same LAN. That is, the LAN IP addresses for the access points need to be in the same network.
   - If you are using DHCP, for all access points, in the Internet IP Address section of the Basic Settings screen, the **Get Dynamically from ISP** check box should be selected.
   - Access point devices need to use the same SSID, channel, authentication mode, and encryption.
3. Verify connectivity across the LANs. A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other computers or servers connected to any of the three WLAN segments.

Port Forwarding and Port Triggering

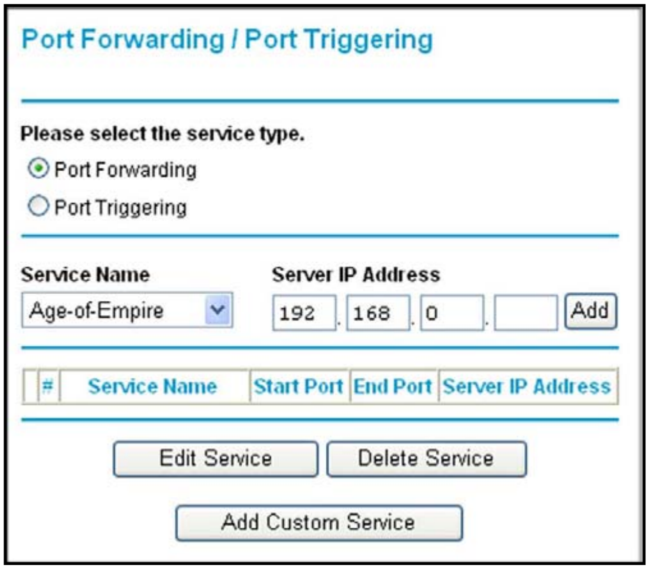
Port forwarding and port triggering are advanced features that affect the behavior of the firewall in your wireless modem router. Using the Port Forwarding / Port Triggering screen, you can make local computers or servers available to the Internet for different services (for example, FTP or HTTP), to play Internet games (like Quake III), or to use Internet applications (like CU-SeeMe).

- Port triggering monitors outbound traffic. When the router detects traffic on the specified outbound port, it remembers the IP address of the computer that sent the data and triggers the incoming port. Incoming traffic on the triggered port is then forwarded to the triggering computer. Port triggering allows requests from the Internet only after a designated port is triggered. Port triggering applies to chat and Internet games.
- Port forwarding is designed for FTP, web server, or other server-based services. Once port forwarding is set up, requests from the Internet are forwarded to the correct server.

Port Forwarding

➢ **To set up port forwarding:**

1. From the main menu, under the Advanced Heading, select **Port Forwarding/Port Triggering**.



Port Forwarding / Port Triggering

Please select the service type.

● Port Forwarding

○ Port Triggering

Service Name: Age-of-Empire

Server IP Address: 192 . 168 . 0 .

#	Service Name	Start Port	End Port	Server IP Address

2. You can select a service or create a custom service.
   - Select a service from the Service Name drop-down list, and specify the computer’s IP address.
   - If you want to add a service that is not in the list, click the **Add Custom Service** button. Fill in the fields in the Add Custom Service screen.

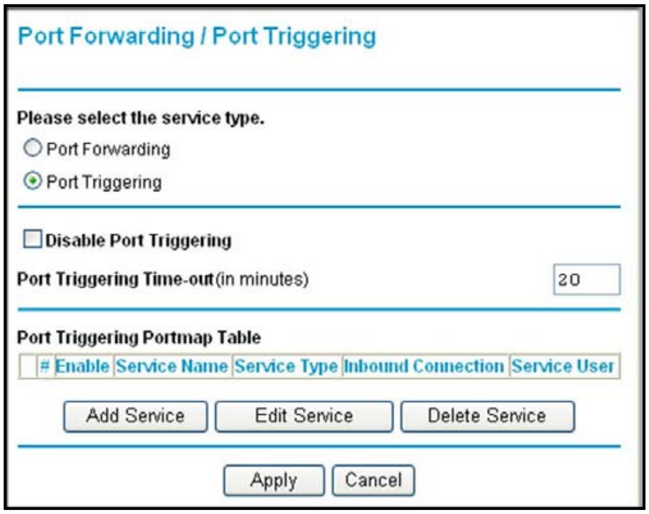
   The service displays in the list.

Port Triggering

➢ **To set up port triggering:**

1. From the main menu, under the Advanced Heading, select **Port Forwarding/Port Triggering**.

2. Select the Port Triggering radio button to display the following screen:



Port Forwarding / Port Triggering

Please select the service type.

○ Port Forwarding

● Port Triggering

□ Disable Port Triggering

Port Triggering Time-out (in minutes) 20

Port Triggering Portmap Table

	#	Enable	Service Name	Service Type	Inbound Connection	Service User

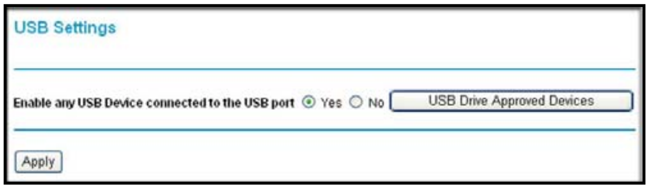
3. Click **Add Service**, and fill in the fields in the Add Service screen.

   The service displays in the list. For more detailed information, see the Port Forwarding/Port Triggering help.

Advanced USB Settings

For added security the router can be set up to share only approved USB devices. To enable this feature, select **No**, and click **Apply**.

To define the approved devices, click **USB Drive Approved Devices**.



USB Settings

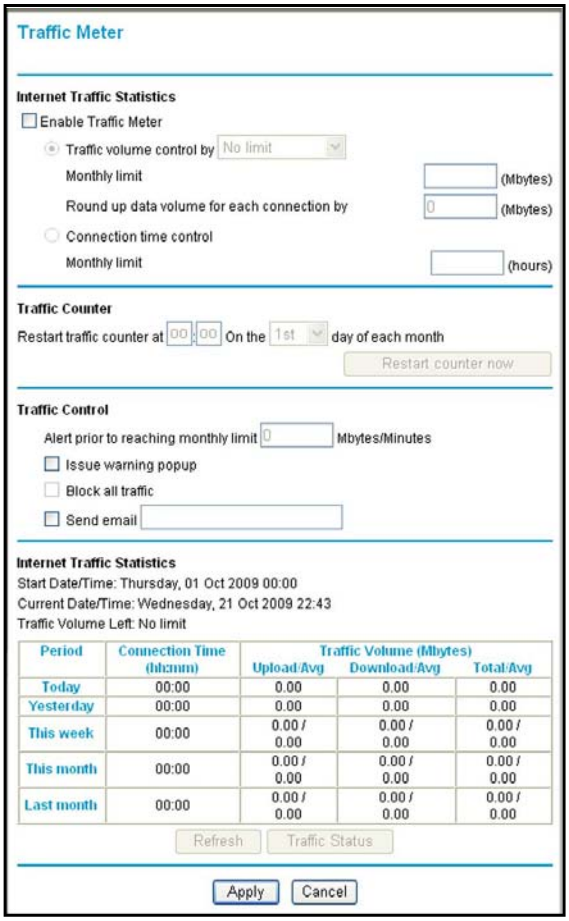
Enable any USB Device connected to the USB port ● Yes ○ No

Traffic Meter

Traffic metering allows you to monitor the volume of Internet traffic passing through your wireless modem 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:**

1. Under Advanced on the main menu, select **Traffic Meter**.



Traffic Meter

Internet Traffic Statistics

☐ Enable Traffic Meter

○ Traffic volume control by No limit

Monthly limit (Mbytes)

Round up data volume for each connection by 0 (Mbytes)

○ Connection time control

Monthly limit (hours)

Traffic Counter

Restart traffic counter at 00 : 00 On the 1st day of each month

Restart counter now

Traffic Control

Alert prior to reaching monthly limit 0 Mbytes/Minutes

☐ Issue warning popup

☐ Block all traffic

☐ Send email

Internet Traffic Statistics

Start Date/Time: Thursday, 01 Oct 2009 00:00

Current Date/Time: Wednesday, 21 Oct 2009 22:43

Traffic Volume Left: No limit

Period	Connection Time (hh:mm)	Traffic Volume (Mbytes)		
		Upload/Avg	Download/Avg	Total/Avg
Today	00:00	0.00	0.00	0.00
Yesterday	00:00	0.00	0.00	0.00
This week	00:00	0.00 / 0.00	0.00 / 0.00	0.00 / 0.00
This month	00:00	0.00 / 0.00	0.00 / 0.00	0.00 / 0.00
Last month	00:00	0.00 / 0.00	0.00 / 0.00	0.00 / 0.00

2. To enable the traffic meter, select the **Enable Traffic Meter** check box.
3. If you would like to record and restrict the volume of Internet traffic, select 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 monthly 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.

Troubleshooting 7

This chapter provides information about troubleshooting your N300 Wireless ADSL2+ Modem Router DGN2200M Mobile Edition. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the router on?

  Go to *Basic Functioning* on page 101.

- Have I connected the router correctly?

  Go to *Basic Functioning* on page 101.

- What are the LEDs on the front panel telling me?

  Go to *Troubleshoot with the LEDs* on page 101.

- I cannot access the router’s configuration with my browser.

  Go to *Cannot Log In to the Wireless-N Modem Router* on page 103.

- I have configured the router, but I cannot access the Internet.

  Go to *Troubleshoot the Internet Connection* on page 104.

- Can my computer communicate with my router or with a remote device on the Internet?

  Go to *Troubleshoot a TCP/IP Network Using the Ping Utility* on page 107.

- I cannot remember the router’s configuration password.

  Go to *Restore the Default Configuration and Password* on page 108.

- I want to clear the configuration and start over again.

  Go to *Restore the Default Configuration and Password* on page 108.

- The date or time is wrong.

  Go to *Problems with Date and Time* on page 108.

Basic Functioning

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 LED is on.
2. After approximately 10 seconds, verify the following:
   - The LAN Ports LEDs are lit for any local ports that are connected.
   - The DSL LED is lit.

   If the DSL link LED is lit, a link has been established to the connected device. If a LAN port is connected to a 100 Mbps device, verify that the port’s LED is green. If the port is 10 Mbps, the LED is amber.

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

Welcome Screen Displays instead of Router Main Menu

This situation can occur if the CD Setup Wizard does not finish successfully; the unit stays in Wizard Mode. If the Welcome screen displays instead of the main menu when you try to go to the Internet or log in to the wireless modem router, you can bypass the wizard using one of the following methods:

- Log in to the wireless modem router at **http://routerlogin.com/basicsetting.htm**.
- Reset the wireless modem router to factory defaults to take the router out of Wizard Mode altogether.

Troubleshoot with the LEDs

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

1. When power is first applied, verify that the Power LED ⏻ is on.
2. After approximately 10 seconds, verify that:
   - The Power LED is green.
   - The LAN Ports LEDs are lit for any local ports that are connected. If a LAN port is connected to a 100 Mbps device, verify that the port’s LED is green. If the port is 10 Mbps, the LED is amber.
   - The DSL LED is lit, indicating that a link has been established to the connected device.
   - The WiFi LED is lit.

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

Table 13. Troubleshooting with the LEDs

Situation	Recommended action
Power LED is off.	If the Power and other LEDs are off when your router is turned on: • Make sure the power cord is securely connected to your router and that the power supply adapter is securely connected to a functioning power outlet. • Check that you are using the power adapter supplied by NETGEAR for this product. If the error persists, you have a hardware problem and should contact technical support at *http://support.netgear.com*.
Power LED is red. The Power LED turns red when you press the Restore Factory Settings button and blinks red three times when that button is released. This is normal and does not indicate a problem.	If the Power LED remains red, there is a fault within the router. • Cycle the power to see if the router recovers. • Clear the router’s configuration to factory defaults. This sets the router’s IP address to 192.168.0.1. This procedure is explained in *Restore the Default Configuration and Password* on page 108. If the error persists, you might have a hardware problem and should contact technical support at *http://support.netgear.com*.
LEDs never turn off.	When the router is turned on, the LEDs turn on for about 10 seconds and then turn off. If all the LEDs stay on, there is a fault within the router. If all LEDs 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 *Restore the Default Configuration and Password* on page 108. If the error persists, you might have a hardware problem and should contact Technical Support at *http://support.netgear.com*.
DSL LED is off.	• Disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being careful to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones. • Check that the telephone company has made the connection to your line and tested it. • Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the ADSL service. It might be necessary to use a swapper if your ADSL signal is on pins 1 and 4 of the RJ-11 jack. The N300 Wireless ADSL2+ Modem Router uses pins 2 and 3.
Internet Port LED is red.	The wireless modem router cannot access the Internet. See *Internet Port LED Is Red* on page 105.

Table 13. Troubleshooting with the LEDs (continued)

Situation	Recommended action
The LAN Ports LEDs are off.	If the LAN Ports LEDs do not light when the Ethernet connection is made, check the following: • Make sure that the Ethernet cable connections are secure at the wireless modem router and computer. • Make sure that power is turned on to the connected modem or computer.
WiFi LED is off.	If the WiFi LED does not come on, verify that the **Enable Wireless Router Radio** check box is selected on the Wireless Settings screen. See *View or Change Wireless Settings* on page 34.

Cannot Log In to the Wireless-N Modem Router

If you are unable to log in to the wireless modem router from a computer on your local network, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router as described in the previous section.
- Make sure that your computer’s IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer’s address should be in the range of 192.168.0.2 to 192.168.0.254.
- If your computer’s IP address is shown as 169.254.x.x, recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 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.
- If your router’s IP address was changed and you do not know the current IP address, clear the router’s configuration to factory defaults. This sets the router’s IP address to 192.168.0.1. This procedure is explained in *Use the Restore Factory Settings Button to Reset the Router* on page 108.
- 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 quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when you enter this information.

If the router does not save changes you have made while logged in, check the following:

- When entering configuration settings, be sure to click the **Apply** button before moving to another screen or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. The changes might have occurred, but the web browser might be caching the old configuration.

Troubleshoot the Internet Connection

If your router is unable to access the Internet, you should check the ADSL or mobile broadband connection, then the WAN TCP/IP connection.

DSL Link

If your router is unable to access the Internet, you should first determine whether you have an ADSL link with the service provider. The state of this connection is indicated with the Internet LED.

DSL LED Is Green or Blinking Green

If your DSL LED is green or blinking green, then you have a good ADSL connection. You can be confident that the service provider has connected your line correctly and that your wiring is correct.

DSL LED Is Blinking Amber

If your DSL LED is blinking amber, then your wireless modem router is attempting to make an DSL connection with the service provider. The LED should turn green within several minutes.

If the DSL LED does not turn green, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being sure to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green DSL LED, there might be a problem with your wiring. If the telephone company has tested the ADSL signal at your network interface device (NID), then you might have poor-quality wiring in your house.

DSL LED Is Off

If the DSL LED is off, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being sure to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green DSL LED, check for the following:

- Check that the telephone company has made the connection to your line and tested it.
- Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the ADSL service. It might be necessary to use a swapper if your ADSL signal is on pins 1 and 4 or the RJ-11 jack. The wireless modem router uses pins 2 and 3.

Internet Port LED Is Red

If the Internet Port LED is red, the device was unable to connect to the Internet. Verify the following:

- Check that your login credentials are correct, or that the information you entered on the Basic Settings screen is correct.
- Check with your ISP to verify that the multiplexing method, VPI, and VCI settings on the ADSL settings screen are correct.
- Check if your ISP has a problem—it might not be that the router cannot connect to the Internet but that your ISP cannot provide an Internet connection.

Connecting to Mobile Broadband

If you are unable to connect to mobile broadband, check the following:

- The Internet account is active.
- Wireless broadband coverage is available where the unit is located. Test this availability by connecting the USB modem to the laptop directly.
- Access the router main menu to verify that the configurations of the broadband settings are correct. Check with your ISP if unsure.
- Check the SIM PIN code (if used).

Obtain an Internet IP Address

If your wireless modem router is unable to access the Internet, and your Internet Port LED is green or blinking green, you should determine whether the wireless modem router is able to obtain an Internet IP address from the ISP. Unless you have been assigned a static IP address, your wireless modem router needs to request an IP address from the ISP. You can determine whether the request was successful using the browser interface.

➢ **To check the Internet IP address from the browser interface:**

1. Launch your browser, and select an external site such as *www.netgear.com*.
2. Access the main menu of the wireless modem router’s configuration at http://192.168.0.1.
3. In the main menu, under Maintenance, select **Router Status**, and check that an IP address is shown for the WAN port. If 0.0.0.0 is shown, your wireless modem router has not obtained an IP address from your ISP.

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

- If you have selected a login program, the service name, user name, or password might be incorrectly set. See the following section, *Troubleshoot PPPoE or PPPoA* .
- Your ISP might check for your computer’s host name. Assign the computer host name of your ISP account to the wireless modem router in the browser-based Setup Wizard.

- 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 can be done in the Basic Settings screen.

Troubleshoot PPPoE or PPPoA

➢ **The PPPoE or PPPoA connection can be debugged as follows:**

1. Access the main menu of the router at http://192.168.0.1.
2. Under Maintenance, select **Router Status**.
3. Click the **Connection Status** button.
4. If all of the steps indicate OK, then your PPPoE or PPPoA connection is up and working.
5. If any of the steps indicates Failed, you can attempt to reconnect by clicking **Connect**. The wireless modem router will continue to attempt to connect indefinitely.

If you cannot connect after several minutes, you might be using an incorrect service name, user name, or password. There also might be a provisioning problem with your ISP.

Note: Unless you connect manually, the wireless modem router will not authenticate using PPPoE or PPPoA until data is transmitted to the network.

Troubleshoot Internet Browsing

If your wireless modem 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 wireless modem router’s configuration, reboot your computer, and verify the DNS address. Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

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

  If your computer obtains its information from the wireless modem router by DHCP, reboot the computer, and verify the wireless modem router address.

Troubleshoot a TCP/IP Network Using the Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshoot a TCP/IP network by using the ping utility in your computer.

Test the LAN Path to Your Wireless-N Modem 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 PC running Windows 95 or later:**

1. From the Windows toolbar, click the **Start** button, and select **Run**.
2. In the field provided, type **ping** followed by the IP address of the router, as in this example:

   ping 192.168.0.1

3. Click **OK**.

   You should see a message like this one:

   ```
   Pinging <IP address> with 32 bytes of data
   ```

   If the path is working, you see this message:

   ```
   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
   ```

   If the path is not working, you see this message:

   ```
   Request timed out
   ```

   If the path is not functioning correctly, you could have one of the following problems:

   - Wrong physical connections
     - Make sure that the LAN Port LED is on. If the LED is off, follow the instructions in *Troubleshoot with the LEDs* on page 101.
     - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
   - Wrong network configuration
     - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer or workstation.
     - Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Test 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. In the Windows Run screen, type:

ping -n 10 IP address

where *IP address* is the IP address of a remote device such as your ISP’s DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Check that your computer has the IP address of your router listed as the default wireless modem router. If the IP configuration of your computer is assigned by DHCP, this information will not be visible in your computer’s Network Control Panel. Verify that the IP address of the router is listed as the default wireless modem router.
- Check to see that the network address of your computer (the portion of the IP address specified by the netmask) 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 need to configure your router to “clone” or “spoof” the MAC address from the authorized computer.

Restore the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router’s administration password to **password** and the IP address to **192.168.0.1**. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function (see *Back Up, Restore, and Erase Your Settings* on page 54).
- Press the Restore Factory Settings button on the bottom of the router.

Use the Restore Factory Settings Button to Reset the Router

To restore the factory default configuration settings when you do not know the administration password or IP address, use the Restore Factory Settings button on the bottom of the router.

➢ **To reset the router:**

1. Press and hold the **Restore Factory Settings** button until the Power LED turns red (about 6 seconds).
2. Release the **Restore Factory Settings** button. The LED blinks red three times and then turns green when the router has reset to the factory default state. Wait for the router to reboot.

Problems with Date and Time

In the main menu, under Security, select **Schedule** to display the current date and time of day. The wireless modem 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:

- Date shown is January 1, 2000.
  Cause. The router has not yet successfully reached a network time server. Check that your Internet access is configured correctly. 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 automatically sense daylight savings time. In the Schedule screen, select the **Adjust for Daylight Savings Time** check box.

Technical Specifications and Factory Default Settings

A

This appendix includes technical specifications for the N300 Wireless ADSL2+ Modem Router DGN2200M Mobile Edition.

Specifications

Table 14. Specifications

Specification	Description
Network protocol and standards compatibility	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM
Power adapter	North America: 120V, 60 Hz, input
	UK, Australia: 240V, 50 Hz, input
	Europe: 230V, 50 Hz, input
	All regions (output): 12V @ 1.5A output
Physical	Dimensions: 6.80 in. x 5.03 in. x 1.28 in. (173 mm x 128 mm x 33 mm)
	Weight: 0.65 lbs without the stand (0.29 kg)
Environmental	Operating temperature: 0° to 40°C (32º to 104ºF)
	Operating humidity: 10% to 90% relative humidity, noncondensing
	Storage temperature: –20° to 70°C (–4º to 158ºF)
	Storage humidity: 5% to 95% relative humidity, noncondensing
Regulatory compliance	FCC Part 15 Class B; VCCI Class B; EN 55 022 (CISPR 22), Class B
Network protocol and standards compatibility	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM
Power adapter	North America: 120V, 60 Hz, input

Table 14. Specifications (continued)

Specification	Description
Regulatory compliance	FCC Part 15 Class B; VCCI Class B; EN 55 022 (CISPR 22), Class B
Interface specifications	LAN: 10BASE-T or 100BASE-Tx, RJ-45 WAN: ADSL, Dual RJ-11, pins 2 and 3 T1.413, G.DMT, G.Lite ITU Annex A or B ITU G.992.5 (ADSL2+)

Factory Default Configuration

You can use the Restore Factory Settings button on the bottom panel of your router to restore factory default settings. Press this button for 6 seconds. Your router will return to the factory configuration settings shown in the following table.

Table 15. Factory default settings

Feature		Default behavior
Router login	User login URL	*http://www.routerlogin.com*
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Internet connection	WAN MAC address	Use default address
	WAN MTU size	1492
	Port speed	Autosensing
Local network (LAN)	LAN IP	192.168.0.1
	Subnet mask	255.255.255.0
	RIP direction	None
	RIP version	Disabled
	RIP authentication	None
	DHCP server	Enabled
	DHCP starting IP address	192.168.0.2
	DHCP ending IP address	192.168.0.254
	DMZ	Enabled or disabled
	Time zone	GMT for WW except NA and GR, GMT+1 for GR, GMT-8 for NA
	Time zone adjusted for daylight savings time	Disabled
	SNMP	Disabled
Firewall	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the HTTP port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled

Table 15. Factory default settings (continued)

Feature		Default behavior
Wireless	Wireless communication	Enabled
	SSID name	Uniquely generated for every device (NETGEAR-3G in older models)
	Security	Uniquely generated for every device (disabled in older models)
	Broadcast SSID	Enabled
	Country/region	United States (in North America; otherwise, varies by region)
	RF channel	Auto
	Operating mode	Up to 145 Mbps
	Data rate	Best
	Output power	Full
	Access point	Enabled
	Authentication type	Open System
	Wireless card access list	All wireless stations allowed

B. Wall-Mounting

B

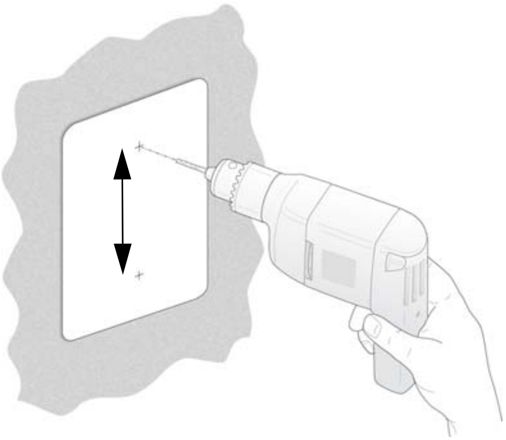
This appendix provides instructions for wall-mounting your wireless modem router.

Your router’s location can affect wireless connections. For example, the thickness and number of walls the wireless signal needs to pass through might limit its range. For best results, place your router:

- Near an AC power outlet, close to computers you plan to connect with Ethernet cables, and near locations where you use wireless computers. For best signal strength, the router should be within line of sight of your wireless devices.
- In an elevated location, keeping the number of walls and ceilings between the wireless modem router and your wireless computers to a minimum.
- Away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, or the base for a cordless phone.

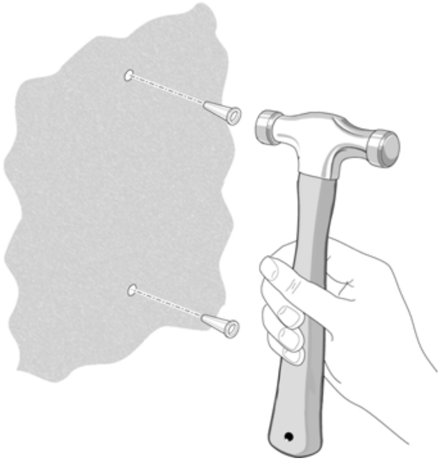
➢ **To wall-mount the wireless modem router:**

1. Drill holes in the wall where you will wall-mount the router.



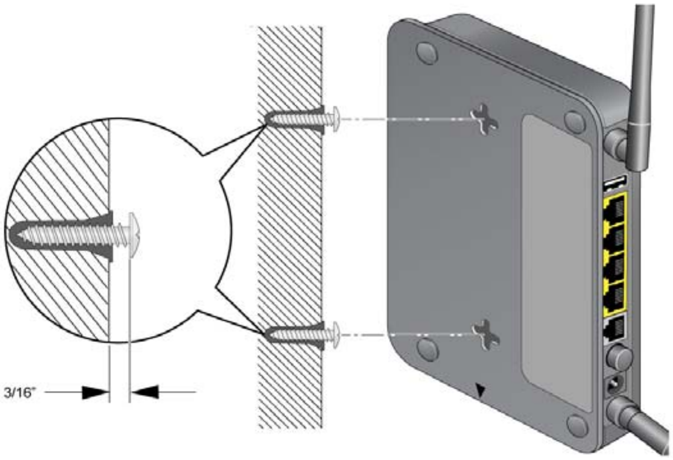
Holes should be 9.5 in. (24.1 cm) center to center.

2. Install wall anchors in the holes.

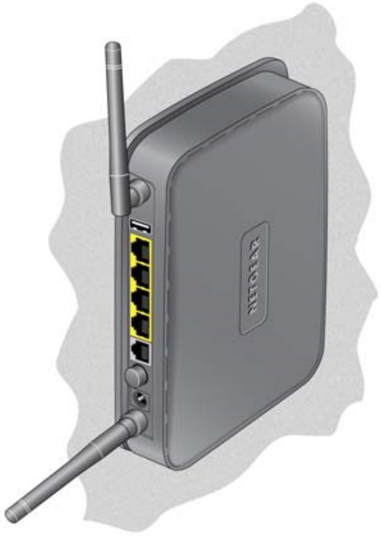


Use pan head Phillips wood screws, 3.5 x 20 mm (diameter x length, European) or #6 type screw, 1 inch long (U.S.).

3. Insert screws into the wall anchors, leaving 3/16 in. (0.5 cm) of each screw exposed.



4. For best wireless performance, position the wireless antennas as shown.



Notification of Compliance

C

NETGEAR Wireless Routers, Gateways, APs

Regulatory Compliance Information

Note: This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

Note: This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

Europe – EU Declaration of Conformity

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 (2.4Ghz), EN301 489-17 EN60950-1

For complete DoC, visit the NETGEAR EU Declarations of Conformity website at: *http://support.netgear.com/app/answers/detail/a_id/11621/*

EDOC in Languages of the European Community

Language	**Statement**
Cesky [Czech]	*NETGEAR* Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 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.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *NETGEAR Inc.* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
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.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
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.
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.
Magyar [Hungarian]	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*NETGEAR Inc.* týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
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.
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.

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the N300 Wireless ADSL2+ Modem Router DGN2200M Mobile Edition complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

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 uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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.
- 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.
- For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.

- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (TBD) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada

Industry Canada

This device complies with RSS-210 of the Industry Canada 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.

IMPORTANT NOTE: Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Caution:

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

GPL License Agreement

GPL may be included in this product; to view the GPL license agreement go to *ftp://downloads.netgear.com/files/GPLnotice.pdf.*

For GNU General Public License (GPL) related information, please visit *http://support.netgear.com/app/answers/detail/a_id/2649 .*

Interference Reduction Table

The table below shows the recommended minimum distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters).

Household Appliance	Recommended Minimum Distance (in feet and meters)
Microwave ovens	30 feet / 9 meters
Baby Monitor - Analog	20 feet / 6 meters
Baby Monitor - Digital	40 feet / 12 meters
Cordless phone - Analog	20 feet / 6 meters
Cordless phone - Digital	30 feet / 9 meters
Bluetooth devices	20 feet / 6 meters
ZigBee	20 feet / 6 meters

Index