NETGEAR

Mobile Broadband 11n Wireless Router MBR1000

User Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

May 2010
202-10577-01
v1.0

Part Number 202-10577-01 v1.0

Technical Support

When you register your product at *http://www.netgear.com/register*, NETGEAR can provide you with faster expert technical support and timely notices of product and software upgrades.

NETGEAR, Inc.
350 East Plumeria Drive
San Jose, CA 95134 USA

E-mail: support@netgear.com

Website: *http://www.netgear.com*

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

Trademarks

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.

Revision History

Publication Part Number	Version	Publish Date
202-10577-01	v1.0	May 2010

Table of Contents

Chapter 5 Advanced

Chapter 6 Troubleshooting

Connecting to the Internet

1

This chapter describes how to configure your NETGEAR Mobile Broadband 11n Wireless Router MBR1000 Internet connection. For help with installation, see the *Mobile Broadband 11n Wireless Router MBR1000 Installation Guide.*

Hardware Features

Router Stand

Use the stand to position your router upright.

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.

   The router must also be located to receive Mobile Broadband signals while indoors if you are planning to connect to the Internet using the Mobile Broadband WAN port.

Router Front Panel

The router front panel shown below contains control buttons and status LEDs.

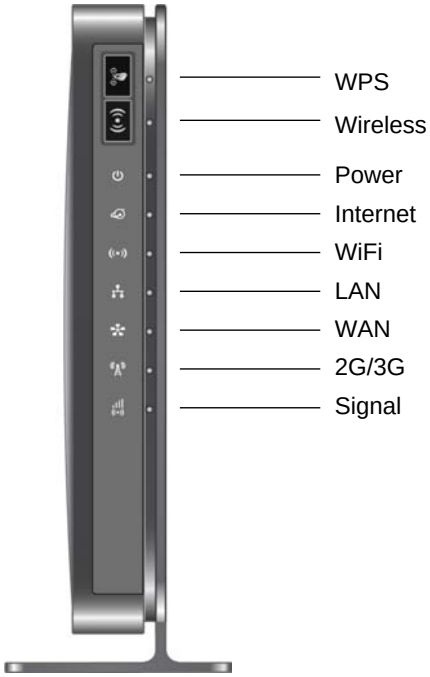


Figure 1 Front panel

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 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 router to connect with other WPS-enabled devices. For more information, about using the WPS method to implement security, see *"Using Push 'N' Connect (WPS) to Configure Your Wireless Network"* on page 22.	
WiFi 	Turn the WiFi radio in the router on and off. The WiFi radio is on by default.	
Power 	Solid green	Solid green. Power is supplied to the router.
	Solid Red	POST (Power-On Self-Test) failure or device malfunction.
	Off	Power is not supplied to the router.
	Restore Factory Settings button	Press button for 6 seconds. Power LED lights briefly. When released, the LED blinks red three times and then turns green as the gateway resets to the factory defaults.

Table 1. Front Panel Button and LED Descriptions

Button/LED	Activity	Description
Internet Port 	Solid green	There is an Internet session.
	Solid red	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 bridged mode.
WiFi 	Solid blue	Indicates that the WiFi local port is initialized.
	Blinking blue	Data is being transmitted or received over the WiFi link.
	Off	The Wireless Access Point is turned off.
LAN Ports 	Solid green	The Ethernet local ports have detected wired links with PCs.
	Blinking	Data is being transmitted or received.
	Off	No link is detected on these ports.
WAN Port 	Solid green	The Ethernet WAN port has detected a link with a wired modem.
	Blinking	Data is being transmitted or received.
	Off	No link is detected on these ports.
2G/3G 	Solid blue	Indicates a 3G mobile broadband signal is being detected.
	Solid green	Indicated a 2G mobile broadband signal is being detected.
	Off	Indicates the router cannot tell if the mobile broadband signal being detected is 2G or 3G.
Signal 	Solid blue	Excellent mobile broadband coverage detected.
	Solid green	Good mobile broadband coverage detected.
	Solid amber	Marginal mobile broadband coverage detected.
	Off	No mobile broadband coverage detected.

Router Back Panel

The back panel of the router contains port connections.

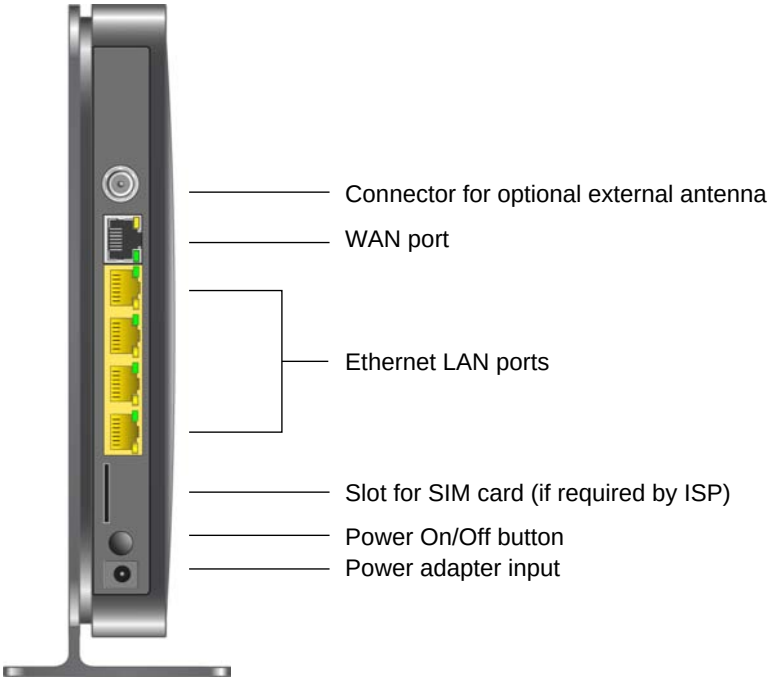


Figure 2 Back panel

Router Label

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

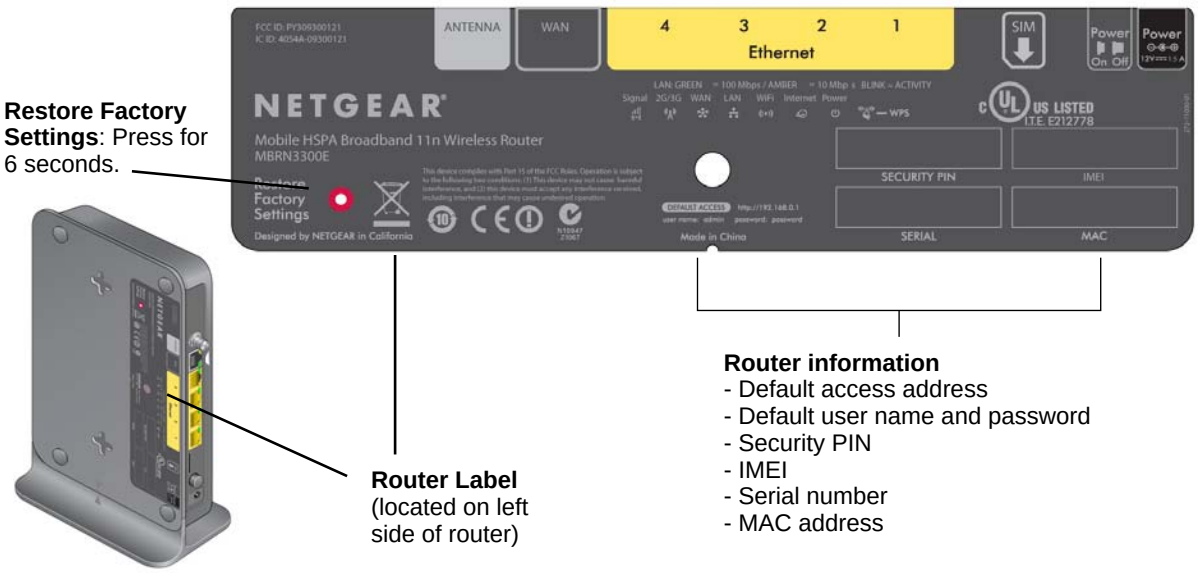


Figure 3 Router label

Logging In to Your Router

When you first connect to your router during installation, a Setup Wizard appears. For help using the Setup Wizard to configure your Internet and wireless network, see the *Mobile Broadband Wireless-N Router MBRN3000 Installation Guide*.

After the initial configuration, you can use your Web browser to log into the router to view or change its settings. Links to Knowledge Base and documentation are also available on the router main menu.

> **Note:** Your computer must be configured for DHCP. For help with configuring DHCP, see the documentation that came with your computer or see the link to the online document in <pdf>“Preparing a Computer for Network Access:” in Appendix B.

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

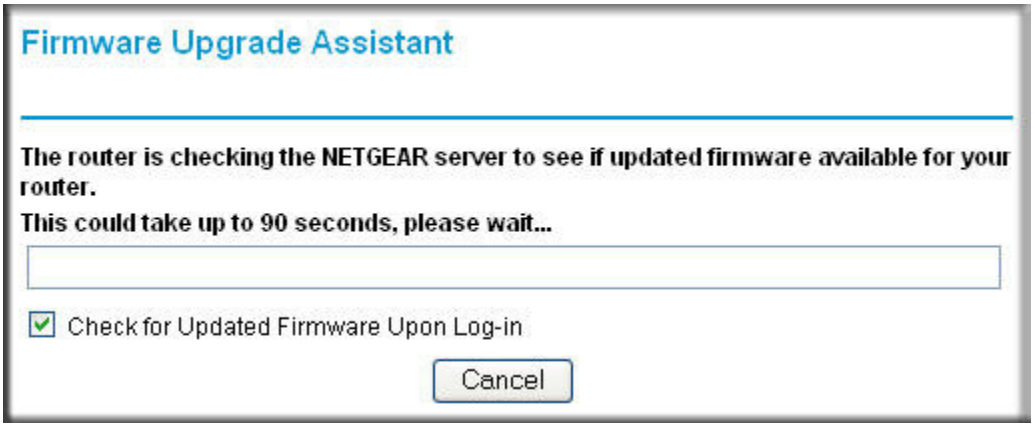
To log in to the router:

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

2. Enter **admin** for the user name and your password (or the default, **password**). For information about how to change the password, see *“Changing the Built-In Password”* on page 27.

> **Note:** If you changed your password and do not remember what it is, you can restore the router to its factory settings. See "Factory Default Settings" in Appendix A.

3. If the router has not been configured, the Smart Wizard screen displays. After the router has been configured, the Firmware Upgrade assistant will appear.
   - **Checking for Firmware Updates screen**. After initial setup, this screen displays unless you have cleared the **Check for Updated Firmware Upon Log-in** checkbox.

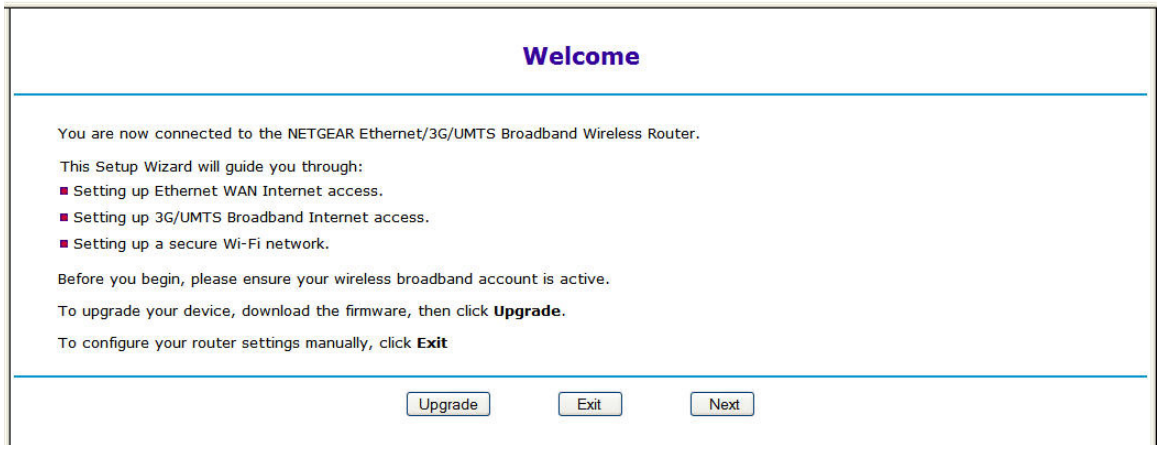


   - **Router Status screen**. The Router Status screen displays if the router's Internet connection has not been set up yet. See *"Router Status"* on page 38.
4. You can use different methods to configure your router.
   - Select Setup Wizard from the router menu to set up your Internet connection and wireless network configuration. See *"Accessing the Configuration Assistant After Installation"* on page 11.
   - You can manually configure the router settings. See *"Manually Configuring Your Internet Settings"* on page 12.

Accessing the Configuration Assistant After Installation

1. Log in to the router as described in *"Logging In to Your Router"* on page 10.

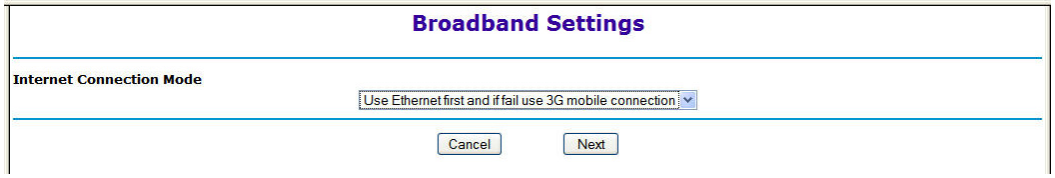
   You will get the Configuration Assistant.



2. Click **Next**.

   The Configuration Assistant prompts you to set up your Internet connection and wireless network as described in the *Mobile Broadband 11n Wireless Router MBR1000 Installation Guide*.

   a. Select your Internet Connection Mode:
      - Use Ethernet first and if fail use 3G mobile connection
      - Use 3G mobile connection only
      - Use Ethernet connection only



   b. Click **Next**.
   c. Select your Country and then your Internet Service Provider.
   d. Click **Done**.

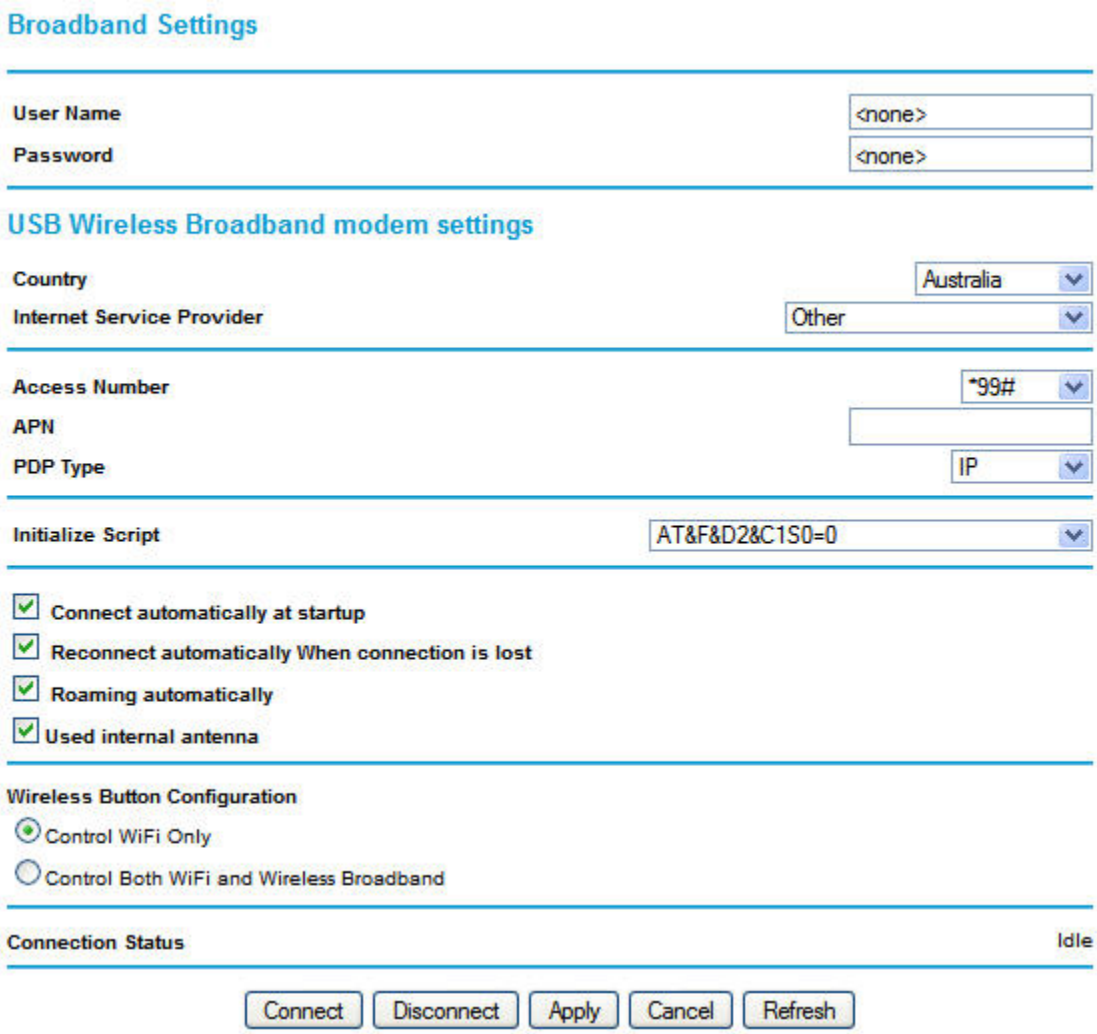
Manually Configuring Your Internet Settings

In order to connect to the network, and active broadband service account is required. Contact your ISP for username, password and the network name.

To manually configure your Internet settings:

1. Log in to the router as described in *"Logging In to Your Router"* on page 10.

2. Select Wireless Broadband Account Settings.



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:
   - **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 2. Broadband Settings fields

Fields and Checkboxes	Description
Username	Internet account login username.
Password	Internet account password for authentication.
Country	Select your country from the pulldown list.
Internet Service Provider	Select your Internet Service Provider from the pulldown 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**:
Initialize Script	Select the initialization script from the pulldown list. • **AT**: • **ATV1**: • **ATE0**: • **ATZ**: • **AT&F&D2&C1S0=0**: • **ATQ0V1E0S0=0&C1&D2+FCLASS=0**: • **Other**:
Connect automatically at startup	If this checkbox 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	If this check box is selected, the modem will attempt to reconnect to the network when the connection is lost. Under normal situation, this setting should be selected.
Connect only to preferred operators	If this checkbox is cleared (not selected) the unit may roam to any available operator in range and may incur roaming charges.
Roaming automatically	If this checkbox is cleared (not selected), the unit will not roam.
Use internal antenna	If this checkbox is selected, the router will use the internal antenna rather than the external antenna.

Table 2. Broadband Settings fields (Continued)

Fields and Checkboxes	Description
Wireless Button Configuration	Select the choice to determine the behavior of the WPS push button on the front panel when depressed. • **Control WiFi Only**: Pressing the push button will toggle the WiFi function. If WiFi is turned on, pressing the push button will turn off the WiFi. Pressing it again will turn on the WiFi. This function is only available if the WiFi function is enabled. The Wireless Broadband function is unaffected. • **Control Both WiFi and Wireless Broadband**: Pressing the push button will toggle both the WiFi function and Wireless Broadband at the same time. If WiFi is turned on, pressing the push button will turn off the WiFi. At the same time, the wireless broadband connection is disconnected. Pressing the push button again, WiFi will be turned on and the router will attempt to re-establish wireless broadband connection. Depending on the coverage, wireless broadband coverage may or may not be connected successfully.
Connection status	Current WAN port status

Wireless Network Configuration

2

For a wireless connection, the SSID, also called the wireless network name, and the wireless security setting must be the same for the router and wireless computers or wireless adapters. NETGEAR strongly recommends that you use wireless security.

Note: Computers can connect wirelessly at a range of several hundred feet. If you do not use wireless security, this can allow others outside of your immediate area to access your network.

Planning Your Wireless Network

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

To configure the wireless network, you can either specify the wireless settings, or you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security.

- To manually configure the wireless settings, you must know the following:
  - SSID. The default SSID for the router is NETGEAR-3G.
  - The wireless mode (80.211n, 802.11g, or 802.11b) that each wireless adapter supports.
  - Wireless security option. To successfully implement wireless security, check each wireless adapter to determine which wireless security option it supports.

  See *"Manually Configuring Your Wireless Settings"* on page 18.
- Push 'N' Connect (WPS) implements WPA/WPA2 wireless security on the router and your wireless computer or device at the same time. The wireless computer or device must be compatible with WPS.

  See *"Using Push 'N' Connect (WPS) to Configure Your Wireless Network"* on page 22.

Wireless Placement and Range Guidelines

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

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

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

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

Wireless Security Options

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

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The Mobile Broadband 11n Wireless Router provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

There are several ways you can enhance the security of your wireless network:

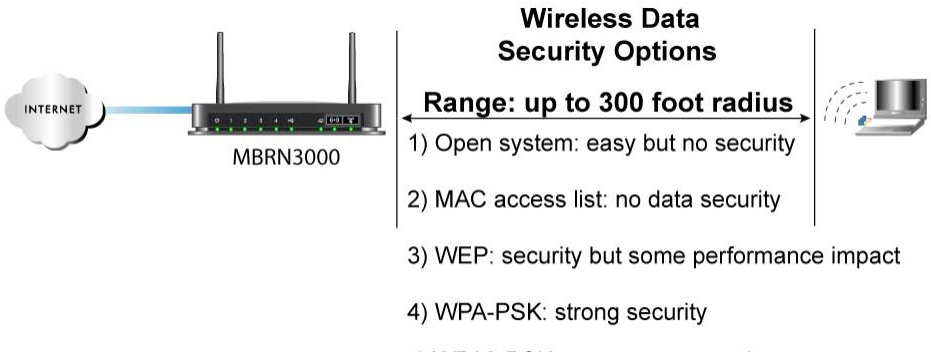


Figure 4 Wireless Security

- **Restrict Access Based on MAC Address**. You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the router. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn Off the Broadcast of the Wireless Network Name SSID**. If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies wireless network 'discovery' feature of some products, such as Windows XP, but the data is still exposed.
- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK.
- **WPA-802.1x, WPA2-802.1x**. Wi-Fi Protected Access (WPA) with user authentication implemented using IEE 802.1x and RADIUS servers.
- **WPA-PSK (TKIP), WPA2-PSK (AES)**. Wi-Fi Protected Access (WPA) using a pre-shared key to perform authentication and generate the initial data encryption keys. The very strong authentication along with dynamic per frame re-keying of WPA makes it virtually impossible to compromise.

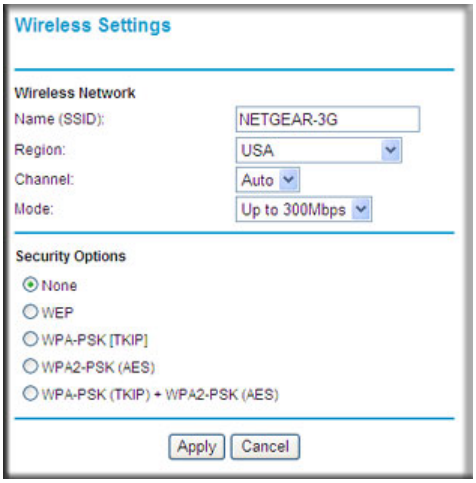
For more information about wireless technology, see the link to the online document in "Wireless Communications:" in Appendix B.

Manually Configuring Your Wireless Settings

Note: If you use a wireless computer to change the wireless network name (SSID) or wireless security, you will be disconnected when you click **Apply**. To avoid this problem, connect your computer to the router with an Ethernet cable while you are making changes.

To view or manually configure the wireless settings:

1. Log in to the router as described in *"Logging In to Your Router"* on page 10.
2. Select Wireless Settings from the main menu:



   The settings for this screen are explained in Table 3.

3. Select the region in which the router will operate.
4. For initial configuration and test, leave the other settings unchanged.
5. To save your changes, click **Apply**.
6. Configure and test your computers for wireless connectivity.

   Set up your wireless computers with the same SSID and wireless security settings as your router. Check that they have a wireless link and are able to obtain an IP address by DHCP from the router. If there is interference, adjust the channel.

Table 3. Wireless Settings

Settings		Description
Wireless Network	Name (SSID)	The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. When there is more than one wireless network, SSIDs provide a means for separating the traffic. To join a network, a wireless computer or device must use the SSID.
	Region	The location where the Router is used.
	Channel	The wireless channel used by the gateway. The default is Auto. Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, you might need to try different channels to see which works best.
	Mode	The default is up to 300 Mbps.

Table 3. Wireless Settings (Continued)

Settings		Description
Security Options	None	You can use this setting to establish wireless connectivity before implementing wireless security. NETGEAR strongly recommends that you implement wireless security.
	WEP	Use encryption keys and data encryption for data security. You can select 64-bit or 128-bit encryption. See Configuring WEP.
	WPA-PSK (TKIP)	Allow only computers configured with WPA to connect to the router. See Configuring WPA, WPA2, or WPA + WPA2.
Security Options (continued)	WPA2-PSK (AES)	Allow only computers configured with WPA2 to connect to the router. See Configuring WPA, WPA2, or WPA + WPA2.
	WPA-PSK (TKIP) + WPA2-PSK (AES)	Allow computers configured with either WPA-PSK or WPA2-PSK security to connect to the router. See Configuring WPA, WPA2, or WPA + WPA2.

Configuring WEP

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

To configure WEP data encryption:

1. Log in to the router as described in *"Logging In to Your Router"* on page 10.
2. From the main menu, select Wireless Settings to display the Wireless Settings screen.
3. In the Security Options section, select the **WEP (Wired Equivalent Privacy)** radio button:

Figure 2-1

4. Select the **Authentication Type**: **Automatic**, **Open System**, or **Shared Key**. The default is Open System.

> **Note:** The authentication is separate from the data encryption. You can select authentication that requires a shared key, but still leaves data transmissions unencrypted. Security is stronger if you use both the Shared Key and WEP encryption settings.

5. Select the **Encryption Strength** setting:
   - **WEP (Wired Equivalent Privacy) 64-bit encryption**. Enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).
   - **WEP (Wired Equivalent Privacy) 128-bit encryption**. Enter 26 hexadecimal digits (any combination of 0–9, a–f, or A–F).
6. Enter the encryption keys. You can manually or automatically program the four data encryption keys. These values must be identical on all computers and Access Points in your network:
   - **Passphrase**. To use a passphrase to generate the keys, enter a passphrase, and click **Generate**. This automatically creates the keys. Wireless stations must use the passphrase or keys to access the router.

> **Note:** Not all wireless adapters support passphrase key generation.

   - **Key 1-Key4**. These values are *not* case-sensitive. You can manually enter the four data encryption keys. These values must be identical on all computers and access points in your network. Enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).
7. Select which of the four keys will be the default.

   Data transmissions are always encrypted using the default key. The other keys can be used only to decrypt received data. The four entries are disabled if WPA-PSK or WPA authentication is selected.
8. Click **Apply** to save your settings.

Configuring WPA, WPA2, or WPA + WPA2

Both WPA and WPA2 provide strong data security. WPA with TKIP is a software implementation that can be used on Windows systems with Service Pack 2 or later; WPA2 with AES is a hardware implementation; see your device documentation before implementing it. Consult the product documentation for your wireless adapter for instructions for configuring WPA settings.

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

To configure WPA or WPA2 in the router:

1. Log in to the router as described in *"Logging In to Your Router"* on page 10.
2. Select Wireless Settings from the main menu.
3. On the Wireless Setting screen, select the radio button for the WPA or WPA2 option of your choice.
4. The settings displayed on the screen depend on which security option you select.
5. For WPA-PSK or WPA2-PSK, enter the passphrase.
6. If prompted, enter the settings for the Radius server. For WPA-802.1x or WPA2-802.1x, these settings are required for communication with the primary Radius server.
   - **Primary Radius Server IP Address**. The IP address of the Radius server. The default is 0.0.0.0
   - **Radius Port**. Port number of the Radius server. The default is 1812.
   - **Shared Key**. This is shared between the wireless access point and the Radius server during authentication.
7. To save your settings, click **Apply**.

Using Push 'N' Connect (WPS) to Configure Your Wireless Network

To use Push 'N' Connect, your wireless computers or devices must support Wi-Fi Protected Setup (WPS). Compatible equipment usually has the  WPS symbol on it. WPS can configure the network name (SSID) and set up WPA/WPA2 wireless security for the router and the wireless computer or device at the same time.

Some considerations regarding WPS are:

- NETGEAR's Push 'N' Connect feature is based on the WPS standard. All other Wi-Fi-certified and WPS-capable products should be compatible with NETGEAR products that implement Push 'N' Connect.
- If your wireless network will include a combination of WPS capable devices and non-WPS capable devices, NETGEAR suggests that you set up your wireless network and security settings manually first, and use WPS only for adding WPS capable devices.

You can connect to the network using WPS either with a push button or a PIN.

- **Push Button**. This is the preferred method. See the following section, WPS Button.
- **Entering a PIN**. See *"WPS PIN Entry"* on page 24.

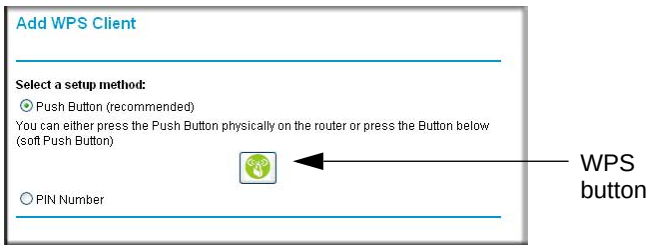
WPS Button

Any wireless computer or wireless adapter that will connect to the router wirelessly is a client. The client must support a WPS button, and must have a WPS configuration utility, such as the NETGEAR Smart Wizard or Atheros Jumpstart.

To use the router WPS button to add a WPS client:

1. Log in to the router as described in *"Logging In to Your Router"* on page 10.
2. On the router main menu, select Add a WPS Client, and then click **Next**.

   By default, the **Push Button (recommended)** radio button is selected.



3. Either click the onscreen button or press the WPS button on the front of the router.

   The router tries to communicate with the client (the computer that wants to join the network) for 2 minutes.

4. Go to the client wireless computer, and run a WPS configuration utility. Follow the utility's instructions to click a WPS button.
5. Go back to the router screen to check for a message.

   The router WPS screen displays a message confirming that the client was added to the wireless network. The router generates an SSID, and implements WPA/WPA2 wireless security. The router will keep these wireless settings unless you change them, or you clear the **Keep Existing Wireless Settings** check box in the WPS Settings screen.

6. Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wireless Settings screen. See *"Manually Configuring Your Wireless Settings"* on page 18.

To access the Internet from any computer connected to your router, launch a browser such as Microsoft Internet Explorer or Mozilla Firefox. You should see the router's Internet LED blink, indicating communication to the ISP.

Note: If no WPS-capable client devices are located during the 2-minute time frame, the SSID will not be changed, and no security will be implemented on the router.

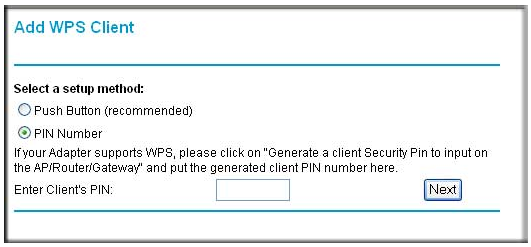
WPS PIN Entry

Any wireless computer or device that will connect to the router wirelessly is a client. The client must support a WPS PIN, and must have a WPS configuration utility, such as the NETGEAR Smart Wizard or Atheros Jumpstart.

The first time you add a WPS client, make sure that the **Keep Existing Wireless Settings** checkbox on the WPS Settings screen is cleared. This is the default setting for the router, and allows it to generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the router automatically selects this checkbox so that your SSID and wireless security settings stay the same if other WPS devices are added later.

To use a PIN to add a WPS client:

1. Log in to the router as described in *"Logging In to Your Router"* on page 10.
2. On the router main menu, select Add a WPS Client (computers that will connect wirelessly to the router are clients), and then click **Next**. The Add WPS Client screen displays:



3. Select the **PIN Number** radio button.
4. Go to the client wireless computer. Run a WPS configuration utility. Follow the utility's instructions to generate a PIN. Take note of the client PIN.
5. From the router Add WPS Client screen, enter the client PIN number, and then click **Next**.
   - The router tries to communicate with the client for 4 minutes.
   - The router WPS screen confirms that the client was added to the wireless network. The router generates an SSID, and implements WPA/WPA2 wireless security.
6. Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wireless Settings screen. See *"Manually Configuring Your Wireless Settings"* on page 18

To access the Internet from any computer connected to your router, launch a browser such as Microsoft Internet Explorer or Mozilla Firefox. You should see the router's Internet LED blink, indicating communication to the ISP.

Note: If no WPS-capable client devices are located during the 2-minute time frame, the SSID will not be changed and no security will be

implemented on the router.

Adding Wireless Computers that Do Not Support WPS

If you set up your network with WPS, and now you want to add a computer that does not support WPS, you must manually configure that computer. To view the wireless settings for the router, see *"Manually Configuring Your Wireless Settings"* on page 18.

Because WPA randomly creates the SSID and WPA/WPA2 keys, they might be difficult to type or remember (that is one reason why the network is so secure). You can change the wireless settings so that they are easier for you to remember. If you do that, then you will need to set up the WPS-compatible computers again.

Changing Wireless Settings for the Network:

Note: Making these changes will cause all wireless computers to be disconnected from network. You will then have to set them up with the new wireless settings.

1. Use an Ethernet cable to connect a computer to the router. That way you will not get disconnected when you change the wireless settings.
2. Log in to the router and select Wireless Settings (see *"Manually Configuring Your Wireless Settings"* on page 18).
3. Make the following changes:
   - Change the Wireless Network Name (SSID) to a meaningful name.
   - On the WPA/PSK + WPA2/PSK screen, select a passphrase.
   - Make sure that the **Keep Wireless Settings** checkbox is selected in the WPS Settings screen so that your new settings will not be erased if you use WPS.
4. Click **Apply** so that your changes take effect. Write down your settings.

   All existing wireless clients are disassociated and disconnected from the router.
5. For the non-WPS devices that you want to connect, open the networking utility and follow the utility's instructions to enter the security settings that you selected in Step 2 (the SSID, WPA/PSK + WPA2/PSK security method, and passphrase).
6. For the WPS devices that you want to connect, follow the procedure *"WPS Button"* on page 23 or *"WPS PIN Entry"* on page 24.

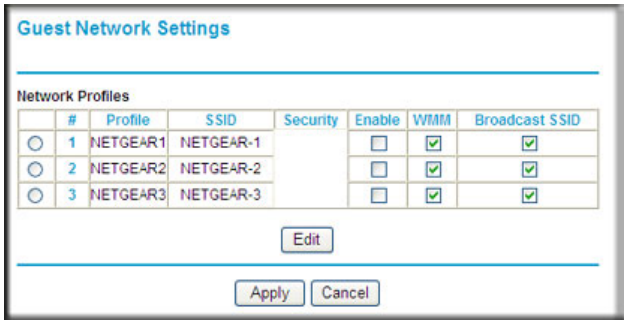
   The settings that you configured in Step 2 are broadcast to the WPS devices so that they can connect to the router.

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 configure a wireless guest network:

1. In the main menu, under Setup, select Wireless Guest Network:



2. Select the radio button for the network profile that you want to set up.
3. You can specify the SSID, Security, WMM, and whether the SSID broadcast is enabled.
   - NETGEAR 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.
   - Wireless security is disabled by default. NETGEAR strongly recommends that you implement wireless security for the guest network.
4. To configure wireless security for the guest network, enter the security options. For more information, see *"Manually Configuring Your Wireless Settings"* on page 18.
5. When you have finished making changes, click **Apply**.

Protecting Your Network

3

This chapter describes how to use the basic firewall features of the router to protect your network.

> **Note:** For information about the advanced content filtering features port forwarding and port triggering, see *"Port Forwarding and Port Triggering"* on page 51.

Protecting Access to Your Mobile Broadband 11n Wireless Router

For security reasons, the router has its own user name and password. Also, after a period of inactivity, the login automatically disconnects. The user name and password are not the same as a user name or password you 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 upper and lower case letters, numbers, and symbols. Your password can be up to 30 characters.

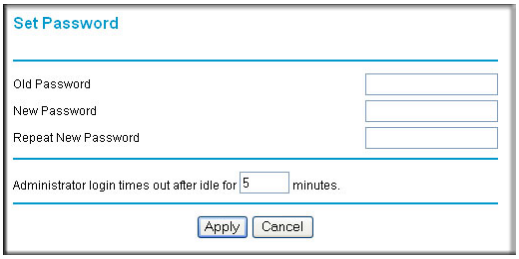
Changing the Built-In Password

1. To log in to the router, type **http://www.routerlogin.net** in the address field of your Internet browser. Enter **admin** for the user name and your password (or the default, **password**).

> **Note:** If you changed the password and do not remember what it is, you can reset the router to its factory default settings. See *"Restoring the*

Default Configuration and Password” on page 73.

2. From the main menu, under the Maintenance heading, select Set Password:



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

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

Changing the Administrator Login Time-out

For security, the administrator login to the 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.

Blocking Sites and Keywords

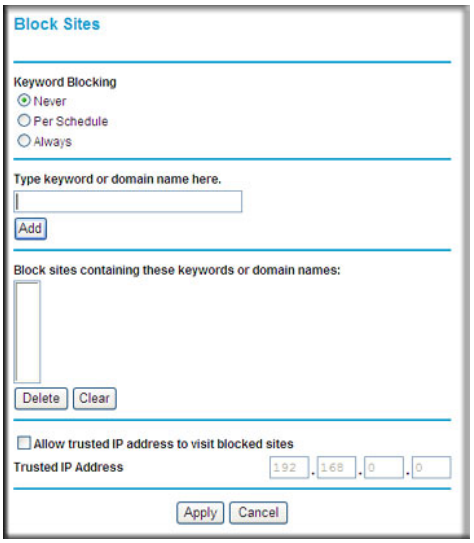
The router provides a variety of options for blocking Internet-based content and communications services. With its content filtering feature, the router prevents objectionable content from reaching your PCs. You can control access to Internet content by screening for keywords within Web addresses. Content 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. 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.

The router allows you to restrict access to Internet content based on Web addresses and Web address keywords.

1. Log in to the router as described in *"Logging In to Your Router"* on page 10.
2. On the main menu, select Block Sites to display the Block Sites screen:



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

   Some examples of keyword applications are shown in the following chart.

Keyword	Result
XXX	Block the URL http://www.badstuf.com/xxx.html.
.com	Only websites with other domain suffixes (such as .edu or .gov) can be viewed.
. (a period)	Block all Internet browsing access.

Up to 32 entries are supported in the Keyword list.

Note: If you block sites, you can set up the router to log attempts to access them. See *"Viewing, Selecting, and Saving Logged Information"* on page 41.

5. To delete a keyword or domain, select it from the list, click **Delete Keyword**, and then click **Apply**.
6. To specify a trusted user, enter that computer's IP address in the **Trusted IP Address** field, and then 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.
7. Click **Apply** to save your settings.

Blocking Services

To block keywords and sites:

1. Log in to the router as described in *"Logging In to Your Router"* on page 10.
2. In the main menu, under Content Filtering, select Block Services to display this screen:

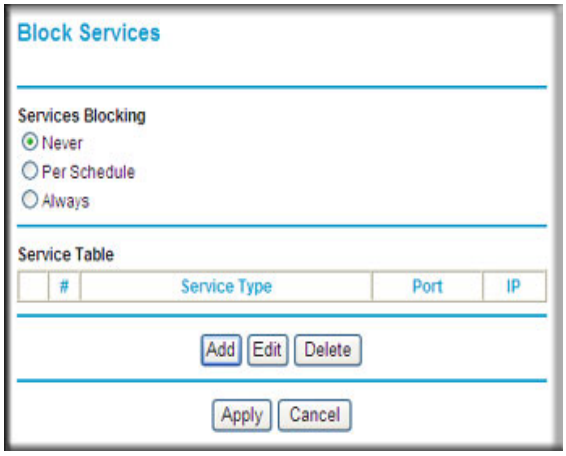
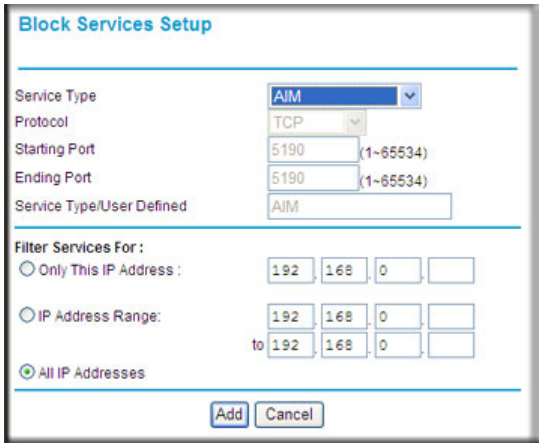


Figure 3-2

3. 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.

4. Click **Add** and the following screen displays:



5. Either select a service from the Service Type drop-down list, or use the **Service/Type User Defined** field to create a custom service.
6. Click **Add** to create the service, and it will be listed in the Service Table on the Block Services screen.
7. Click **Apply** to save your settings.

Scheduling

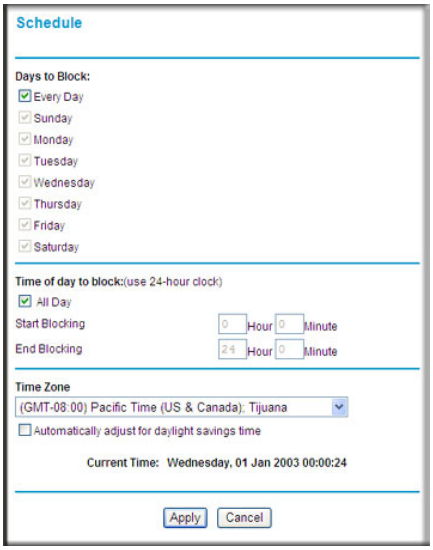
The router uses network time protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet.

Setting Your Time Zone

To localize the time for your log entries, you must specify your time zone:

1. Log in to the router as described in *"Logging In to Your Router"* on page 10.

2. On the main menu below Content Filtering, select Schedule:



3. Select your time zone. This setting will be used for the blocking schedule according to your local time zone and for time-stamping log entries.

   If your time zone is currently in daylight savings time, select the **Automatically adjust for daylight savings time** check box.

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

Scheduling Firewall Services

If you enabled services blocking in the Block Services screen or port forwarding in the Ports screen, you can set up a schedule for when blocking occurs or when access is not restricted.

1. Log in to the router as described in *"Logging In to Your Router"* on page 10.
2. On the main menu, select the Schedule. The Schedule screen appears.
3. To block Internet services based on a schedule, select **Every Day** or select one or more days. 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, fill in the **Start Blocking** and **End Blocking** fields.
4. 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.
5. Click **Apply** to save your changes.

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 is an excellent solution for keeping your family safe online, but like all Web filtering tools, it isn't perfect. NETGEAR reminds you there's 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 Web sites requesting personal or financial information.

To download **Live Parental Controls**, click the Live Parental Controls link on the router menu to go to the website: *http://www.netgear.com/lpc.*

Web-based GUI

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 thru the router. It not only protects 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 may have your own computer or you may be sharing a computer with other members in the family. Default and per-user settings allow customizable configurations for different computing arrangement and personalize the settings for each person. Per-time setting allows Internet access during scheduled time slots, to help manage work/play balance.

Minimal software installation

Installation requires a one-time installation of the Management Utility. 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

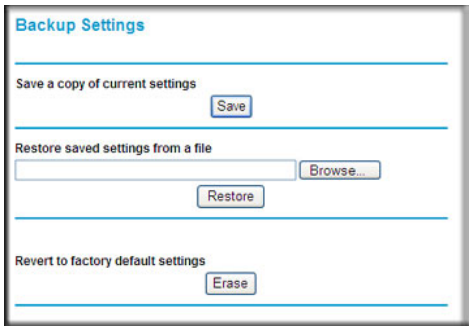
This chapter describes how to perform network management tasks with your Mobile Broadband 11n Wireless Router.

Backing Up, Restoring, or Erasing Your Settings

The configuration settings of the router are stored in a configuration file in the router. This file can be backed up to your computer, restored, or reverted to factory default settings. The procedures below explain how to do these tasks.

Backing Up the Configuration to a File

1. Log in to the router. Type **http://www.routerlogin.net** in the address field of your Internet browser. Enter **admin** for the user name and your password (or the default, **password**).
2. Under the Maintenance heading on the main menu, select Backup Settings to display the Backup Settings screen:



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

Restoring the Configuration from a File

To restore the configuration:

1. Log in to the router. Type **http://www.routerlogin.net** in the address field of your Internet browser. Enter **admin** for the user name and your password (or the default, **password**).
2. Under the Maintenance heading on the main menu, select Backup Settings.
3. Enter the full path to the file on your network, or click **Browse** to locate the file.
4. When you have located the .cfg file, click **Restore** to upload the file to the router.
5. The router reboots.

Erasing the Configuration

You can use the Erase feature to erase its configuration settings and restore the router to the factory default settings.

To erase the configuration:

1. Under the Maintenance heading on the main menu select, Backup Settings.
2. Click **Erase**.
3. The router reboots.

   After an erase, the router password is **password**, the LAN IP address is **192.168.0.1**, and the router 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 router for 6 seconds.

Upgrading the Router Firmware

The router firmware is stored in flash memory, and can be upgraded as new firmware is released by NETGEAR. Upgrade files can be downloaded from the NETGEAR website. If the upgrade file is compressed (a .zip file), you must first extract the binary (.bin or .img) file before uploading it to the router.

NETGEAR recommends that you back up your configuration before doing a firmware upgrade. After the upgrade is complete, you might need to restore your configuration settings.

1. Download and unzip the new firmware file from NETGEAR.

The Web browser used to upload new firmware into the router must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer 5.0 or newer, or Mozilla Firefox 2.0 or newer.

2. Log in to the router. Type **http://www.routerlogin.net** in the address field of your Internet browser. Enter **admin** for the user name and your password (or the default, **password**).
3. From the main menu, under the Maintenance heading, select Router Upgrade to display this screen:

4. Click **Browse** to locate the binary (.bin or .img) upgrade file.
5. Click **Upload**.

WARNING!

When uploading firmware to the 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 might corrupt the firmware, causing router to be unworkable and inaccessible. When the upload is complete, your router will automatically restart. The upgrade process typically takes about 1 minute. In some cases, you might need to clear the configuration and reconfigure the router after upgrading.

Router Status

From the main menu, below the Maintenance heading, select Router Status to view this screen.

You can use this screen to view the status of the router, to show statistics, or to view the connection status.

- For information about the fields on this screen, see Table 4.
- See *"Showing Statistics"* on page 39 for information about statistics.
- For information about the Internet connection, see *"Connection Status"* on page 40

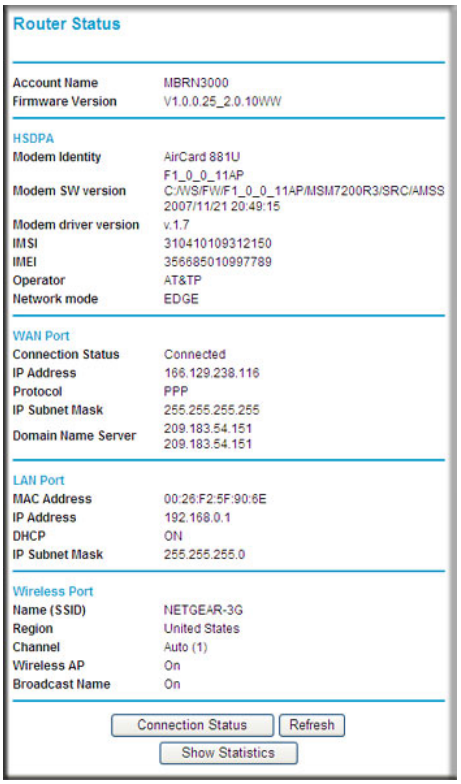


Table 4. Router Status Fields

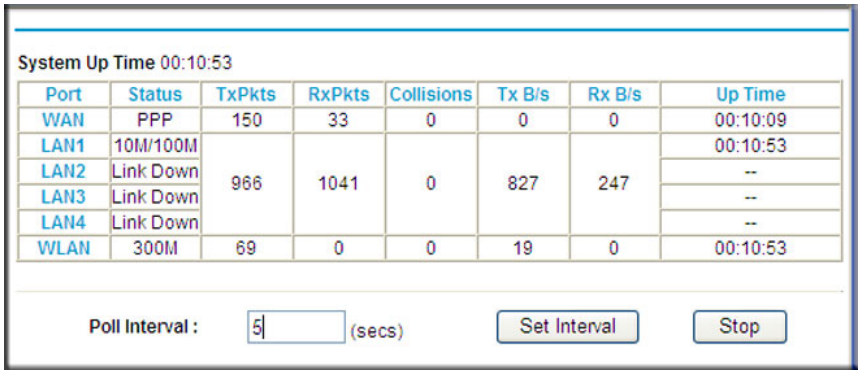
Field		Description
Firmware Version		This field displays the router firmware version.
HSDPA (High-Speed Downlink Packet Access)	Modem Identity	Shows the modem in use.
	Modem sw version	The software version of the modem.
	Modem driver version	The driver version of the modem.
	IMSI	International Mobile Subscriber Identity. SIM card identity.
	IMEI	International Mobile Equipment Identity. Unique identity of the modem.
	Operator	The ISP for the broadband wireless network.
	Network mode	The mode of the current network the modem is connected to. This is dependent on coverage and distance from the cell site.

Table 4. Router Status Fields (Continued)

Field		Description
WAN Port	Connection Status	The status of the Internet connection.
	IP Address	The IP address used by the modem. If no address is shown, the router cannot connect to the Internet.
	Protocol	The protocol for the Internet connection, which is PPP (Point-to-Point).
	IP Subnet Mask	The IP subnet mask used by the router's USB port.
	Gateway IP Address	The IP address used by the router.
	Domain Name Server	The DNS server IP addresses used by the router. These addresses are usually obtained dynamically from the ISP.
LAN Port	MAC Address	The Ethernet MAC address used by the router's LAN port.
	IP Address	The LAN port IP address. The default is 192.168.0.1.
	DHCP	• **Off:** The router will not assign IP addresses to PCs on the LAN. • **On:** The router assigns IP addresses to PCs on the LAN.
	IP Subnet Mask	The LAN port IP subnet mask. The default is 255.255.255.0.
Wireless Port (See *"Manually Configuring Your Wireless Settings"* on page 18.	Name (SSID)	The service set ID, also known as the wireless network name.
	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 disabled or not. If not enabled, the Wireless LED on the front panel will be off.
	Broadcast Name	Indicates if the router is configured to broadcast its SSID.

Showing Statistics

Click the **Show Statistics** button on the Router Status screen to display router usage statistics:



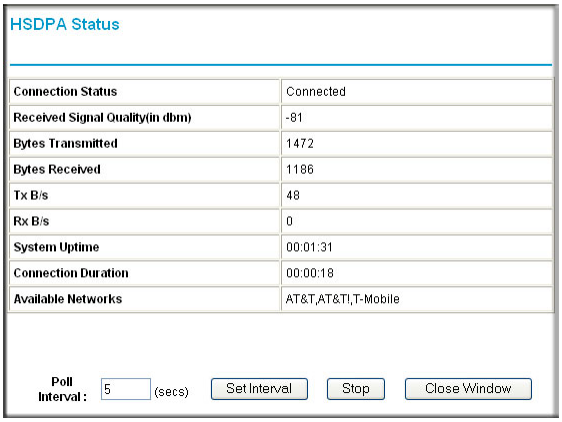
This following table explains the statistic fields.

Table 5. Router Statistics Fields

Field	Description
Status	The link status. Note that LAN2, LAN3, and LAN4 are guest networks.
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 average egress line utilization for this port.
Rx B/s	The average ingress line utilization for this port.
Up Time	The time elapsed since the last power cycle or reset.

Connection Status

Click the **Connection Status** button on the Router Status screen:



This screen shows the following statistics:

Table 6. Connection Status Fields for HSDPA Status

Field	Description
Connection Status	The status of the Internet connection. • **Scanning**. The modem is scanning for broadband wireless networks in your area. • **Connected**. The router is connected to the Internet. • **No USB Device Attached**. The router does not detect a USB modem connected to its USB port. Either the modem is disconnected, or it is not correctly seated. To correct the problem remove the modem and reinsert it into the port.
Received Signal Quality (in dbm)	Modem radio reception. A small, negative number indicates good signal quality.
Bytes Transmitted	The number of bytes transmitted in the most recent connection session.
Bytes Received	The number of bytes received in the most recent connection session.
Tx B/s	The transmission rate.
Rx B/s	The receiving rate.
System Uptime	Time elapsed since the last reboot.
Connection Duration	The time elapsed since the most recent connection to the Internet.
Available Networks	The broadband wireless networks available in your area.

Viewing Attached Devices

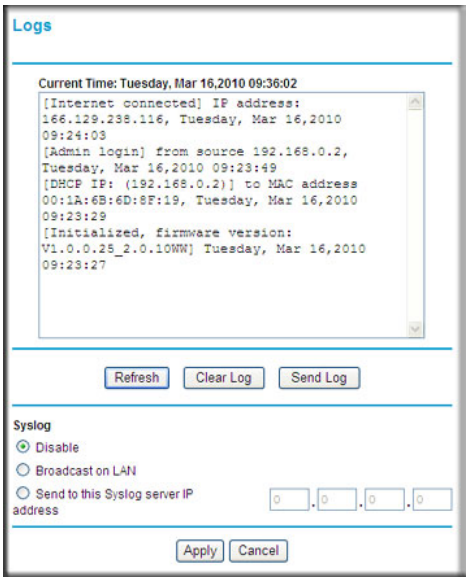
The Attached Devices screen shows all IP devices that the router discovered on the local network. From the main menu, under the Maintenance heading, select Attached Devices:

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

Viewing, Selecting, and Saving Logged Information

The router logs security-related events such as denied incoming service requests, hacker probes, and administrator logins. If you enabled content filtering in the Block Sites screen, the Logs screen can show you when someone on your network tries to access a blocked site.

On the router menu, below the Content Filtering heading, select Logs to display this screen:



Note: You can enable e-mail notification to receive these logs in an e-mail message. See *"Enabling Security Event E-mail Notification"* on page 44.

Log entries and action buttons are described in the following table.

Table 7. Security Log Entry and Button Descriptions

Field	Description
Current 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.
Button	**Description**
Refresh	Refresh the log screen.
Clear Log	Clear the log entries.
Send Log	Email the log immediately.

Table 7. Security Log Entry and Button Descriptions (Continued)

Field	Description
Apply	Apply the current settings.
Cancel	Clear the current settings.

Selecting Which Information to Log

Besides the standard information listed previously, you can choose to log additional information. Those optional selections are as follows:

- Attempted access to blocked site
- Connections to the router menu
- Router operation (start up, get time, and so on)
- Known DoS attacks and port scans

Saving Log Files on a Server

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

Examples of Log Messages

Following are examples of log messages. In all cases, the log entry shows the timestamp as: Day, Year-Month-Date Hour:Minute:Second.

Activation and Administration

```
Tue, 2002-05-21 18:48:39 - NETGEAR activated
```

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

```
Tue, 2002-05-21 18:55:00 - Administrator login successful - IP:192.168.0.2
Thu, 2002-05-21 18:56:58 - Administrator logout - IP:192.168.0.2
```

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

```
Tue, 2002-05-21 19:00:06 - Login screen timed out - IP:192.168.0.2
```

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

```
Wed, 2002-05-22 22:00:19 - Log emailed
```

[This entry shows when the log was e-mailed.]

Dropped Packets

```
Wed, 2002-05-22 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, 2002-05-22 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, 2002-05-22 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, User Datagram Protocol (UDP) packet (port 6970), and 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.

Enabling Security Event E-mail Notification

To set up the router so that you can receive logs and alerts by e-mail, select Email from the router menu to display the following screen:

To receive alerts and logs by e-mail:

1. Select the **Turn E-mail Notification On** check box.
2. Fill in the fields to send alerts and logs through email.
   - **Your Outgoing Mail Server**. Enter the name or IP address of the outgoing SMTP mail server of your ISP (such as mail.myISP.com).
   - **Send to This E-mail Address.** Enter the e-mail address where you want to send the alerts and logs. Use a full e-mail address, such as ChrisXY@myISP.com.
   - **My mail server requires authentication**. Select this check box if you need to log in to your SMTP server to send E-mail. If you select this feature, you must enter the user name and password for the mail server.

Tip: If you cannot remember this information, check the settings in your email program.

3. Specify when you want the alerts and logs to be sent:
   - **Send alert immediately**. Select the corresponding 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.

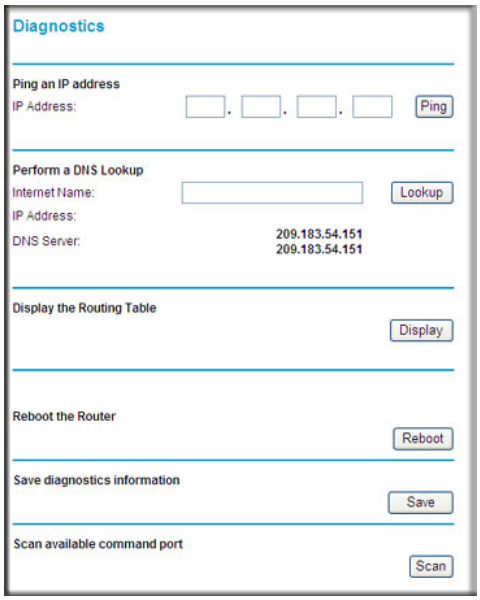
   If the **Weekly**, **Daily**, or **Hourly** option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, it is cleared from the router's memory. If the router cannot e-mail the log file, the log buffer might fill up. In this case, the router overwrites the log and discards its contents.
4. Click **Apply** so that your changes take effect.

Running Diagnostic Utilities and Rebooting the Router

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

- Ping an IP address to test connectivity to see if you can reach a remote host. If Ping VPN is enabled, the ping packet always goes through the VPN if the VPN tunnel is enabled and working.
- 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 routers the router is communicating with.
- Reboot the router to enable new network configurations to take effect or to clear problems with the router's network connection.

From the main menu, under the Maintenance heading, select Diagnostics:



- **Ping**: Ping an IP address.
- **Lookup**: A DNS (Domain Name Server) converts the Internet name such as www.netgear.com to an IP address. If you need the IP address of a server on the Internet, you can do a DNS lookup to find the IP address.
- **Display**: View the internal routing table. Typically, this information is used only by Technical Support.
- **Reboot**: Shut down and restart the router.

> **Note:** If you reboot the router you will lose your connection. To access the router you will need to log in again after it has finished rebooting.

- **Save**: Save diagnostic information.
- **Scan**:

Enabling 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 router.

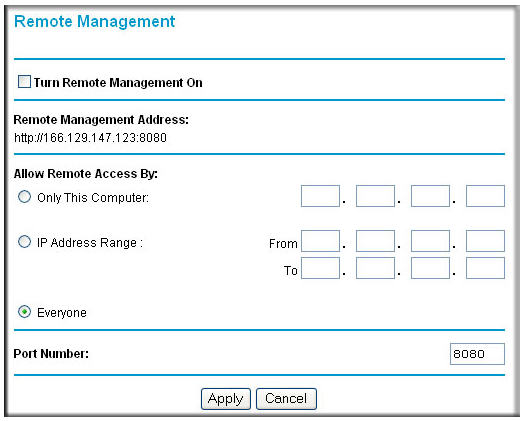
Tip: Be sure to change the router default password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper-case and lower-case), numbers, and symbols. Your password can be up to 30 characters.

Configuring Remote Management

1. Log in to the router. Type **http://www.routerlogin.net** in the address field of your Internet browser. Enter **admin** for the user name and your password (or the default, **password**).
2. Under the Advanced heading, select Remote Management:
3. Select the **Turn Remote Management On** checkbox.
4. Specify which external addresses will be allowed to access the router's remote management.

   For security, restrict access to as few external IP addresses as practical:

   - To allow access from any IP address on the Internet, select **Everyone**.
   - To allow access from a range of IP addresses on the Internet, select **IP address range**. Enter a beginning and ending IP address to define the allowed range.
   - To allow access from a single IP address on the Internet, select **Only This Computer**. Enter the IP address that will be allowed access.



5. Specify the port number that will be used for accessing the router menu.

   Access normally uses the standard HTTP service port 80. For greater security, you can enter a different port number. 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.

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

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

   http://134.177.0.123:8080

Note: In this case, you must include http:// in the address.

Advanced

5

This chapter describes how to configure the advanced features of your Mobile Broadband 11n Wireless Router.

Advanced Wireless Settings

From the main menu, select Advanced Wireless Settings to display the following screen:

Table 8. Advanced Wireless Settings

Field	Description
Enable Wireless Access Point	Selected by default, this setting enables the wireless radio, which allows the router to work as a wireless access point. Turning off the wireless radio can be helpful for configuration, network tuning, or troubleshooting.

Table 8. Advanced Wireless Settings (Continued)

Field	Description
Allow Broadcast Name (SSID)	Selected by default, the router broadcasts its SSID, allowing wireless stations that have a null (blank) SSID to adopt the correct SSID. If you disable broadcast of the SSID, only devices with the correct SSID can connect. This nullifies the wireless network discovery feature of products such as Windows XP, but the data is still exposed to equipment like wireless sniffers. For this reason NETGEAR recommends that you also enable wireless security.
Fragmentation Length, CTS/RTS Threshold, and Preamble Mode	These should be left at their default settings.
Router PIN	The PIN number used for Push 'N' Connect.
Disable Router PIN	By default, this check box is cleared. This allows the WPS clients to discover the router's PIN.
Keep Wireless Settings	By default, this check box is cleared. This allows the router to automatically generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the router automatically selects the **Keep Existing Wireless Settings** check box so that your SSID and wireless security settings remain the same if other WPS-enabled devices are added later.
Turn Access Control On	Access control is disabled by default so that any computer configured with the correct SSID can connect. See Restricting Access by MAC Address.

Wireless Station Access Control

By default, any wireless PC that is configured with the correct SSID and wireless security settings is allowed access to your wireless network. You can use Wireless Access Point settings in the Wireless Setting screen to further restrict wireless access to your network:

- **Turning off wireless connectivity completely**.
  You can completely turn off the wireless portion of the router. For example, if you use your notebook computer to wirelessly connect to your router, and you take a business trip, you can turn off the wireless portion of the router while you are traveling. Other members of your household who use computers connected to the router via Ethernet cables can still use the router. To do this, clear the **Enable Wireless Access Point** check box on the Wireless Settings screen, and then click **Apply**.
- **Hiding your wireless network name (SSID)**.
  By default, the 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 router. You must configure your wireless devices to match the wireless network name (SSID) of the router.

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

Restricting Access by MAC Address

For increased security, you can restrict access to the wireless network to allow only specific PCs based on their MAC addresses. You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the Mobile Broadband 11n Wireless Router. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.

To restrict access based on MAC addresses:

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

1. From the main menu, select Wireless Settings, and then click **Setup Access List** to display the Wireless Station Access List screen.

2. Adjust the list as needed for your network. You can add devices to the Trusted Wireless Stations list. Click **A**dd to display the following screen:

3. You can add devices to the list using either of the following methods:
   - If the computer is in the Available Wireless Cards table, select its radio button to capture its MAC address.
   - Use the Wireless Card Entry fields to enter the MAC address of the device to be added. The MAC address can usually be found on the bottom of the wireless device.

Note: If no device name appears when you enter the MAC address, you can type a descriptive name for the computer that you are adding.

4. Click **Apply** to save these settings. Now, only devices on this list will be allowed to wirelessly connect to the router.

Port Forwarding and Port Triggering

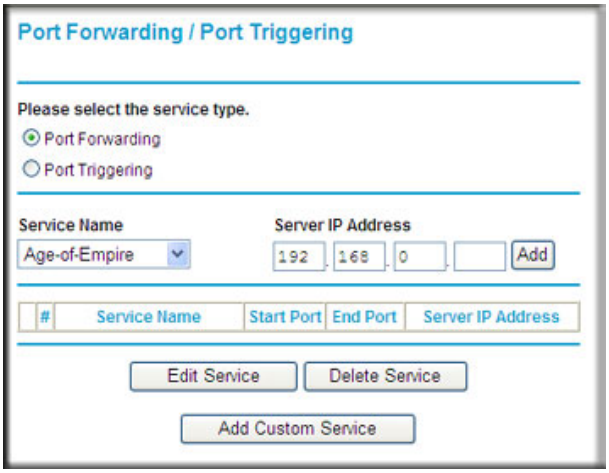
Port forwarding and port triggering are advanced features that affect the behavior of the firewall in your router. In the Port Forwarding / Port Triggering screen, you can make local computers or servers available to the Internet for different services (for example, FTP or HTTP), to play Internet games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

- Port 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 proper server.
- 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

To set up port forwarding:

1. From the main menu, under the Advanced Heading, select Port Forwarding/Port Triggering. The following screen displays:



By default, the **Port Forwarding** radio button is selected.

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 appears 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:

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

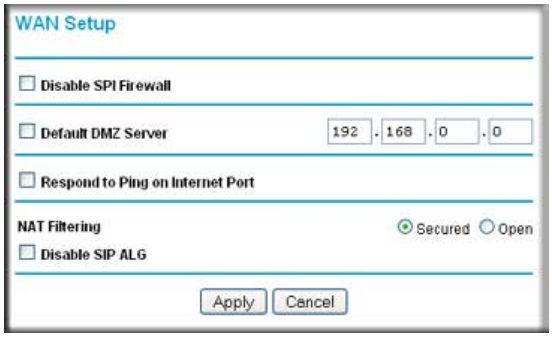
   The service appears in the list. For more detailed information, see the Port Forwarding/Port Triggering help.

WAN Setup

Note: To change broadband Internet connection settings, use the Broadband Settings screen, as described in *"Manually Configuring Your Internet Settings"* on page 12.

To view or change the WAN Setup:

1. From the main menu, select WAN Setup to display the WAN Setup screen:



2. Make the changes that you want, and then click **Apply** to save the settings.

The WAN Setup fields are described in the following table:

Table 9. WAN Setup Settings

Setting	Description
Disable SPI Firewall	This check box is usually clear so that the firewall protects your LAN against port scans and denial of service (DOS) attacks. This check box should be selected only in special circumstances.
Default DMZ Server	This feature is sometimes helpful when you are using some online games and videoconferencing. Be careful when using this feature because it makes the firewall security less effective. See *"Setting Up a Default DMZ Server"* on page 53.
Respond to Ping on Internet WAN Port	If you want the router to respond to a ping from the Internet, select this check box. This should be used only as a diagnostic tool, since it allows your router to be discovered. Do not select this check box unless you have a specific reason to do so.
NAT Filtering, Disable SIP Alg	

Setting Up a Default DMZ Server

WARNING!

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.

The default DMZ server feature is helpful when you are using some online games and videoconferencing applications that are incompatible with NAT. The router is programmed to recognize some of these applications and to work properly with them, but there are other

applications that may not function well. In some cases, one local computer can run the application properly if that computer's IP address is entered as the default DMZ server.

Incoming traffic from the Internet is normally discarded by the router unless the traffic is a response to one of your local computers or a service that you have configured in the Ports 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. Go to the WAN Setup screen as described in the previous section.
2. Select the **Default DMZ Server** check box.
3. Type the IP address for that server.
4. Click **Apply** to save your changes.

LAN IP Settings

The LAN IP Setup screen allows configuration of LAN IP services such as DHCP and RIP. These features can be found under the Advanced heading in the router main menu.

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

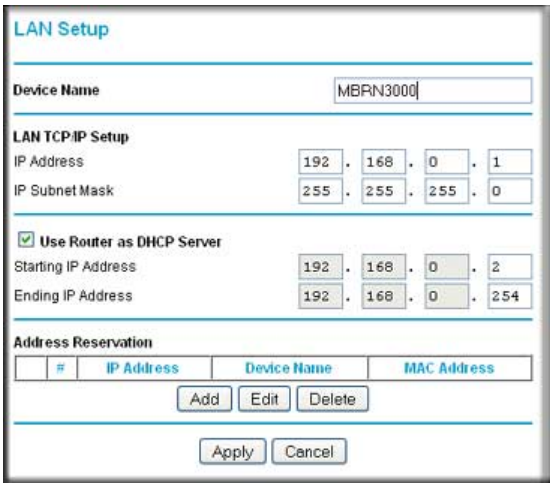
- LAN IP addresses: 192.168.0.1
- Subnet mask: 255.255.255.0

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 in this screen.

To view or change the LAN IP Setup:

Tip: If you change the LAN IP address of the router while connected through the browser, you will be disconnected and so will others connected to the router. To connect to the router, you must open a new connection to the new IP address and log in again. Others using the router must restart their computers to connect to the router again.

1. Select LAN IP to display the LAN Setup screen:



2. Change the settings. For more information, see Table 10, *"DHCP Settings"* on page 56 or *"Reserved IP Addresses"* on page 56.
3. Click **Apply** to save the changes.

The LAN TCP/IP Setup parameters are explained in the following table.

Table 10. LAN IP Setup

Settings		Description
Device Name		
LAN TCP/IP Setup	IP Address	The LAN IP address of the router.
	IP Subnet Mask	The LAN subnet mask of the router. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.
DHCP Server For more information, see *"DHCP Settings"* on page 56.	Use Router as a DHCP Server	This check box is usually selected so that the router functions as a Dynamic Host Configuration Protocol (DHCP) server. See *"DHCP Settings"* on page 56.
	Starting IP Address	Specify the start of the range for the pool of IP addresses in the same subnet as the router.
	Ending IP Address	Specify the end of the range for the pool of IP addresses in the same subnet as the router.
Address Reservation For more information, see *"DHCP Settings"* on page 56.		When you specify a reserved IP address for a computer on the LAN, that computer receives the same IP address each time it access the router's DHCP server. Assign reserved IP addresses to servers that require permanent IP settings.

DHCP Settings

By default, the 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 router's LAN. The assigned default gateway address is the LAN address of the router. IP addresses is assigned to the attached PCs 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. See the online document listed in "Internet Networking and TCP/IP Addressing:" in Appendix B for an explanation of DHCP and information about how to assign IP addresses for your network.

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 on the LAN IP Setup screen. Otherwise, leave it selected.

Specify the pool of IP addresses to be assigned by filling in the **Starting IP Address** and **Ending IP Address** fields. 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 parameters to any LAN device that requests DHCP:

- An IP address from the range you have defined.
- Subnet mask.
- Gateway IP Address 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 (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 address of Windows PCs 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 PCs to browse the network using the Network Neighborhood feature of Windows.

Reserved IP Addresses

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

To reserve an IP address:

1. 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 on your network, it is listed on the same page for your convenience. Clicking the radio button for each entry in the attached device list fills in the fields automatically with the computer's MAC address and name.

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. Click the button next to the reserved address you want to edit or delete.
2. Click **Edit** or **Delete**.

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 to register your domain to their IP address, and forward traffic directed at your domain to your frequently changing IP address.

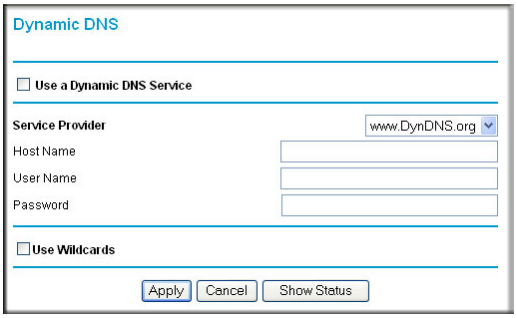
The router contains a client that can connect to a Dynamic DNS service provider. To use this feature, you must select a service provider and obtain an account with them. After you have configured your account information in the router, whenever your ISP-assigned IP address changes, your router will automatically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

Configuring Dynamic DNS

WARNING!

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 will not be routed on the Internet.

1. From the main menu, select Dynamic DNS to display the Dynamic DNS screen:



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. Fill in the **Host Name**, **User Name**, and **Password** fields.

   The dynamic DNS service provider may call the host name a domain name. If your URL is myName.dyndns.org, then your host name is myName. The password can be a key for your dynamic DNS account.

6. 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 will cause *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org.

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

Using 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 must 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 is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the 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.

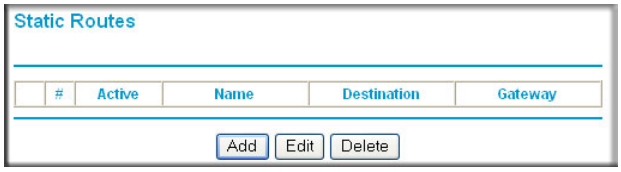
In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100.

In this example:

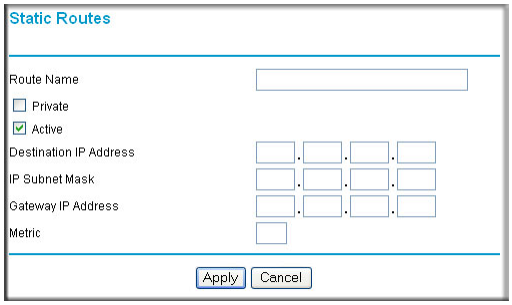
- The **Destination IP Address** and **IP Subnet Mask** fields specify that this static route applies to all 134.177.x.x addresses.
- The **Gateway IP Address** fields specify that all traffic for these addresses should be forwarded to the ISDN router at 192.168.0.100.
- In the **Metric** field, a value of 1 will work since the ISDN router is on the LAN. This represents the number of routers between your network and the destination. This is a direct connection, so it is set to 1.
- **Private** is selected only as a precautionary security measure in case RIP is activated.

To configure static routes:

1. From the main menu, under the Advanced heading, select Static Routes to view the Static Routes screen:



2. Click **Add** or **Edit** to display the following screen:

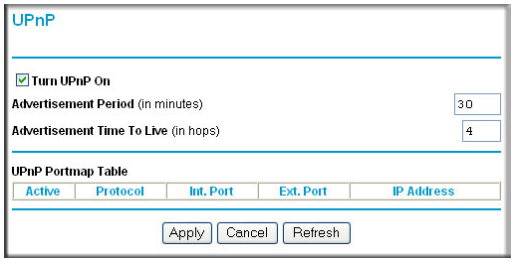


3. Fill in or change the fields:
   - **Route Name.** The route name is for identification purposes only.
   - **Private**. Select this check box if you want to limit access to the LAN only. The static route will not be reported in RIP.
   - **Active**. Select this check box to make this route effective.
   - **Destination IP Address**, and **IP Subnet Mask**. If the destination is a single host, type a subnet value of **255.255.255.255**.
   - **Gateway IP Address**. This must be a router on the same LAN segment as the router.
   - **Metric**. Type a number between 2 and 15. This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 2.
4. Click **Apply** to either save your changes. If you added a static route, it is added to the Static Routes screen.

Universal Plug and Play (UPnP)

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.

1. Select UPnP on the main menu to display the UPnP screen:



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 disabled, the router will not allow any

device to automatically control the resources, such as port forwarding (mapping), of the router.

- **Advertisement Period**. The advertisement period is how often the router advertises (broadcasts) its UPnP information. This value can range from 1 to 1440 minutes. The default period is for 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. A hop is the number of 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 router and which ports (internal and external) that device has opened.

3. To save, cancel your changes, or refresh the table:
   - Click **Apply** to save the new settings to the 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.

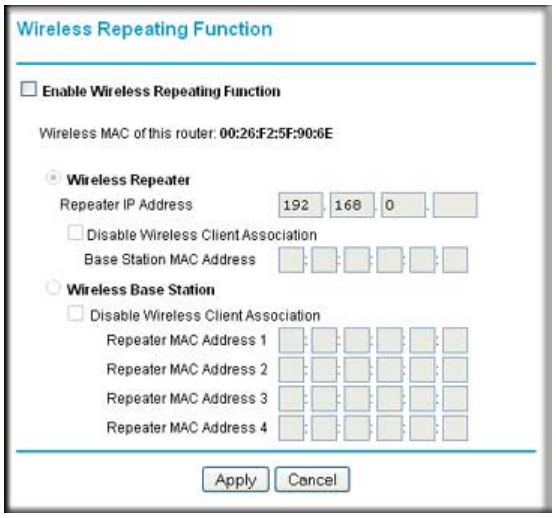
Wireless Bridging and Repeating

You can build large bridged wireless networks by using the router to configure a wireless distribution system (WDS). Some examples of wireless bridged configurations are:

- **Point-to-Point bridge**. The router communicates with another bridge-mode wireless station. See Point-to-Point Bridge Configuration.
- **Multi-Point bridge**. The 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 Configuration.
- **Repeater with wireless client association**. Sends all traffic to the remote access point. See Repeater with Wireless Client Association.

Note: Unless you change the security configuration, the wireless bridging and repeating feature uses the default security profile to send and receive traffic.

On the main menu, below the Advanced heading, select Wireless Repeating Function to display the following screen:



Point-to-Point Bridge Configuration

In Point-to-Point Bridge mode, the router communicates as an access point with another bridge-mode wireless station. The following figure shows an example of Point-to-Point Bridge mode.

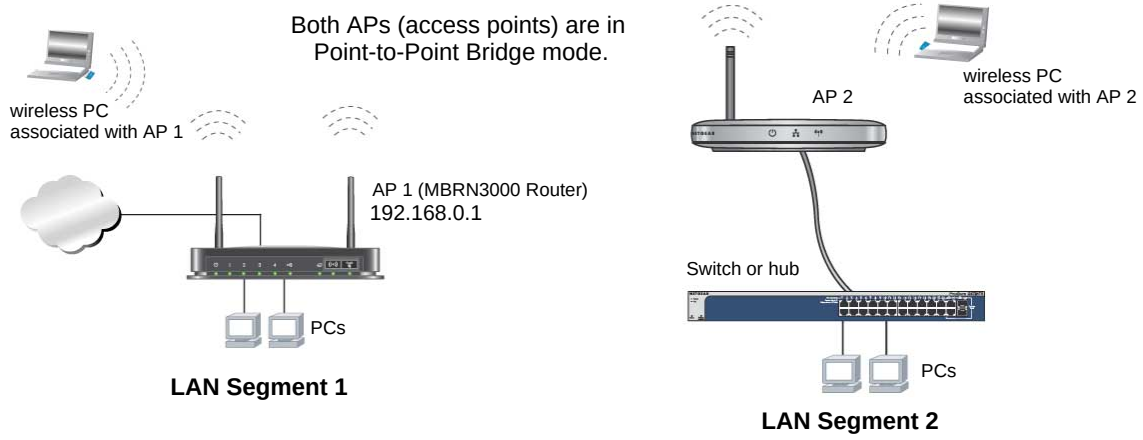


Figure 4 Point-to-Point Bridge

As a bridge, wireless client associations are disabled—only wired clients can be connected. You must enter the MAC address of the other bridge-mode wireless station in the field provided. Use wireless security to protect this communication.

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

1. Configure the MBR1000 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 MBR1000 router must have AP 2's MAC address in its **Remote MAC Address** field, and AP 2 must have the MBR1000's MAC address in its **Remote MAC Address** field.

3. Configure and verify the following for both access points:

   Both access points must use the same SSID, channel, authentication mode, if any, and security settings if security is in use.

4. Disable the DHCP server on AP2. AP1 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 PCs or servers connected to LAN segment 1 or LAN segment 2.

Multi-Point Bridge Configuration

Multi-Point Bridge mode allows a router to bridge to multiple peer access points simultaneously. As a bridge, wireless client associations are disabled—only wired clients can be connected. The figure below shows an example of a Multi-Point Bridge mode configuration.

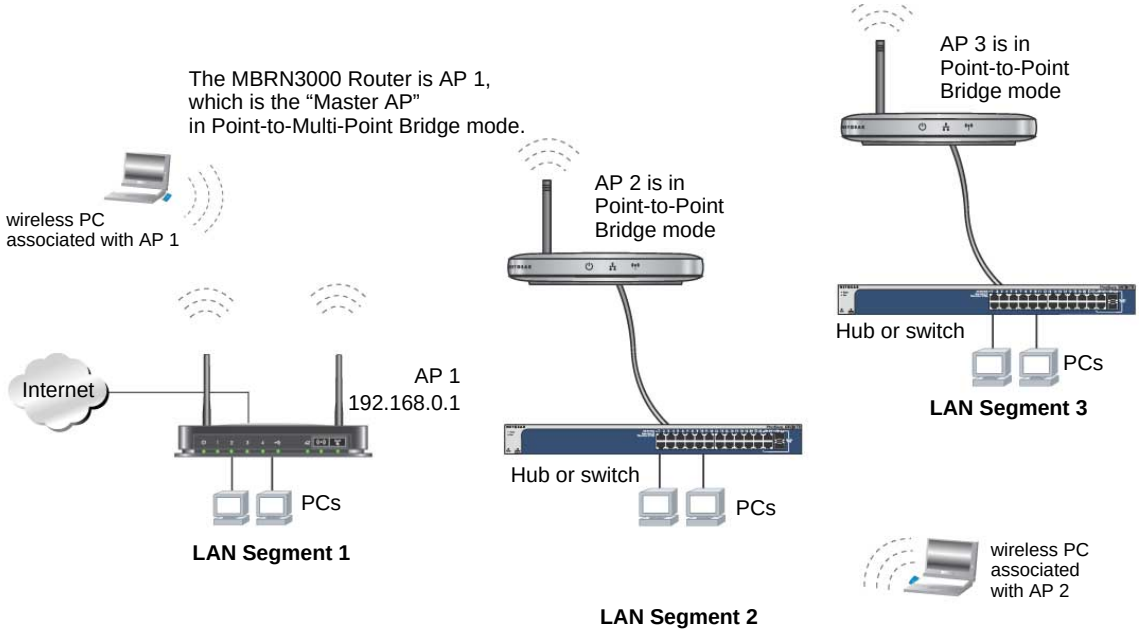


Figure 5 Multi-Point Bridge

Multi-Point Bridge mode configuration includes the following steps:

- Entering the MAC addresses of the other access points in the fields provided.
- Setting the other bridge-mode access points to Point-to-Point Bridge mode, using the MAC address of this MBR1000 router as the Remote MAC Address.
- Using wireless security to protect this traffic.

To set up the multi-point bridge configuration:

1. Configure the operating mode of the routers.
   - Because it is in a central location, configure the MBR1000 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 (AP2) on LAN Segment 2 in Point-to-Point Bridge mode with the remote MAC address of the MBR1000 router.
   - Configure the access point (AP3) on LAN Segment 3 in Point-to-Point Bridge mode with the remote MAC address of the MBR1000 router.
2. Disable the DHCP server on AP2 and AP3. AP1 will then be the DHCP server.
3. Verify the following for all access points:
   - The LAN network configuration of the 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 MBR1000 router, is configured in Point-to-Multi-Point Bridge mode; all the others are in Point-to-Point Bridge mode.
   - All access points, including the MBR1000 router, must be on the same LAN. That is, all the access point LAN IP addresses must be in the same network.
   - All access points, including the MBR1000 router, must use the same SSID, channel, authentication mode, if any, and encryption in use.
   - All point-to-point access points must have the MAC address of AP 1 (the MBR1000 router in the above diagram) 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 PCs or servers connected to any of the three LAN segments.

Note: Wireless stations configured as they are in the previous example will not be able to connect to the 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 this mode, the Mobile Broadband 11n Wireless Router sends all traffic to a remote AP. For Repeater mode, you must enter the MAC address of the remote “parent” access point. Alternatively, you can configure the Mobile Broadband 11n Wireless Router as the parent by entering the address of a “child” access point. Note that the following restrictions apply:

- You cannot disable client associations with this Mobile Broadband 11n Wireless Router.

- You cannot configure a sequence of parent/child access points. You are limited to only one parent access point, although if the MBR1000 router is the parent access point, it can connect with up to four child access points.

The following figure shows an example of a Repeater Mode configuration.

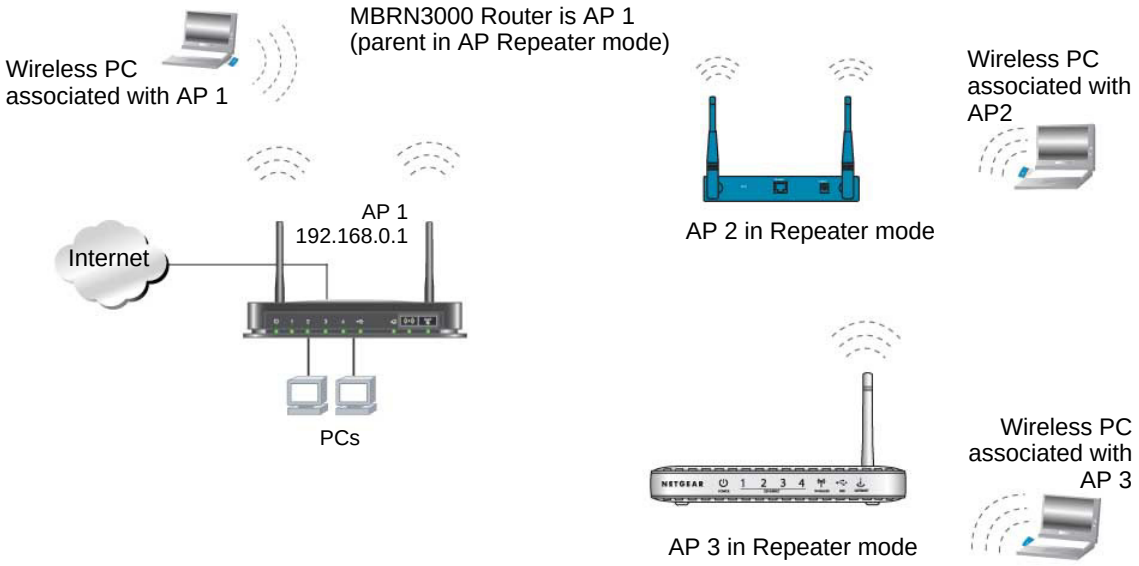


Figure 6 Repeater Mode

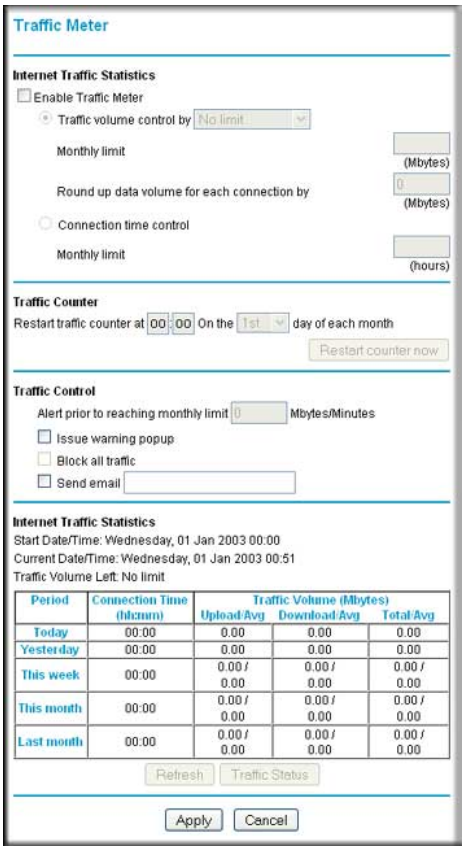
To set up a repeater with wireless client association:

1. Configure the operating mode of the devices.
   - Configure AP 1 the MBR1000 router in the previous figure) on LAN Segment 1 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 access points must be on the same LAN. That is, the LAN IP addresses for the access points must be in the same subnet.
   - Access point devices must use the same SSID, channel, authentication mode, and encryption.
3. Disable the DHCP servers on repeaters AP2 and AP3. AP1 will then be the DHCP server.
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 PCs or servers connected to any of the three WLAN segments.

Traffic Meter

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

To monitor traffic on your router:



1. Under the Advanced heading on the router menu, select Traffic Meter.
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 month limit of Mbytes or hours is reached. You can select one of the following to occur when the limit is attained:
   - The Internet LED flashes green or amber.
   - The Internet connection is disconnected and disabled.
7. Set up **Internet Traffic Statistics** to monitor the data traffic.
8. Click the **Traffic Status** button if you want a live update on Internet traffic status on your router.
9. Click **Apply** to save your settings.

Troubleshooting

6

This chapter gives information about troubleshooting your Mobile Broadband 11n Wireless Router. 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?
- Have I connected the router correctly?

  Go to *"Basic Functioning"* on page 67.
- I can't access the router's configuration with my browser.

  Go to *"Troubleshooting Access to the Router Main Menu"* on page 69.
- I've configured the router but I can't access the Internet.

  Go to *"Troubleshooting the ISP Connection"* on page 70.
- I want to clear the configuration and start over again.

  Go to *"Restoring the Default Configuration and Password"* on page 73.

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 that:
   a. The Power LED is still solid green. A red light indicates the unit has failed its power-on self-test (POST).
   b. The Internet LED is lit.
   c. The WiFi radio LED is lit. The WiFi radio is on by default.

d. The Ethernet LAN port LED is lit when any local ports are connected.

If a LAN port's 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.

e. The Ethernet WAN port LED is lit when the router is connected to a wired modem.

f. The Signal LED is lit when the router has detected a Mobile Broadband signal.

- A blue LED indicates excellent coverage.
- A green LED indicates good coverage.
- An amber LED indicates marginal coverage.

If any of these conditions does not occur, refer to the following table.

Table 11. Troubleshooting with the LEDs

LED		Action
Power 	Power LED is off.	• Make sure that the power cord is properly connected to your router and that the power supply adapter is properly 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.
	Power LED is red	There is a fault within the router. Try to clear the fault as follows: • 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 *"Restoring the Default Configuration and Password"* on page 73. If the error persists, you might have a hardware problem and should contact technical support.
Internet Port 	Internet LED is red.	The router cannot connect to the Internet. Check the Internet connection option being used. • For the Mobile Broadband connection option, check the Signal LED. • For the Ethernet connection option, check the WAN LED.
	Internet LED is blinking red and green	The Traffic meter feature is enabled and the limit set has been reached.
WiFi 	WiFi LED is off.	The WiFi radio has been turned off. If a WiFi connection is desired with the router, push the WiFi button to turn the WiFi radio back on.
	WiFi LED is not blinking.	If this LED does not blink when attempting to send data over the WiFi link, log into the router menu using the Ethernet LAN connection and check your router's wireless (WiFi) configuration.

Table 11. Troubleshooting with the LEDs (Continued)

LED		Action
LAN Ports 	LAN LED is off.	If this LED does not light when an Ethernet connection is made, check the following: • Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation. • Make sure that power is turned on to the connected hub or workstation.
WAN Port 	WAN LED is off.	If this LED does not light when an Ethernet connection is made using the Ethernet connection option, check the following: • Make sure that the Ethernet cable connections are secure at the router and at the modem. • Make sure that power is turned on to the modem.
2G/3G 	2G/3G LED is off.	The router cannot tell if the Mobile Broadband connection uses 2G or 3G signals.
Signal 	Signal LED of off.	If this LED does not light when the Mobile Broadband connection option is used, check the following: • Check with your ISP to ensure there is good coverage in the area. • Ensure your mobile broadband account is active. • Ensure the SIM card is inserted properly into the router. • Locate the router near the window or other area of the building. Make sure the Signal LED is lit, indicating that there is mobile broadband coverage with the router. • Log in to the router menu and check your router's Internet configuration. Check that the user name, password, and APN with ISP are set correctly. If you use a PIN to connect to the Internet, make sure it is entered correctly.

Troubleshooting Access to the Router Main Menu

If you are unable to access the router main menu 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 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. See the online document listed in "Internet Networking and TCP/IP Addressing:" in Appendix Bt o find your computer's IP address.

Note: If your computer's IP address is shown as 169.254.x.x: Recent versions of Windows and MacOS generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated 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 will set the router's IP address to 192.168.0.1. This procedure is explained in *"Restoring the Default Configuration and Password"* on page 73.
- 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 entering this information.

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

- When entering configuration settings, be sure to click 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.

Troubleshooting the ISP Connection

Connecting to the Internet

If unable to connect to internet, check these:

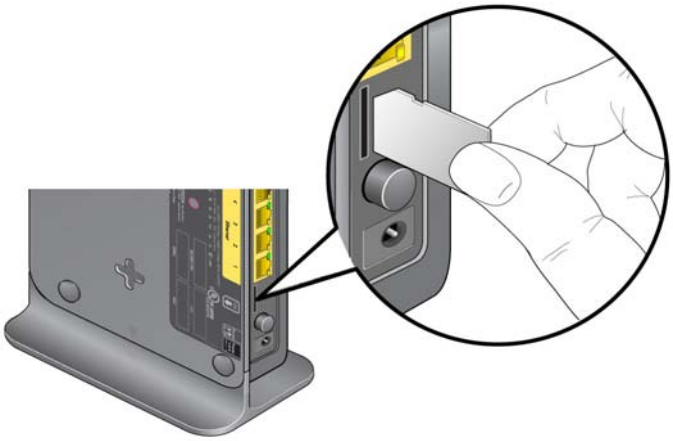
1. The Internet account is active.

   If your ISP has provided you with a SIM card and you haven't inserted it into the SIM card slot on the back of the router yet, do so now.

2. Wireless broadband coverage is available where the unit is located.
3. Access the router main menu to verify configurations in broadband settings is correct. Check with ISP if unsure.
4. The location of the router.

   a. Move the router closer to a window for better access to the Internet signal.

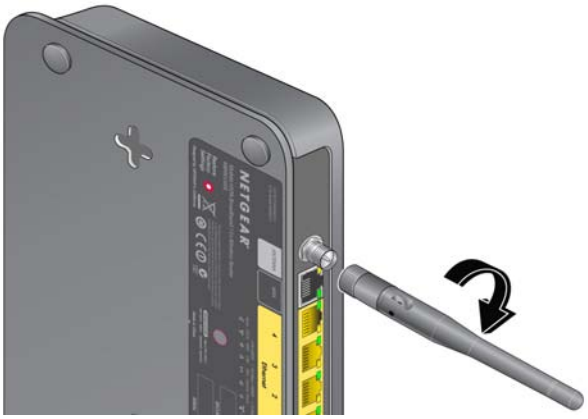
   - A blue Signal LED indicates excellent coverage.
   - A green Signal LED indicates good coverage.



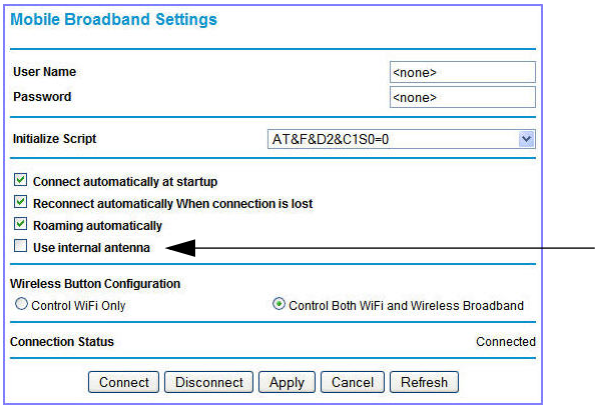
- An amber Signal LED indicates marginal coverage.
- A dark Signal LED indicates no coverage.

b. Maintain recommended minimum distances between NETGEAR equipment and household appliances to reduce interference (see *"Regulatory Compliance Information"* on page 80).

5. Using an external antenna for greater signal strength (especially indoors).



a. Install external antenna. (The external antenna is an optional accessory that can be obtained by the user.)



b. Deselect **Use Internal Antenna** on Mobile Broadband Settings screen and then click **Apply**.

c. Click **Connect** to connect to the Internet.

Troubleshooting Internet Browsing

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

- Traffic meter is enabled and limit may have been reached.

  By configuring the traffic meter to not block, you can resume Internet access. If you have an usage limit, your ISP may charge you for the overage.

- Your computer might not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your computer and verify the DNS address as described in "Internet

Networking and TCP/IP Addressing:" in Appendix B. Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

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

  If your computer obtains its information from the router by DHCP, reboot the computer, and verify the router address as described in the link to the online document "Internet Networking and TCP/IP Addressing:" in Appendix B.

Troubleshooting 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. Troubleshooting a TCP/IP network is made very easy by using the ping utility in your computer.

Testing the LAN Path to Your Router

You can ping the router from your PC 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 working 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 Table 11 on page 68.

  - 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 PC or workstation.
  - Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your Computer to a Remote Device

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

1. From the Windows toolbar, click the **Start** button, and select **Run**.
2. In the Windows Run window, type:

   `PING -n 10` *IP address*

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

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

- Check that your PC has the IP address of your router listed as the default router. If the IP configuration of your PC is assigned by DHCP, this information is not visible in your PC's Network Control Panel. Verify that the IP address of the router is listed as the default router as described in the online document listed in <pdf>"Preparing a Computer for Network Access:" in Appendix B.
- Make sure that the network address of your PC (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 PC, 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 PCs. Many broadband ISPs restrict access by allowing only traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your router to clone or spoof the MAC address from the authorized PC. See the *Mobile Broadband Wireless-N Router MBRN3000 Installation Guide*.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router's admin 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 feature (see *“Backing Up, Restoring, or Erasing Your Settings”* on page 35).
- Press the Restore Factory Settings on the bottom of the router for 6 seconds. Use this method for cases when the administration password or IP address is not known.

The factory default settings are shown in "Factory Default Settings" in Appendix A.

Problems with Date and Time

The E-mail screen in the Content Filtering section displays the current date and time of day. The Mobile Broadband 11n Wireless Router uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include the following:

- Date shown is January 1, 2000.
  Cause: The router has not yet successfully reached a network time server. Check that your Internet access settings are 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. On the E-mail screen, select or clear the **Adjust for Daylight Savings Time** check box.

Factory Default Settings and Technical Specifications

A

Factory Default Settings

You can use the Restore Factory Settings button located on the bottom of your router to reset all settings to their factory defaults. This is called a hard reset. To perform a hard reset, push and hold the Restore Factory Settings button for 6 seconds. Your router will return to the factory configiuration settings that are shown in the following table.

Feature		Default Behavior
Router login	User login URL	http://www.routerlogin.net *or* 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	AutoSense
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	Disabled
	Time zone	PST for North America, GMT for other locations
	Daylight saving time adjustment	Disabled

Feature (Continued)		Default Behavior (Continued)
Firewall	Inbound communication from the Internet	Disabled (except traffic on port 80, the http port)
	Outbound communication to the Internet)	Enabled (all)
	Source MAC filtering	Disabled
Wireless	Wireless communication	Enabled
	SSID name	NETGEAR
	Security	Disabled
	Broadcast SSID	Enabled
	Transmission speed	Auto[1]
	Country/Region	United States (in North America; otherwise, varies by region)
	RF channel	11 until the region is selected
	Operating mode	Up to 300 Mbps
	Data rate	Best
	Output power	Full
	Access point	Enabled
	Authentication type	Open system
	~~Wireless card access~~ list	All wireless stations allowed

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

Technical Specifications

Technical Specifications	
Network Protocol and Standards Compatibility	TCP/IP, DHCP
Power adapter	• North America: 120V AC, 60 Hz, input • United Kingdom, Australia: 240V AC, 50 Hz, input • Europe: 230V AC, 50 Hz, input • Japan: 100V AC, 50/60 Hz, input • All regions (output): 12 V DC @ 1.0A output
Physical specifications	• Dimensions: 6.8" x 5.03" x 1.28" (173 mm x 128 mm x 33 mm) • Weight: 0.65 lbs. without the stand (0.29 kg)
Environmental Specifications	• Operating temperature: 0° to 40° C (32º to 104º F) • Operating humidity: 90% maximum relative humidity, noncondensing
Electromagnetic Emissions	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: USB

Related Documents

B

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

Document	Link
Windows XP and Vista Wireless Configuration Utilities Application Note	http://documentation.netgear.com/reference/enu/winzerocfg/index.htm
Internet Networking and TCP/IP Addressing:	http://documentation.netgear.com/reference/enu/tcpip/index.htm
Wireless Communications:	http://documentation.netgear.com/reference/enu/wireless/index.htm
Preparing a Computer for Network Access:	http://documentation.netgear.com/reference/enu/wsdhcp/index.htm
Virtual Private Networking (VPN):	http://documentation.netgear.com/reference/enu/vpn/index.htm
Glossary:	http://documentation.netgear.com/reference/enu/glossary/index.htm

Notification of Compliance

NETGEAR Wireless Routers, Gateways, AP's

C

Regulatory Compliance Information

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.

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, Santa Clara, CA 95134, declare under our sole responsibility that the NETGEAR® Mobile Broadband 11n Wireless Router MBR1000 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, (NETGEAR® Mobile Broadband 11n Wireless Router MBR1000), 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.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the Class B category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

Interference Reduction Table

Household Appliance	Recommended Minimum Distance between NETGEAR equipment and household appliance to reduce interference (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

IC Statement

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.

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 and your body.

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

Europe – EU Declaration of Conformity

Marking with 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, EN301 893 (5Ghz), EN60950-1
- 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.
- For complete DoC, visit the NETGEAR EU Declarations of Conformity website at: *http://kb.netgear.com/app/answers/detail/a_id/11621/*

EDOC in Languages of the European Community

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.

Index

T

U

W