

Mobile Broadband Wireless-N Router MBRN3000 User Manual



NETGEAR®

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

202-10578-01
October 2009
v1.0

Trademarks

NETGEAR and the NETGEAR logo are trademarks of Netgear, Inc. Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving 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.

FCC Statement

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 generates, 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 of the following measures:

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

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.

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.

The radio module has been evaluated under FCC Bulletin OET 65C (01-01) and found to be compliant to the requirements as set forth in CFR 47 Sections, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices. This model meets the applicable government requirements for exposure to radio frequency waves.

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. For product available in the USA market, only channels 1~11 can be operated. Selection of other channels is not possible

Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

European Union Statement of Compliance

Hereby, NETGEAR, Inc. declares that this router is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Ěeský [Czech]	NETGEAR, Inc. tímto prohlašuje, že tento Mobile Broadband Wireless-N Router MBRN3000 je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede NETGEAR, Inc. erklærer herved, at følgende udstyr Mobile Broadband Wireless-N Router MBRN3000 overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt NETGEAR, Inc., dass sich das Gerät Mobile Broadband Wireless-N Router MBRN3000 in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab NETGEAR, Inc. seadme Mobile Broadband Wireless-N Router MBRN3000 vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, NETGEAR, Inc., declares that this Mobile Broadband Wireless-N Router MBRN3000 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 Mobile Broadband Wireless-N Router MBRN3000 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 Mobile Broadband Wireless-N Router MBRN3000 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 Mobile Broadband Wireless-N Router MBRN3000 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 Mobile Broadband Wireless-N Router MBRN3000 è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo NETGEAR, Inc. deklarā, ka Mobile Broadband Wireless-N Router MBRN3000 atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo NETGEAR, Inc. deklaruoja, kad šis Mobile Broadband Wireless-N Router MBRN3000 atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

Nederlands [Dutch]	Hierbij verklaart NETGEAR, Inc. dat het toestel Mobile Broadband Wireless-N Router MBRN3000 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 Mobile Broadband Wireless-N Router MBRN3000 jikkonforma mal-tiġiet essenzjali u ma provvedimenti orajni relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, NETGEAR, Inc. nyilatkozom, hogy a Mobile Broadband Wireless-N Router MBRN3000 megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Polski [Polish]	Niniejszym NETGEAR, Inc. oświadczam, że Mobile Broadband Wireless-N Router MBRN3000 jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	NETGEAR, Inc. declara que este Mobile Broadband Wireless-N Router MBRN3000 está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR, Inc. izjavlja, da je ta Mobile Broadband Wireless-N Router MBRN3000 v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	NETGEAR, Inc. týmto vyhlasuje, že Mobile Broadband Wireless-N Router MBRN3000 spáda základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	NETGEAR, Inc. vakuuttaa täten että Mobile Broadband Wireless-N Router MBRN3000 tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar NETGEAR, Inc. att denna Mobile Broadband Wireless-N Router MBRN3000 står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

A printed copy of the EU Declaration of Conformity certificate for this product is provided in the MBRN3000 product package.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das Mobile Broadband Wireless-N Router MBRN3000 gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entworfen ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Certificate of the Manufacturer/Importer

It is hereby certified that the Mobile Broadband Wireless-N Router MBRN3000 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for

example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the second 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.

Customer Support

Refer to the Support Information Card that shipped with your Mobile Broadband Wireless-N Router MBRN3000.

World Wide Web

NETGEAR maintains a World Wide Web home page that you can access at the universal resource locator (URL) <http://www.netgear.com>. A direct connection to the Internet and a Web browser such as Internet Explorer or Mozilla Firefox are required.

Product and Publication Details

Model Number:	MBRN3000
Publication Date:	October 2009
Product Family:	Router
Product Name:	Mobile Broadband Wireless-N Router MBRN3000
Home or Business Product:	Home
Language:	English
Publication Part Number:	202-10578-01
Publication Version Number:	1.0

Contents

Mobile Broadband Wireless-N Router MBRN3000 User Manual

About This Manual

Conventions, Formats, and Scope	i
How to Print This Manual	ii
Revision History	ii

Chapter 1

Configuring Your Router to the Internet

Hardware Features	1-1
Router Front Panel	1-1
Router Back Panel	1-3
Router Label	1-4
Using the Router Stand	1-4
Logging In to Your Router	1-5
Accessing the Setup Wizard after Installation	1-6
Manually Configuring Your Internet Settings	1-7

Chapter 2

Wireless Network Configuration

Planning Your Wireless Network	2-1
Wireless Placement and Range Guidelines	2-2
Wireless Security Options	2-3
Manually Configuring Your Wireless Settings	2-4
Configuring WEP	2-6
Configuring WPA, WPA2, or WPA + WPA2	2-8
Using Push 'N' Connect (WPS) to Configure Your Wireless Network	2-9
Using a WPS Button to Add a WPS Client	2-9
Using PIN Entry to Add a WPS Client	2-11
Connecting Additional Wireless Client Devices After WPS Setup	2-12
Adding More WPS Clients	2-12

Adding Both WPS and Non-WPS Clients	2-13
Chapter 3	
Protecting Your Network	
Protecting Access to Your Wireless Router	3-1
Changing the Built-In Password	3-1
Changing the Administrator Login Time-out	3-2
Configuring Basic Firewall Services	3-2
Blocking Keywords, Sites, and Services	3-3
Firewall Rules	3-5
Inbound Rules (Port Forwarding)	3-6
Outbound Rules (Service Blocking)	3-8
Order of Precedence for Rules	3-10
Services	3-10
Defining Services	3-11
Setting Times and Scheduling Firewall Services	3-11
Setting Your Time Zone	3-12
Scheduling Firewall Services	3-13
Chapter 4	
Managing Your Network	
Backing Up, Restoring, or Erasing Your Settings	4-1
Backing Up the Configuration to a File	4-1
Restoring the Configuration from a File	4-2
Erasing the Configuration	4-2
Upgrading the Router Firmware	4-2
Network Management Information	4-4
Router Status	4-4
Showing Statistics	4-6
Connection Status	4-7
Viewing Attached Devices	4-8
Viewing, Selecting, and Saving Logged Information	4-9
Examples of Log Messages	4-11
Enabling Security Event E-mail Notification	4-12
Running Diagnostic Utilities and Rebooting the Router	4-13
Enabling Remote Management	4-14
Configuring Remote Management	4-14

Chapter 5 Advanced Configuration

Advanced Wireless Settings	5-2
Wireless Station Access Control	5-3
Restricting Access by MAC Address	5-4
WAN Setup	5-5
Setting Up a Default DMZ Server	5-6
LAN IP Settings	5-7
DHCP Settings	5-10
Reserved IP Addresses	5-11
Dynamic DNS	5-11
Configuring Dynamic DNS	5-12
Using Static Routes	5-13
Static Route Example	5-13
Configuring Static Routes	5-14
Universal Plug and Play (UPnP)	5-15
Wireless Bridging and Repeating	5-16
Point-to-Point Bridge Configuration	5-17
Multi-Point Bridge Configuration	5-19
Repeater with Wireless Client Association	5-20

Chapter 6 Troubleshooting

Basic Functioning	6-1
Troubleshooting Access to the Router Main Menu	6-2
Troubleshooting the ISP Connection	6-4
Obtaining a WAN IP Address	6-4
Troubleshooting PPPoE or PPPoA	6-5
Troubleshooting Internet Browsing	6-5
Troubleshooting a TCP/IP Network Using the Ping Utility	6-6
Testing the LAN Path to Your Router	6-6
Testing the Path from Your Computer to a Remote Device	6-7
Restoring the Default Configuration and Password	6-7
Problems with Date and Time	6-8

Appendix A
Technical Specifications and Factory Default Settings

Factory Default Settings A-2

Appendix B
Related Documents

About This Manual

The *NETGEAR® Mobile Broadband Wireless-N Router MBRN3000 User Manual* describes how to install, configure, and troubleshoot the Mobile Broadband Wireless-N Router MBRN3000. The information in this manual is intended for readers with intermediate computer and Internet skills.


Conventions, Formats, and Scope


The conventions, formats, and scope of this manual are described in the following paragraphs:


- **Typographical Conventions.** This manual uses the following typographical conventions:

<i>Italic</i>	Emphasis, books, CDs, file and server names, extensions
Bold	User input, IP addresses, GUI screen text
<i>Italic</i>	URL links

- **Formats.** This manual uses the following formats to highlight special messages:

	Note: This format is used to highlight information of importance or special interest.
---	--

	Tip: This format is used to highlight a procedure that will save time or resources.
---	--

	Warning: Ignoring this type of note might result in a malfunction or damage to the equipment.
---	--

- **Scope.** This manual is written for the Wireless Router according to these specifications:

Product Version	Mobile Broadband Wireless-N Router MBRN3000
Manual Publication Date	October 2009

For more information about network, Internet, firewall, and VPN technologies, see the links to the NETGEAR website in [Appendix B, “Related Documents”](#).”



Note: Product updates are available on the NETGEAR, Inc. website at <http://kbserver.netgear.com/products/MBRN3000.asp>.

How to Print This Manual

To print this manual, your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe website at <http://www.adobe.com>.



Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Revision History

Part Number	Version Number	Date	Description
202-10578-01	1.0	October 2009	Original publication

Chapter 1

Configuring Your Router to the Internet

This chapter describes how to configure your Mobile Broadband Wireless-N Router MBRN3000 Internet connection. For help with installation, see the *Mobile Broadband Wireless-N Router MBRN3000 Installation Guide*.

Hardware Features

The following sections describe the front panel, rear panel, and label.

Router Front Panel

The router front panel shown below contains status LEDs.

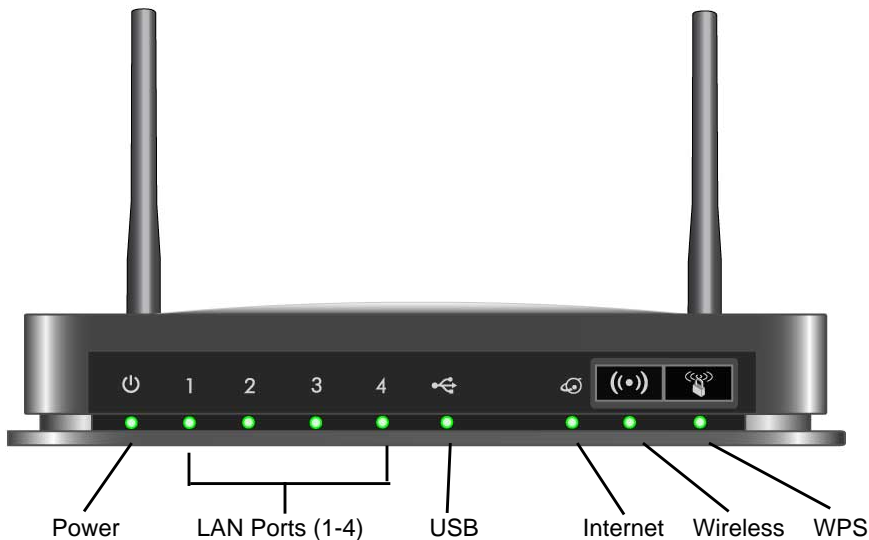


Figure 1

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. LED and Front Panel Button Descriptions









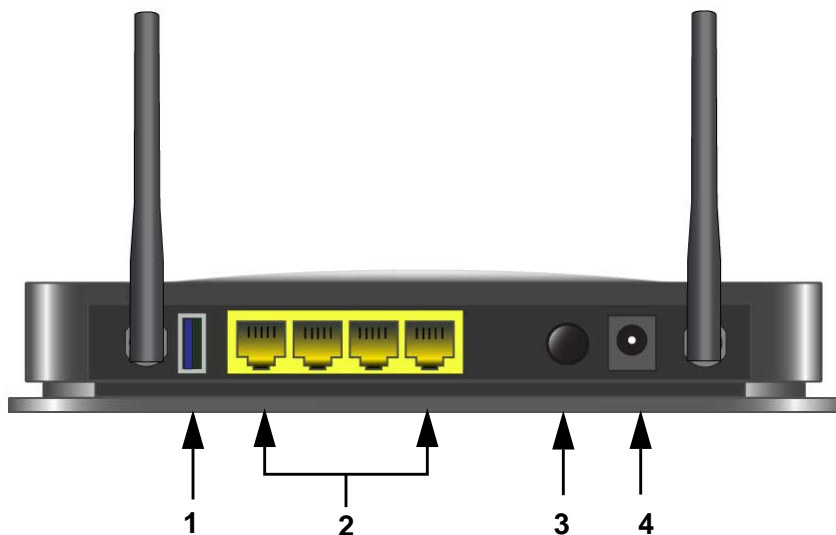
LED	LED Activity	Description
	Solid green	Solid green. Power is supplied to the router.
	Solid Red	POST (Power-On Self-Test) failure or device malfunction
	Off	Power is not supplied to the router
	Factory Reset	Lights momentarily when the Restore Factory Settings button is pressed for 6 seconds, then blinks red three times when released. It then turns green as the gateway resets to the factory defaults.
LAN Ports 1 - 4 	Solid green	The Local port has detected an Ethernet link with a device.
	Blinking green	Data is being transmitted or received.
	Off	No link is detected on this port.
USB 	Off	<ul style="list-style-type: none"> No USB device connected. "Safely Remove Hardware" has been activated. An error has occurred with the device.
	Solid green	USB device is ready to use.
	Blinking green	USB device is in use.
Internet Port 	Solid green	There is an Internet session. If the session is dropped due to an idle timeout, and an ADSL connection is still present, the light will remain green. If the session is dropped for any other reason, the light will turn off.
	Solid red	IP connection failed (no DHCP or PPPoE response, PPPoE authentication failed).
	Blinking green	Data is being transmitted over the ADSL port.
	Off	No Internet connection detected or device in bridged mode.
Wireless 	Solid green	Indicates that the Wireless port is initialized.
	Blinking green	Data is being transmitted or received over the wireless link.
	Off	The Wireless Access Point is turned off.
WPS 	Solid green	WPS wireless security is being enabled.
	Blinking green	The device is in the 2-minute interval to synchronize security.
	Off	WPS is not being set or enabled.
Button	Description	

Table 1. LED and Front Panel Button Descriptions (continued)

LED	LED Activity	Description
 Wireless On/Off		Turn the wireless radio in the router on and off. The wireless radio is on by default. The LED located below this button indicates if the wireless radio is on or off.
 Push 'N' Connect (WPS)		Pushing this button opens 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 1-22.

Router Back Panel

The back panel of the router contains port connections.

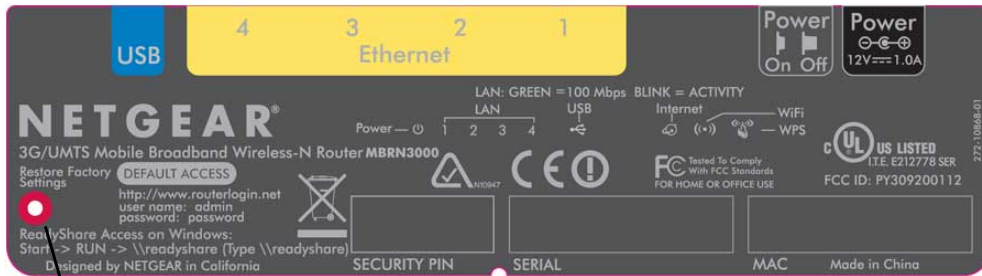
**Figure 2**

Viewed from left to right, the rear panel contains the following elements:

1. USB port for 3G/UMTS modem.
2. Four local Ethernet RJ-45 LAN ports for connecting the router to the local computers.
3. Power On/Off button.
4. AC power adapter input.

Router Label

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



Factory Default Reset. Press for 6 seconds to reset the router to its factory default settings.

Figure 3

Using the Router Stand

For optimal wireless network performance, use the stand (included in the package) to position your router upright.

1. Orient your router vertically.
2. Insert the tabs of the stand into the slots on the bottom of your router as shown:



Figure 4

- Place your router in a suitable area for installation (near an AC power outlet and accessible to the Ethernet cables for your wired computers).

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 “Preparing Your Network” in Appendix B.

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


To log in to the router:

- Type **http://www.routerlogin.net**, or **http://www.routerlogin.com**, or the router’s LAN IP address (default is 192.168.0.1) in the address field of your browser, and then press Enter. A login window displays:

User name: admin
Password:
 Remember my password
OK Cancel

Figure 1-1

2. Enter **admin** for the router 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 3-2.

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

3. If the router has never 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 configuration, this screen displays unless you previously cleared the **Check for Updated Firmware Upon Log-in** check box.

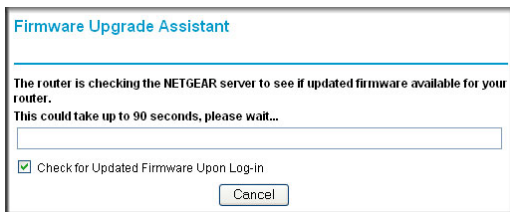


Figure 1-2

- **Router Status screen.** The Router Status screen displays if the router has not been configured yet or has been reset to its factory default settings. See [“Viewing Modem Router Status Information”](#) on page 4-4.
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 Setup Wizard after Installation”](#) on page 1-6.
 - You can manually configure the router settings. See [“Manually Configuring Your Internet Settings”](#) on page 1-7.

Accessing the Setup Wizard after Installation

1. Log in to the router as described in the previous section, [“Logging In to Your Router”](#) on page 1-5.

2. Select Setup Wizard to go to the Setup Wizard screen:

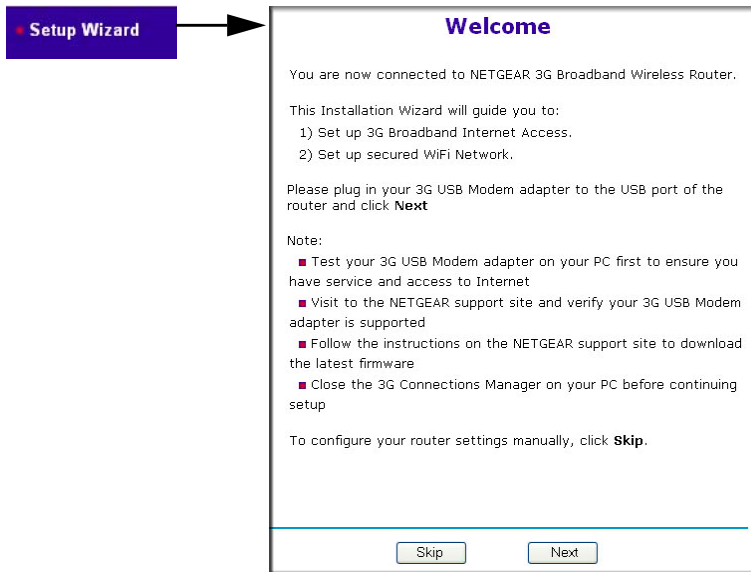


Figure 1-3

3. Click **Next**.

The Setup Wizard prompts you to configure your Internet connection and wireless network as described in the *Mobile Broadband Wireless-N Router MBRN3000 Installation Guide*.

Manually Configuring Your Internet Settings

In order to connect to the network, and active broadband service account is required. Please 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 the previous section.

2. Select Broadband Settings, and the following screen displays:

Figure 1-4

Table 1-1. Broadband Settings fields

Fields and Checkboxes	Description
Username	Internet account login username
Password	Internet account password for authentication
Pin code	Pin code of the SIM card, where applicable
Network name/APN	ISP network name
PDP type	Type of packet data protocol
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.
Connection status	Current WAN port status

The following buttons are available:

- Click **Connect** when you want to manually connect to the network.

- Click **Disconnect** when you want to manually disconnect from current network.
- Click **Apply** when you finish changing the settings.
- Click **Cancel** to discard changes.
- Click **Refresh** to update connection status.

Chapter 2

Wireless Network Configuration

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.



Warning: Computers can connect wirelessly at a range of several hundred feet. This can allow others outside of your immediate area to access your network.

This chapter includes:

- [“Planning Your Wireless Network”](#)
- [“Manually Configuring Your Wireless Settings”](#) on page 2-4
- [“Configuring WEP”](#) on page 2-6
- [“Using Push 'N' Connect \(WPS\) to Configure Your Wireless Network”](#) on page 2-9
- [“Using Push 'N' Connect \(WPS\) to Configure Your Wireless Network”](#) on page 2-9
- [“Connecting Additional Wireless Client Devices After WPS Setup”](#) on page 2-12

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 (802.11n, 802.11g, or 802.11b) that each wireless adapter supports.
 - Wireless security option. To successfully implement wireless security, check each wireless adapter to determine which wireless security option it supports.

See [“Manually Configuring Your Wireless Settings”](#) on page 2-4.

- Push 'N' Connect (WPS) automatically implements wireless security on the router while, at the same time, allowing you to automatically implement wireless security on any WPS-enabled devices (such as wireless computers and wireless adapter cards). You activate WPS by pressing a WPS button on the router, clicking an onscreen WPS button, or entering a PIN number. This generates a new SSID and implements WPA/WPA2 security.

To set up your wireless network using the WPS feature:

- Use the WPS button on the side of the router (there is also an onscreen WPS button), or enter the PIN of the wireless device.
- Make sure that all wireless computers and wireless adapters on the network are Wi-Fi certified and WPA or WPA 2 capable, and that they support WPS configuration.

See [“Using Push 'N' Connect \(WPS\) to Configure Your Wireless Network”](#) on page 2-9.

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 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:

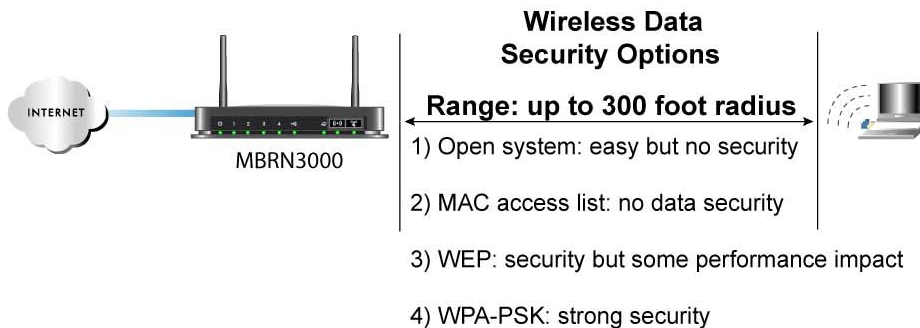


Figure 2-1

- **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

You can view or manually configure the wireless settings for the router in the Wireless Settings screen. If you want to make changes, make sure to note the current settings first.



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

To view or manually configure the wireless settings:

1. Log in to the router at its default LAN address of **http://192.168.0.1** with its default user name of **admin**, and default password of **password**, or using whatever user name, password, and LAN address you have chosen for the router.
2. Select Wireless Settings from the main menu to display the Wireless Settings screen:

Wireless Settings

Wireless Network

Name (SSID):

Region:

Channel:

Mode:

Security Options

None

WEP

WPA-PSK (TKIP)

WPA2-PSK (AES)

WPA-PSK (TKIP) + WPA2-PSK (AES)

Figure 2-2

The settings for this screen are explained in [Table 2-1](#).

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.

Program the wireless adapter of your computers to have 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 2-1. 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. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you want to participate in a wireless network must use the SSID.
	Region	The location where the Product Family is used.
	Channel	The wireless channel used by the gateway. The default is Auto. Do not change the wireless channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, you might need to experiment with different channels to see which is the best.
	Mode	The default is up to 300 Mbps.
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” .

Table 2-1. Wireless Settings (continued)

Settings		Description
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

	<p>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.</p>
---	--

To configure WEP data encryption:

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

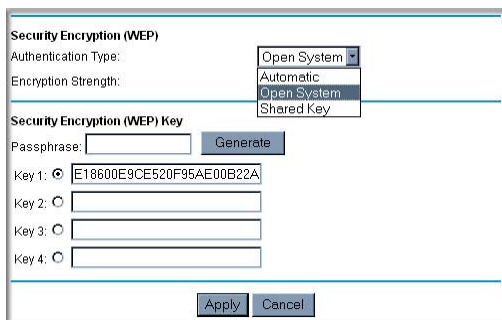


Figure 2-3

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



Note: The authentication scheme is separate from the data encryption. You can select an authentication scheme that requires a shared key but still leaves the data transmissions unencrypted. If you require strong security, 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 at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever user name, password, and LAN address you have chosen for the router.
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

If your wireless clients support Wi-Fi Protected Setup (WPS), you can use this feature to configure the router's SSID and security settings and, at the same time, connect the wireless client securely and easily to the router. Look for the  symbol on your client device (computers that will connect wirelessly to the router are clients). WPS automatically configures the network name (SSID) and wireless security settings for the router (if the router is in its default state) and broadcasts these settings to the wireless client.

Some considerations regarding WPS are:

- WPS supports only WPA-PSK and WPA2-PSK wireless security. WEP security is not supported by WPS.
- 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 additional WPS capable devices. See [“Adding Both WPS and Non-WPS Clients” on page 2-13](#).

A WPS client can be added using the Push Button method or the PIN method.

- **Using the Push Button.** This is the preferred method. See the following section, [“Using a WPS Button to Add a WPS Client”](#).
- **Entering a PIN.** For information about using the PIN method, see [“Using PIN Entry to Add a WPS Client” on page 2-11](#).

Using a WPS Button to Add a WPS Client

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

- On the router main menu, select Add a WPS Client, and then click **Next**. The following screen displays:

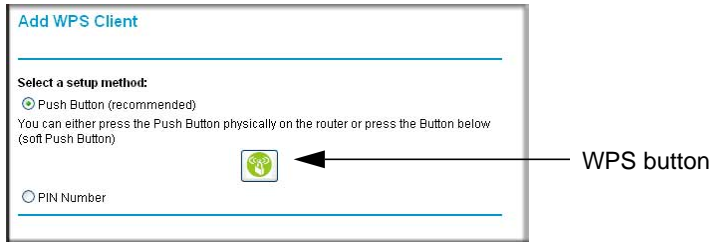


Figure 2-4

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

- Either press the WPS button on the side of the router, or click the onscreen button.
The router tries to communicate with the client for 2 minutes.
- Go to the client wireless computer, and run a WPS configuration utility. Follow the utility's instructions to click a WPS button.
- 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.

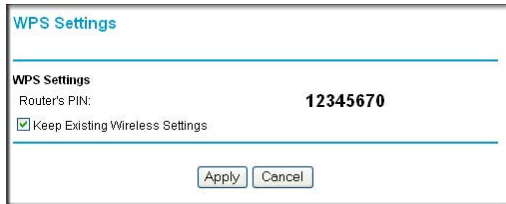


Figure 2-5

- 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 2-4](#).

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 timeframe, the SSID will not be changed, and no security will be implemented on the router.

Using PIN Entry to Add a WPS Client

Any wireless computer or wireless adapter 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** check box 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 check box so that your SSID and wireless security settings remain the same if other WPS-enabled devices are added later.

To use a PIN to add a WPS client:

1. Log in to the router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. 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:

Add WPS Client

Select a setup method:

Push Button (recommended)

PIN Number

If your Adapter supports WPS, please click on "Generate a client Security Pin to input on the AP/Router/Gateway" and put the generated client PIN number here.

Enter Client's PIN:

Figure 2-6

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 displays a message confirming 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 2-4](#)

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 timeframe, the SSID will not be changed and no security will be implemented on the router.

Connecting Additional Wireless Client Devices After WPS Setup

You can add more WPS clients to your wireless network, or you can add a combination of WPS-enabled clients and clients without WPS.

Adding More WPS Clients



Note: Your wireless settings remain the same when you add another WPS-enabled client, as long as the **Keep Existing Wireless Settings** checkbox is selected in the Advanced Wireless screen (listed under the Advanced heading in the router main menu). If you clear this checkbox, when you add the client, a new SSID and passphrase will be generated, and all existing connected wireless clients will be disassociated and disconnected from the router.

To add a wireless client device that is WPS-enabled:

1. Follow the procedures in [“Using a WPS Button to Add a WPS Client” on page 2-9](#) or [“Using PIN Entry to Add a WPS Client” on page 2-11](#).

2. To view a list of all devices connected to your router (including wireless and Ethernet-connected), see [“Viewing Attached Devices” on page 4-8](#).

Adding Both WPS and Non-WPS Clients

For non-WPS clients, you cannot use the WPS setup procedures to add them to the wireless network. You must record, and then manually enter your security settings (see [“Manually Configuring Your Wireless Settings” on page 2-4](#)).

To connect a combination of non-WPS enabled and WPS-Enabled clients to the router:

1. Restore the router to its factory default settings (press both the Wireless and WPS buttons on the side of the router for 5 seconds).

When the factory settings are restored, all existing wireless clients are disassociated and disconnected from the router.

2. Configure the network names (SSIDs), select the WPA/PSK + WPA2/PSK radio button on the Wireless Settings screen (see [“Manually Configuring Your Wireless Settings” on page 2-4](#)). and click **Apply**. On the WPA/PSK + WPA2/PSK screen, select a passphrase and click **Apply**. Record this information to add additional clients.
3. 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).
4. For the WPS devices that you want to connect, follow the procedure [“Using a WPS Button to Add a WPS Client” on page 2-9](#) or [“Using PIN Entry to Add a WPS Client” on page 2-11](#).

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



Note: To make sure that your new wireless settings remain in effect, verify that the **Keep Existing Wireless Settings** checkbox is selected in the WPS Settings screen.

5. To view a list of all devices connected to your router (including wireless and Ethernet-connected), see [“Viewing Attached Devices” on page 4-8](#).

Chapter 3

Protecting Your Network

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

Protecting Access to Your Wireless Router

For security reasons, the router has its own user name and password. Also, after a period of inactivity for a set length of time, the administrator login automatically disconnects. When prompted, enter **admin** for the router user name and **password** for the router password. You can use procedures in the following sections to change the router password and the amount of time for the administrator's login time-out.



Note: 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. Log in to the router at its default LAN address of **http://192.168.0.1** with its default user name of **admin**, default password of **password**, or using whatever password and LAN address you have chosen for the router.

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

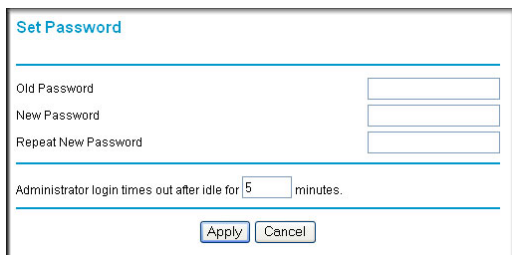



Figure 3-1

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

	<p>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.</p>
---	---

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.

Configuring Basic Firewall Services

Basic firewall services you can configure include access blocking and scheduling of firewall security. These topics are presented in the following sections.

Blocking Keywords, Sites, and Services

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 following section explains how to configure your router to perform these functions.

Blocking Keywords and Sites

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

1. Log in to the router at its default LAN address of **http://192.168.0.1** with its default user name of **admin**, and default password of **password**, or using whatever password and LAN address you have chosen for the router.
2. On the main menu, select Block Sites to display the Block Sites screen:


The screenshot shows the 'Block Sites' configuration page. It includes a 'Keyword Blocking' section with radio buttons for 'Never', 'Per Schedule', and 'Always'. Below that is a text input field for 'Type Keyword or Domain Name Here.' and an 'Add Keyword' button. A section titled 'Block Sites Containing these Keywords or Domain Names:' contains a large empty list box, with 'Delete Keyword' and 'Clear List' buttons below it. At the bottom, there is a checkbox for 'Allow Trusted IP Address to Visit Blocked Sites' and a 'Trusted IP Address' field with four input boxes for IP octets. 'Apply' and 'Cancel' buttons are at the very bottom.

Figure 3-2

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 4-9.
---	---

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.

Firewall Rules

Firewall rules block or allow specific traffic passing through from one side of the router to the other. Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Outbound rules (LAN to WAN) determine what outside resources local users can have access to.

The default inbound and outbound rules of the router are:

- **Inbound.** Block all access from outside except responses to requests from the LAN side.
- **Outbound.** Allow all access from the LAN side to the outside.

You can define additional rules that will specify exceptions to the default rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. You can also choose to log traffic that matches or does not match the rule you have defined.

You can change the order of precedence of rules so that the rule that applies most often will take effect first. See “[Order of Precedence for Rules](#)” for more details.

To view or change firewall rules, select Firewall Rules on the main menu.

The screenshot shows the 'Firewall Rules' configuration interface. It features two main sections: 'Outbound Services' and 'Inbound Services'. Each section contains a table with the following columns: '#', 'Enable', 'Service Name', 'Action', 'LAN Users', 'WAN Servers', and 'Log'. Below each table are buttons for 'Add', 'Edit', 'Move', and 'Delete'. At the bottom of the page are 'Apply' and 'Cancel' buttons.

#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
Default	Yes	Any	ALLOW always	Any	Any	Never

#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
Default	Yes	Any	BLOCK always	Any	Any	Never

Figure 3-3

- To edit an existing rule, select its button on the left side of the table and click **Edit**.
- To delete an existing rule, select its button on the left side of the table and click **Delete**.
- To move a rule to a different position in the table, select its button, and then click **Move**. At the prompt, enter the number of the desired new position, and then click **OK**.

Inbound Rules (Port Forwarding)

Because the router uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly access any of your local computers. However, by defining an inbound rule you can make a local server (for example, a Web server or game server) visible and available to the Internet. The rule tells the router to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding.



Note: Some broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP might periodically check for servers and might suspend your account if it discovers any active services at your location. If you are unsure, see the acceptable use policy of your ISP.

Remember that allowing inbound services opens holes in your firewall. Enable only those ports that are necessary for your network. Following are two application examples of inbound rules.

Inbound Rule Example: A Local Public Web Server

If you host a public Web server on your local network, you can define a rule to allow inbound Web (HTTP) requests from outside IP addresses to the IP address of your Web server at any time of day. This rule is shown in the following figure:

The screenshot shows the 'Inbound Services' configuration window. It includes the following fields and values:

- Service:** HTTP(TCP:80)
- Action:** ALLOW always
- Send to LAN Server:** 192 . 168 . 0 . 99
- WAN Users:** Any
- start:** 0 . 0 . 0 . 0
- finish:** 0 . 0 . 0 . 0
- Log:** Never

Buttons at the bottom include Back, Apply, and Cancel.

Figure 3-4

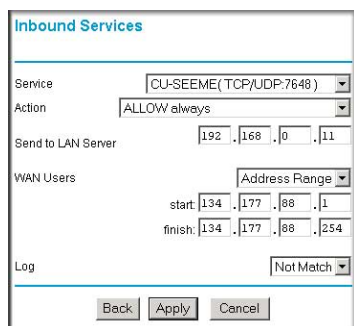
The settings are:

- **Service.** From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the Services screen to add any additional services or applications that do not already appear.

- **Action.** Select when you want this type of traffic to be handled. You can block or allow always, or you can choose to block or allow according to the schedule you have defined in the Schedule screen.
- **Send to LAN Server.** Enter the IP address of the computer or server on your LAN which will receive the inbound traffic covered by this rule.
- **WAN Users.** These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the option that you want:
 - **Any.** All IP addresses are covered by this rule.
 - **Address range.** If this option is selected, you must enter the **Start** and **Finish** fields.
 - **Single address.** Enter the required address in the **Start** field.
- **Log.** You can select whether the traffic will be logged. The choices are:
 - **Never.** No log entries will be made for this service.
 - **Always.** Any traffic for this service type will be logged.
 - **Match.** Traffic of this type that matches the rule will be logged.
 - **Not match.** Traffic of this type that does not match the rule will be logged.

Inbound Rule Example: Allowing Videoconferencing

You can create an inbound rule to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office. In this example, CU-SeeMe connections are allowed only from a specified range of external IP addresses. This example also specifies logging of any incoming CU-SeeMe requests that do not match the allowed parameters.



The screenshot shows the 'Inbound Services' configuration window. The 'Service' dropdown is set to 'CU-SEEME(TCP/UDP:7648)'. The 'Action' dropdown is set to 'ALLOW always'. The 'Send to LAN Server' field contains the IP address '192.168.0.11'. The 'WAN Users' dropdown is set to 'Address Range'. The 'start' field contains '134.177.88.1' and the 'finish' field contains '134.177.88.254'. The 'Log' dropdown is set to 'Not Match'. At the bottom, there are 'Back', 'Apply', and 'Cancel' buttons.

Figure 3-5

Considerations for Inbound Rules

If your external IP address is assigned dynamically by your ISP, the IP address might change periodically as the DHCP lease expires. Consider using the Dynamic DNS feature so that external users can always find your network.

If the IP address of the local server computer is assigned by DHCP, it might change when the computer is rebooted. To avoid this, use the Reserved IP address feature in the LAN IP menu to keep the computer's IP address constant.

Local computers must access the local server using the computer's local LAN address (192.168.0.11 in the previous example). Attempts by local computers to access the server using the external WAN IP address will fail.

Outbound Rules (Service Blocking)

The router allows you to block the use of certain Internet services by computers on your network. This is called service blocking or port filtering. You can define an outbound rule to block Internet access from a local computer based on the following:

- IP address of the local computer (source address)
- IP address of the Internet site being contacted (destination address)
- Time of day
- Type of service being requested (service port number)

Outbound Rule Example: Blocking Instant Messenger

If you want to block Instant Messenger usage by employees during working hours, you can create an outbound rule to block that application from any internal IP address to any external address according to the schedule that you have created in the Schedule screen. You can also have the router log any attempt to use Instant Messenger during that blocked period.

The following screen shows AIM selected in the **Service** list:

The screenshot shows the 'Outbound Services' configuration window. At the top, the title is 'Outbound Services'. Below it, there are several sections:

- Service:** A dropdown menu with 'AIM(TCP:5190)' selected.
- Action:** A dropdown menu with 'BLOCK by schedule, otherwise allow' selected.
- LAN users:** A dropdown menu with 'Any' selected. Below it are 'start' and 'finish' IP address input fields, both currently empty.
- WAN Users:** A dropdown menu with 'Any' selected. Below it are 'start' and 'finish' IP address input fields, both currently empty.
- Log:** A dropdown menu with 'Match' selected.

 At the bottom of the window are three buttons: 'Back', 'Apply', and 'Cancel'.

Figure 3-6

The Outbound Services screen includes the following fields:

- **Service.** Select the application or service from the drop-down list to be allowed or blocked. You can use the Add Custom Service feature to add any additional services or applications that are not in the list; see “[Defining Services](#)” for details.
- **Action.** Choose when you want this type of traffic to be handled. You can block or allow always, or you can block or allow according to the schedule defined in the Schedule screen.
- **LAN users.** This setting determine which packets are covered by the rule, based on their source LAN IP address. Select the desired option:
 - **Any.** All IP addresses are covered by this rule.
 - **Address range.** If this option is selected, you must fill in the **Start** and **Finish** fields.
 - **Single address.** Enter the required address in the Start field.
- **WAN users.** This setting determines which packets are covered by the rule, based on their destination WAN IP address. Select the option that you want:
 - **Any.** All IP addresses are covered by this rule.
 - **Address range.** If this option is selected, you must fill in the **Start** and **Finish** fields.
 - **Single address.** Enter the required address in the **Start** field.
- **Log.** Select whether the traffic will be logged. The choices are:
 - **Never.** No log entries will be made for this service.
 - **Always.** Any traffic for this service type will be logged.
 - **Match.** Traffic of this type that matches the rule will be logged.
 - **Not match.** Traffic of this type that does not match the rule will be logged.

Order of Precedence for Rules

As you define new rules, they are added to the tables in the Firewall Rules screen, as shown:

Outbound Services							
	#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
	1	<input checked="" type="checkbox"/>	AIM	BLOCK by schedule	Any	Any	Match
	Default	Yes	Any	ALLOW always	Any	Any	Never
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Move"/> <input type="button" value="Delete"/>							
Inbound Services							
	#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
	1	<input checked="" type="checkbox"/>	CU-SEEME	ALLOW always	192.168.0.11	134.177.88.1 - 134.177.88.254	Not Match
	2	<input checked="" type="checkbox"/>	HTTP	ALLOW always	192.168.0.99	Any	Never
	Default	Yes	Any	BLOCK always	--	Any	Match
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Move"/> <input type="button" value="Delete"/>							

Figure 3-7

For any traffic attempting to pass through the firewall, the packet information is subjected to the rules in the order shown in the rules table, beginning at the top and proceeding to the default rules at the bottom. In some cases, the order of precedence of two or more rules might be important in determining the disposition of a packet. The Move button allows you to relocate a defined rule to a new position in the table.

Services

Services are functions performed by server computers at the request of client computers. For example, Web servers serve Web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (Web server) request.

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC 1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application.

Although the router already holds a list of many service port numbers, you are not limited to these choices. Use the following procedure to define your own services.

Defining Services

To define a service:

1. Log in to the router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** default password of **password**, or using whatever password and LAN address you have chosen for the router.
2. Under the Content Filtering heading, select Services to display this screen:



Figure 3-8

- To create a new service, click **Add Custom Service**.
 - To edit an existing service, select its button on the left side of the table, and then click **Edit Service**.
 - To delete an existing service, select its button on the left side of the table, and then click **Delete Service**.
3. Use the screen shown in the following figure to define or edit a service.

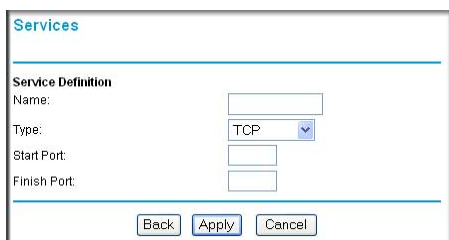


Figure 3-9

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

Setting Times and Scheduling Firewall Services

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 at its default LAN address of **http://192.168.0.1** with its default user name of **admin**, default password of **password**, or using whatever password and LAN address you have chosen for the router.
2. On the main menu, select Schedule to display the Schedule screen:

Figure 3-10

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 **Adjust for daylight savings time** check box.



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

4. The router has a list of NETGEAR NTP servers. If you prefer to use a particular NTP server as the primary server, enter its IP address in the **Use this NTP Server** field.
5. 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 at its default LAN address of **http://192.168.0.1** with its default user name of **admin** default password of **password**, or using whatever password and LAN address you have chosen for the router.
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.

Chapter 4

Managing Your Network

This chapter describes how to perform network management tasks with your 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 at its default LAN address of **http://192.168.0.1** with its default user name of **admin** default password of **password**, or using whatever user name, password and LAN address you have chosen for the router.
2. Under the Maintenance heading on the main menu, select Backup Settings to display the Backup Settings screen:

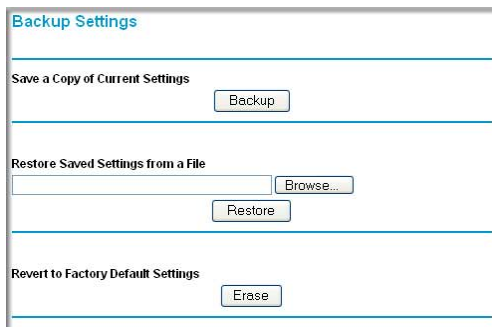


Figure 4-1

3. Click **Backup** 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 at its default LAN address of **http://192.168.0.1** with its default user name of **admin** default password of **password**, or using whatever user name, password and LAN address you have chosen for the router.
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 both the Wireless button and WPS button on the side of the router for 5 seconds.

Upgrading the Router Firmware

The software of the router is stored in flash memory, and can be upgraded as new software 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 later, or Mozilla Firefox 2.0 or later.

2. Log in to the router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** default password of **password**, or using whatever user name, password and LAN address you have chosen for the router.
3. From the main menu, under the Maintenance heading, select Router Upgrade to display this screen:

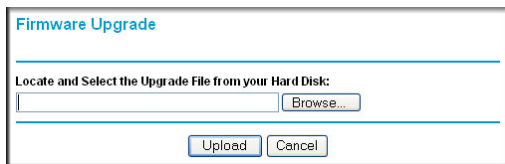



Figure 4-2

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

	<p>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.</p>
---	---

Network Management Information

The router provides a variety of status and usage information which is discussed in the following sections.

Router Status

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

The screenshot displays the Router Status page with the following information:

Router Status	
Firmware Version	V6.00.21.09_RC10
HSDPA	
Modem Identity	AirCard 981U F1_0_0_11AP
Modem SW version	C:\WS\FW\F1_0_0_11AP\MSM7200R3\SRC\AMSS 2007/11/21 20:49:15
Modem driver version	v.1.2.6b
IMSI	310410065357791
IMEI	356685010801031
Operator	AT&T
Network mode	EDGE
WAN Port	
Connection Status	Connected
IP Address	166.129.162.41
Protocol	PPP
IP Subnet Mask	255.255.255.255
Gateway Ip Address	10.64.64.64
Domain Name Server	209.183.54.151 209.183.54.151
LAN Port	
MAC Address	00:1F:33:B3:F3:94
IP Address	192.168.0.1
DHCP	ON
IP Subnet Mask	255.255.255.0
Wireless Port	
Name (SSID)	NETGEAR
Region	USA
Channel	03
Wireless AP	ON
Broadcast Name	ON

At the bottom of the screen, there are three buttons: **Connection Status**, **Refresh**, and **Show Statistics**.

Figure 4-3

The Router Status screen provides status and usage information. This screen shows the following parameters:

Table 4-1. 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 3G modem.
	Operator	The ISP for the broadband wireless network.
	Network mode	The mode of the current network the 3G modem is connected to. This is dependent on coverage and distance from the cell site.
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	<ul style="list-style-type: none"> • 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 2-4.	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:

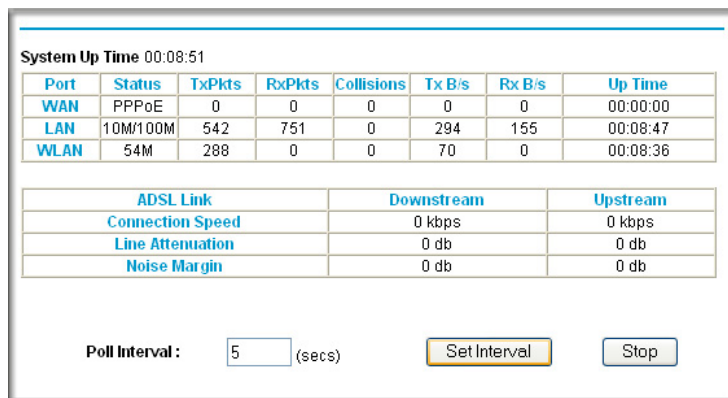


Figure 4-4

This following table explains the statistic fields.

Table 4-2. Router Statistics Fields

Field	Description	
WAN (Internet), LAN, or WLAN (Wireless LAN) statistics	Status	The link status of the port.
	TxPkts	The number of packets transmitted on this port since reset or manual clear.
	RxPkts	The number of packets received on this port since reset or manual clear.
	Collisions	The number of collisions on this port since reset or manual clear.
	Tx B/s	The 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.

Table 4-2. Router Statistics Fields (continued)

Field		Description
ADSL Link Downstream or Upstream These statistics might help your technical support representative if there is a connection problem.	Connection Speed	Typically, the downstream speed is faster than the upstream speed.
	Line Attenuation	The line attenuation increases the further you are physically located from your ISP's facilities.
	Noise Margin	This is the signal-to-noise ratio and is a measure of the quality of the signal on the line.
	Poll Interval	Specifies the interval at which the statistics are updated in this window. Click Stop to freeze the display.

Connection Status

Click the **Connection Status** button on the Router Status screen to view the connection status:

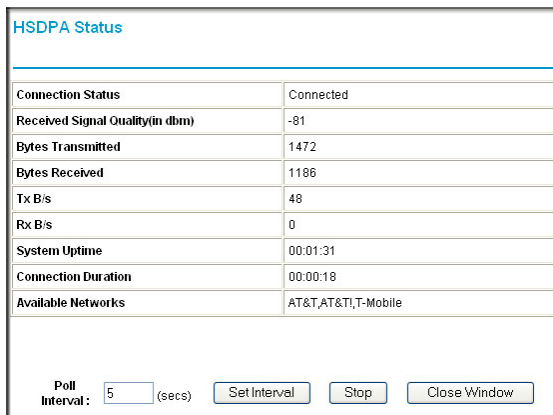


Figure 4-5

This screen shows the following statistics:

Table 4-3. Connection Status Fields for HSDPA Status

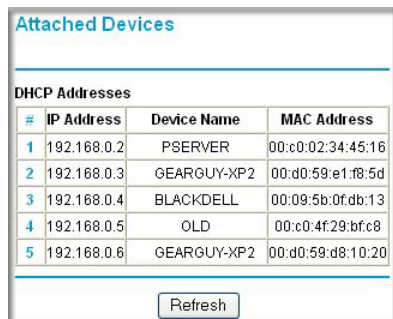
Field	Description
Connection Status	<p>The status of the Internet connection.</p> <ul style="list-style-type: none"> • Scanning. The modem is scanning for broadband wireless networks in your area. • Connected. The router is connected to the Internet. • No USB Device Attached. The router does not detect 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.

Table 4-3. Connection Status Fields for HSDPA Status (continued)

Field	Description
Received Signal Quality (in dbm)	3G 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 contains a table of all IP devices that the router has discovered on the local network. From the main menu, under the Maintenance heading, select Attached Devices. The Attached Devices screen displays:



The screenshot shows a web interface titled "Attached Devices". Below the title is a table with the heading "DHCP Addresses". The table has four columns: "#", "IP Address", "Device Name", and "MAC Address". There are five rows of data. Below the table is a "Refresh" button.

DHCP Addresses			
#	IP Address	Device Name	MAC Address
1	192.168.0.2	PSERVER	00:c0:02:34:45:16
2	192.168.0.3	GEARGUY-XP2	00:d0:59:e1:f8:5d
3	192.168.0.4	BLACKDELL	00:09:5b:0f:db:13
4	192.168.0.5	OLD	00:c0:4f:29:bf:c8
5	192.168.0.6	GEARGUY-XP2	00:d0:59:d8:10:20

Figure 4-6

For each device, the table shows the IP address, device name if available, and the Ethernet MAC address. Note that if the router is rebooted, the table 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. If you enabled e-mail notification, you receive these logs in an e-mail message. If you do not have e-mail notification enabled, you can view the logs here.

An example of the logs file is shown in the following figure:

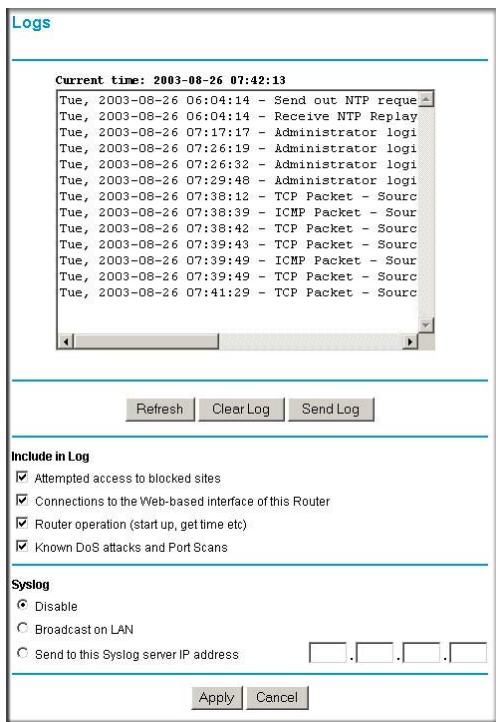


Figure 4-7

Log entries are described in the following table.

Table 4-4. Security Log Entry 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.

Table 4-4. Security Log Entry Descriptions

Field	Description
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.

Log action buttons are described in the following table.

Table 4-5. Log Action Buttons

Field	Description
Refresh	Refresh the log screen.
Clear Log	Clear the log entries.
Send Log	Email the log immediately.
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 Web-based interface of the router
- Router operation (start up, get time, etc.)
- 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:

The screenshot shows the 'E-mail' configuration page. At the top, there is a checkbox labeled 'Turn E-mail Notification On'. Below this, the section 'Send Alerts and Logs Via E-mail' contains several input fields: 'Your Outgoing Mail Server', 'Send To This E-mail Address', 'User Name', and 'Password'. There is also a checkbox for 'My Mail Server requires authentication'. The 'Send E-Mail alerts immediately' section has three checkboxes: 'If a DoS attack is detected.', 'If a Port Scan is detected.', and 'If someone attempts to access a blocked site.'. The 'Send Logs According to this Schedule' section includes a dropdown menu for 'None', a 'Day' dropdown set to 'Sunday', and a 'Time' dropdown set to '12:00' with radio buttons for 'a.m.' and 'p.m.'. At the bottom of the form are 'Apply' and 'Cancel' buttons.

Figure 4-8

- **Turn e-mail notification on.** Select this check box if you want to receive e-mail logs and alerts from the router.
- **Send alerts and logs via email.**
 - **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.
 - **Outgoing Mail Server.** Enter the name or IP address of the outgoing SMTP mail server of your ISP (such as mail.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 e-mail program.

- **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.

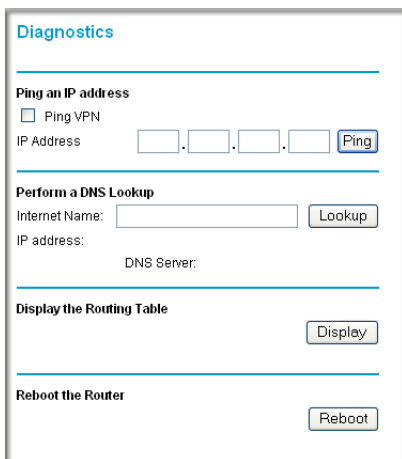
If the **Weekly**, **Daily**, or **Hourly** option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, it is cleared from the router's memory. If the router cannot e-mail the log file, the log buffer might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

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 Router Diagnostics to display the Diagnostics screen:



Diagnostics

Ping an IP address

Ping VPN

IP Address: . . .

Perform a DNS Lookup

Internet Name:

IP address:

DNS Server:

Display the Routing Table

Reboot the Router

Figure 4-9

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 at its default LAN address of **http://192.168.0.1** with its default user name of **admin** default password of **password**, or using whatever user name, password and LAN address you have chosen for the router.

- Under the Advanced heading of the main menu, select Remote Management to display the Remote Management screen:

Figure 4-10

- Select the **Turn Remote Management On** check box.
- 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.

- Specify the port number that will be used for accessing the management interface.

Web browser access normally uses the standard HTTP service port 80. For greater security, you can change the remote management Web interface to a custom port by entering that number in the field provided. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

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

When accessing your router from the Internet, you will 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.

Chapter 5

Advanced Configuration

This chapter describes how to configure the advanced features of your Wireless Router. The following topics are in this chapter:

- “Advanced Wireless Settings”
- “WAN Setup” on page 5-5.
- “LAN IP Settings” on page 5-7.
- “Dynamic DNS” on page 5-11.
- “Using Static Routes” on page 5-13.
- “Universal Plug and Play (UPnP)” on page 5-15.
- “Wireless Bridging and Repeating” on page 5-16.

To view or change these settings, log in to the router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever password and LAN address you have chosen for the router.

Advanced Wireless Settings

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

Figure 5-1

Table 5-1. Advanced Wireless Settings

Advanced Wireless Settings	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.
	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.


Table 5-1. Advanced Wireless Settings (continued)

WPS 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.
Wireless Station Access List	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.


	<p>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.</p>
---	---

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 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:

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



Note: If you configure the Product Family 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.

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

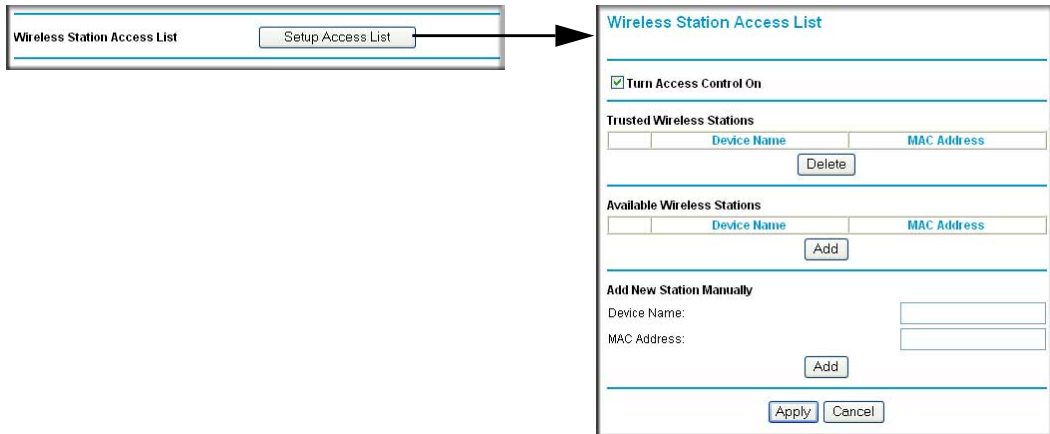



Figure 5-2


The trusted wireless stations listed on this screen are the wireless clients that will have access to the wireless network when the list is enabled.

- Adjust the list as needed for your network. You can add devices to the Trusted Wireless Stations list using either of the following methods:
 - If the computer is in the Available Wireless Stations table, select the radio button of that computer to capture its MAC address.
 - Use the Add New Station Manually 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.
---	--

- Click **Add**, and then click **Apply** to save these settings. Now, only devices on this list will be allowed to wirelessly connect to the Product Family.

WAN Setup

	Note: To change broadband Internet connection settings, use the Broadband Settings screen, as described in “Manually Configuring Your Internet Settings” on page 1-7.
---	--

To view or change the WAN Setup:

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

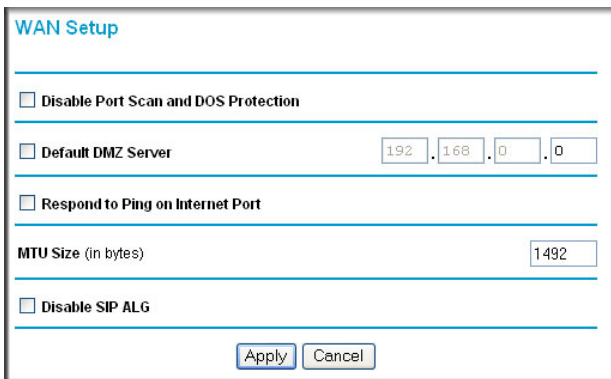


Figure 5-3

- 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 5-2. WAN Setup Settings

Setting	Description
Disable Port Scan and DOS Protection	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 5-6.
Respond to Pin 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.
MTU Size (in bytes)	The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 bytes, or 1492 Bytes for PPPoE connections. For some ISPs you might need to reduce the MTU. This is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

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:



Warning: 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 IP Setup screen:

LAN IP Setup

LAN TCP/IP Setup

IP Address: 192 . 168 . 0 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

RIP Direction: None

RIP Version: Disabled

Use Router as DHCP Server

Starting IP Address: 192 . 168 . 0 . 2

Ending IP Address: 192 . 168 . 0 . 254

Address Reservation

#	IP Address	Device Name	Mac Address

Add Edit Delete

Apply Cancel

Figure 5-4

2. Change the settings. For more information, see [Table 5-3, “DHCP Settings”](#) on page 5-10 or [“Reserved IP Addresses”](#) on page 5-11.
3. Click **Apply** to save the changes.

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

Table 5-3. LAN IP Setup

Settings		Description
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.
	RIP Direction	RIP (Router Information Protocol) allows a router to exchange routing information with other routers. This setting controls how the router sends and receives RIP packets. Both is the default. <ul style="list-style-type: none"> • Both or Out Only. The router broadcasts its routing table periodically. • Both or In Only. The router incorporates the RIP information that it receives. • None. The router will not send any RIP packets and will ignore any RIP packets received.
	RIP Version	This controls the format and the broadcasting method of the RIP packets that the router sends. It recognizes both formats when receiving. By default, this is RIP-1 . <ul style="list-style-type: none"> • RIP-1 is universally supported. It is adequate for most networks, unless you have an unusual network setup. • RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format. RIP-2B uses subnet broadcasting. RIP-2M uses multicasting.
DHCP Server For more information, see "DHCP Settings" on page 5-10.	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 5-10.
	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 5-10.		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. Log in to the router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** default password of **password**, or using whatever user name, password and LAN address you have chosen for the router.
2. From the main menu, select Dynamic DNS to display the Dynamic DNS screen:

Dynamic DNS

Use a Dynamic DNS Service

Service Provider: www.DynDNS.org

Host Name:

User Name:

Password:

Use Wildcards

Apply Cancel Show Status

Figure 5-5

3. 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.

4. Select the **Use a Dynamic DNS Service** check box.
5. Select the name of your dynamic DNS service provider.
6. 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.

7. 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.

8. 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. The static route would look like [Figure 5-7](#).

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.

Configuring Static Routes

1. Log in to the router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever user name, password and LAN address you have chosen for the router.
2. From the main menu, under the Advanced heading, select Static Routes to view the Static Routes screen:

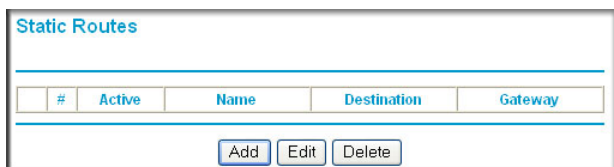


Figure 5-6

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

The screenshot shows the 'Static Routes' configuration page with the following fields and options:

- Route Name: [Text input field]
- Private
- Active
- Destination IP Address: [Four digit input fields separated by dots]
- IP Subnet Mask: [Four digit input fields separated by dots]
- Gateway IP Address: [Four digit input fields separated by dots]
- Metric: [Text input field]

At the bottom of the form are two buttons: 'Apply' and 'Cancel'.

Figure 5-7

4. 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.
5. 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:

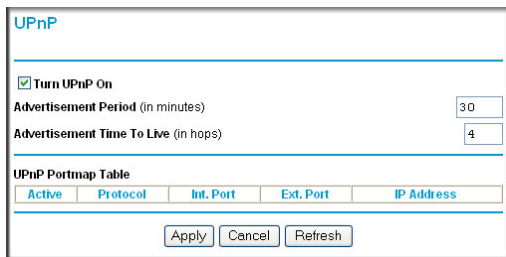


Figure 5-8

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 to display the following screen:

The following screen displays:

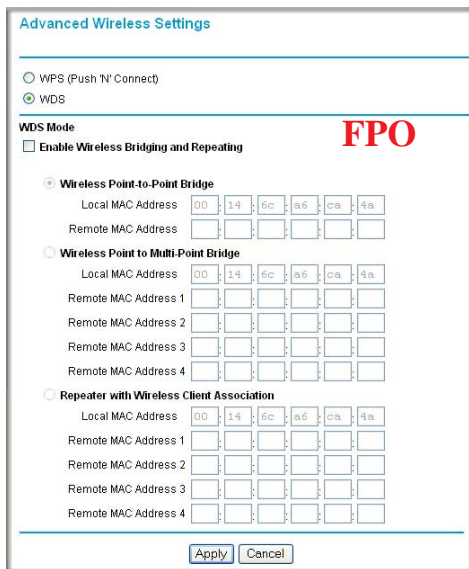


Figure 5-9

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.

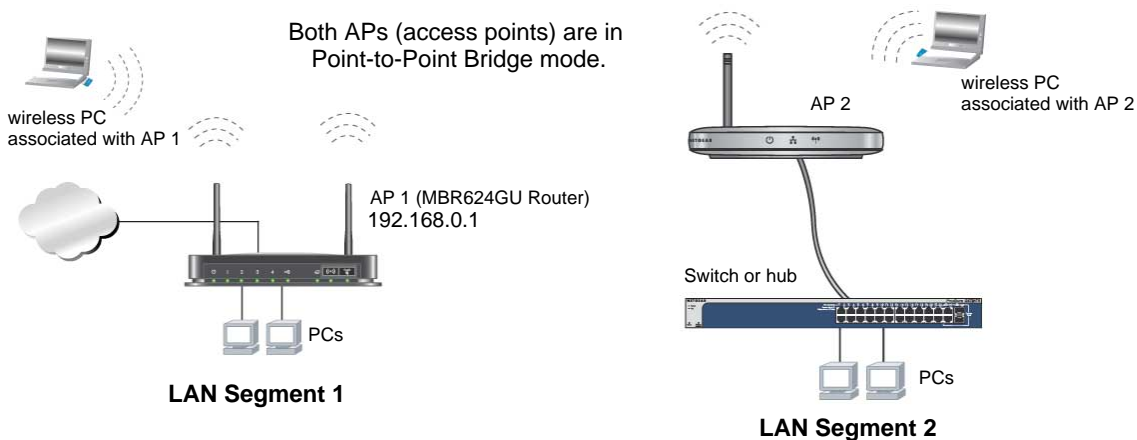


Figure 5-10

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 (shown in [Figure 5-10](#)):

1. Configure the MBRN3000 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 MBRN3000 router must have AP 2's MAC address in its **Remote MAC Address** field, and AP 2 must have the MBRN3000's MAC address in its **Remote MAC Address** field.

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

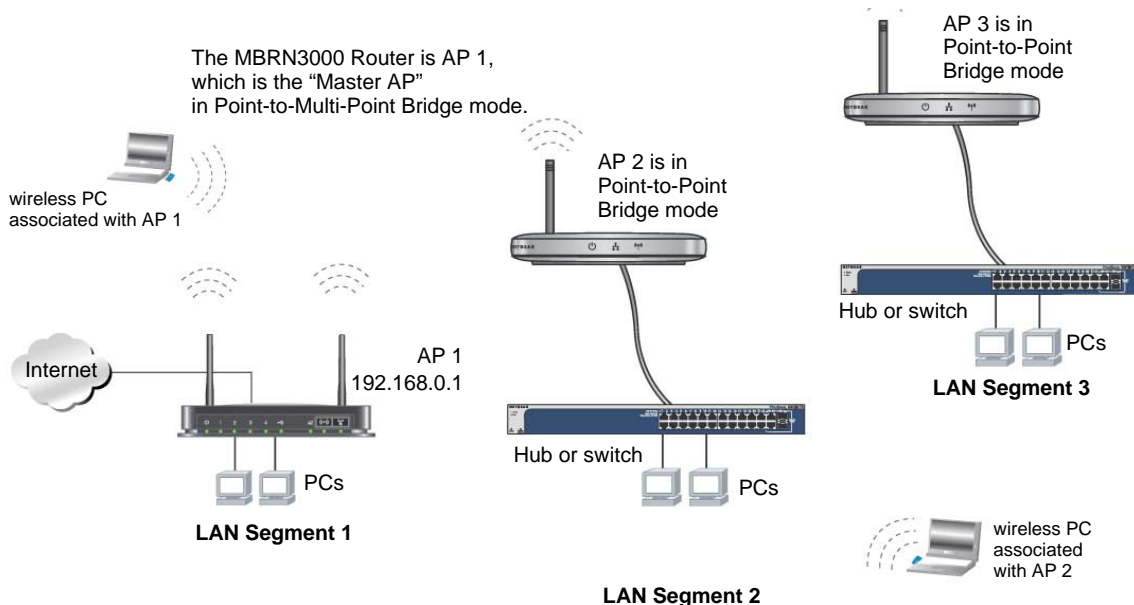


Figure 5-11

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 MBRN3000 router as the Remote MAC Address.
- Using wireless security to protect this traffic.

To set up the multi-point bridge configuration shown in [Figure 5-11](#):

1. Configure the operating mode of the routers.
 - Because it is in a central location, configure the MBRN3000 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 MBRN3000 router.

- Configure the access point (AP3) on LAN Segment 3 in Point-to-Point Bridge mode with the remote MAC address of the MBRN3000 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 AP, the MBRN3000 router in [Figure 5-11](#), is configured in Point-to-Multi-Point Bridge mode; all the others are in Point-to-Point Bridge mode.
 - All APs, including the MBRN3000 router, must be on the same LAN. That is, all the AP LAN IP addresses must be in the same network.
 - All APs, including the MBRN3000 router, must use the same SSID, channel, authentication mode, if any, and encryption in use.
 - All point-to-point APs must have the MAC address of AP 1 (the MBRN3000 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 [Figure 5-11](#) 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 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 Wireless Router as the parent by entering the address of a “child” access point. Note that the following restrictions apply:

- You *do not* have the option of disabling client associations with this Wireless Router.
- You cannot configure a sequence of parent/child APs. You are limited to only one parent AP, although if the MBRN3000 router is the parent AP it can connect with up to four child APs.

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

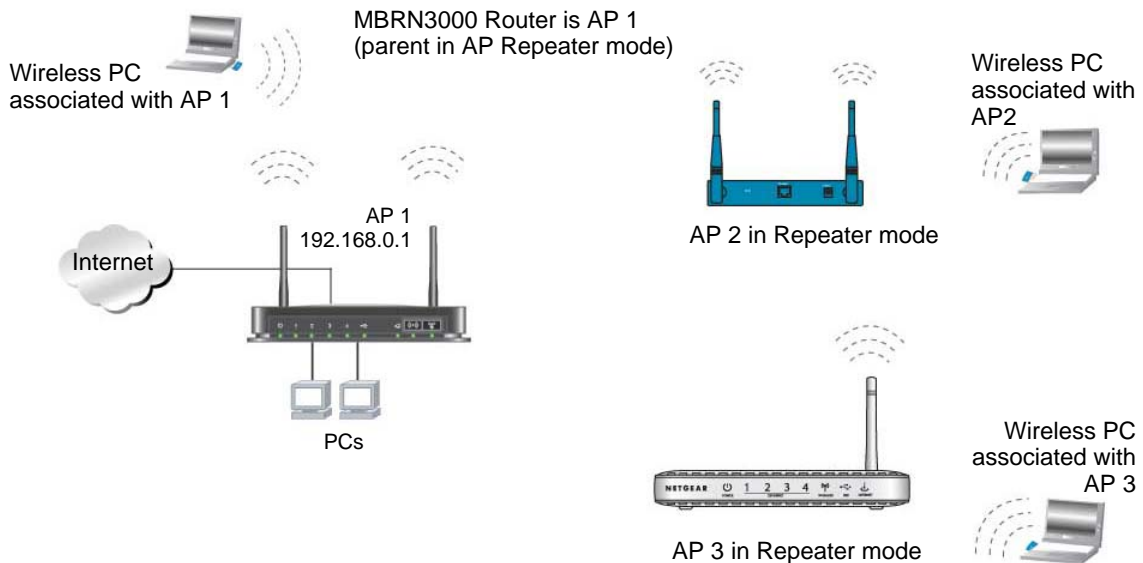


Figure 5-12

To set up a repeater with wireless client association:

1. Configure the operating mode of the devices.
 - Configure AP 1 (the MBRN3000 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 APs must be on the same LAN. That is, the LAN IP addresses for the APs must be in the same subnet.
 - AP 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.

Chapter 6


Troubleshooting

This chapter gives information about troubleshooting your 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 6-1.
- I can’t access the router’s configuration with my browser.
Go to [“Troubleshooting Access to the Router Main Menu”](#) on page 6-2.
- I’ve configured the router but I can’t access the Internet.
Go to [“Troubleshooting the ISP Connection”](#) on page 6-4.
- I want to clear the configuration and start over again.
Go to [“Restoring the Default Configuration and Password”](#) on page 6-7.

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 Ethernet LAN port LEDs are lit for any local ports that 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.
 - c. The USB and Internet LEDs are lit.

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

Table 6-1. Troubleshooting with the LEDs

LED	Action
Power LED is off.	<ul style="list-style-type: none"> • 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	<p>There is a fault within the router. Try to clear the fault as follows:</p> <ul style="list-style-type: none"> • 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 6-7. <p>If the error persists, you might have a hardware problem and should contact technical support.</p>
Internet LED is red.	<p>The router cannot connect to the Internet.</p> <ul style="list-style-type: none"> • Make sure the USB LED is lit, indicating that the wireless modem is securely connected to the router. • Your wireless modem must be activated and there must be coverage in your area. To test coverage, connect your modem to your PC, and try to connect to the Internet directly from your computer. • Check the NETGEAR website to ensure that your wireless modem is supported. • Close the 3G Connection manager if it is running on your PC.
LAN LEDs are off.	<p>If these LEDs do not light when the Ethernet connection is made, check the following:</p> <ul style="list-style-type: none"> • 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.

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 [“Preparing a Computer for Network Access”](#) in [Appendix B](#) to 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 6-7](#).
- 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

Obtaining a WAN IP Address

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

To check the WAN IP address:

1. Launch your browser, and select an external site such as www.netgear.com.
2. Access the router main menu at **<http://192.168.0.1>**.
3. Under the Maintenance heading, check that an IP address is shown for the WAN port. If 0.0.0.0 is shown, your router has not obtained an IP address from your ISP.

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

- Your ISP might require a multiplexing method or virtual path identifier or virtual channel identifier parameter.
Verify with your ISP the multiplexing method and parameter value, and update the router's ADSL settings accordingly.
- Your ISP might require a login program.
Ask your ISP whether they require PPP over Ethernet (PPPoE) or PPP over ATM (PPPOA) login.
- If you have selected a login program, the service name, user name, and password might be set incorrectly. See "[Troubleshooting PPPoE or PPPoA](#)", below.
- Your ISP might check for your computer's host name.
Assign the computer host name of your ISP account to the router in the browser-based Setup Wizard.
- Your ISP only allows one Ethernet MAC address to connect to Internet, and might check for your computer's MAC address. In this case try either of the following:
 - Inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.
 - Configure your router to spoof your computer's MAC address. This can be done in the Basic Settings screen.

Troubleshooting PPPoE or PPPoA

The PPPoE or PPPoA connection can be debugged as follows:

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

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



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

Troubleshooting Internet Browsing

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

- Your computer might not recognize any DNS server addresses.

A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your computer and verify the DNS address as described in [“Preparing a Computer for Network Access” 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 [“Preparing a Computer for Network Access” 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 6-1 on page 6-2](#).
 - 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 [“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 administration password to **password** and the IP address to **192.168.0.1**. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function (see [“Backing Up, Restoring, or Erasing Your Settings” on page 4-1](#)).

- Press both the Wireless button and WPS button on the side of the router for 5 seconds. Use this method for cases when the administration password or IP address is not known.



Note: Pressing the reset button on the router reboots the unit but does not restore the factory default settings.

Problems with Date and Time

The E-mail screen in the Content Filtering section displays the current date and time of day. The 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.

Appendix A

Technical Specifications and Factory Default Settings

This appendix provides technical specifications for the Mobile Broadband Wireless-N Router MBRN3000.

Network Protocol and Standards Compatibility

Data and Routing Protocols: 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 (32° to 104° F)
Operating humidity: 90% maximum relative humidity, noncondensing

Electromagnetic Emissions

Meets requirements of: 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

Factory Default Settings

You can use the Restore Factory Settings button that is 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 configuration 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
	Time zone adjusted for daylight saving time	Disabled
Firewall		

Feature		Default Behavior
	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the http port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled
Wireless		
	Wireless communication	Enabled
	SSID name	NETGEAR
	Security	Disabled
	Broadcast SSID	Enabled
	Transmission speed	Auto*
	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

*. 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.

Appendix B

Related Documents

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
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