

NETGEAR®

Mobile LTE Broadband 11n Wireless Router MBR1516 User Manual

ENGLISH

Routeur sans fil 11n LTE à haut débit mobile MBR1516 Guide de l'utilisateur

FRANÇAIS



350 East Plumeria Drive
San Jose, CA 95134
USA

September 2012
202-11159-01
v1.0

© 2012 NETGEAR, Inc. All rights reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of NETGEAR, Inc.

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, or get support online, visit us at <http://support.netgear.com/general/contact/default.aspx>.

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

Phone (Other Countries): See support information card.

Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. Other brand and product names are registered trademarks or trademarks of their respective holders. © 2012 NETGEAR, Inc. All rights reserved.

Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Contents

Chapter 1 Hardware Setup

Unpack Your Router	7
Hardware Features	8
Front Panel	8
Back Panel	10
Label	11
Restore Factory Settings	11
Insert the SIM Card	12
Install Optional External Antennas	12
Position Your Router	14

Chapter 2 Getting Started with NETGEAR genie

Router Setup Preparation	16
Use Standard TCP/IP Properties for DHCP	16
Wireless Devices and Security Settings	16
Types of Logins and Access	16
NETGEAR genie Setup	16
Use NETGEAR genie after Installation	18
Upgrade Router Firmware	18
Router Dashboard (BASIC Home Screen)	19
Add Wireless Devices or Computers to Your Network	20
Manual Method	20
Wi-Fi Protected Setup (WPS) Method	20

Chapter 3 NETGEAR genie BASIC Settings

Internet Setup	22
Internet Setup Screen Fields	22
Wireless Settings	24
Wireless Settings Screen Fields	25
Change WPA Security Option and Passphrase	26
Attached Devices	26
Parental Controls	27
SMS Message	30
View SMS Messages	30
Send SMS Messages	31

Chapter 4 NETGEAR genie ADVANCED Home

Setup Wizard	33
WPS Wizard	34
Setup Menu	35
Broadband Settings	36
Mobile Broadband Settings	36
WAN Setup	38
Default DMZ Server	39
Change the MTU Size	39
LAN Setup	41
LAN Setup Screen Settings	42
Use the Router as a DHCP Server	42
Address Reservation	43
Quality of Service Setup	44

Chapter 5 Security

Keyword Blocking of HTTP Traffic	50
Block Services (Port Filtering)	51
Schedule Blocking	53
Security Event Email Notifications	54

Chapter 6 Administration

Router Status	56
Logs	60
Attached Devices	60
Backup Settings	60
Back Up Settings	61
Restore Configuration Settings	61
Erase	61
Set Password	62
Password Recovery	62
Diagnostics	63
Router Upgrade	64
Module Upgrade	65

Chapter 7 Advanced Settings

SIM Settings	68
SMS Messages	68
Wireless Settings	69
Wireless Repeating	71
Wireless Repeating Function	72
Set Up the Base Station	73
Set Up a Repeater Unit	73

Port Forwarding and Port Triggering	74
Remote Computer Access Basics	74
Port Triggering to Open Incoming Ports	76
Port Forwarding to Permit External Host Communications	77
How Port Forwarding Differs from Port Triggering	78
Set Up Port Forwarding to Local Servers	78
Set Up Port Triggering	80
Dynamic DNS	82
Static Routes	83
Remote Management	85
Universal Plug and Play	86
Traffic Meter	88

Chapter 8 Troubleshooting

Basic Functioning	90
Troubleshoot Access to the Router Main Menu	92
Troubleshoot the ISP Connection	93
Connect to the Internet	93
Troubleshoot Internet Browsing	95
Troubleshoot a TCP/IP Network Using the Ping Utility	95
Test the LAN Path to Your Router	95
Test the Path from Your Computer to a Remote Device	96
Problems with Date and Time	97
Restore the Default Configuration and Password	97

Appendix A Supplemental Information

Factory Default Settings	99
Technical Specifications	101

Appendix B Notification of Compliance

Index

Hardware Setup

1

Getting to know your router

The Mobile LTE Broadband 11n Wireless Router MBR1516 provides you with an easy and secure way to set up a wireless home network with fast access to the Internet over the high-speed 4G wireless (LTE/HSPA+) network. It lets you block unsafe Internet content and applications and protects the devices (computers, gaming consoles, and so on) that you connect to your home network.

If you have not already set up your new router using the installation guide that comes in the box, this chapter walks you through the hardware setup. [Chapter 3, NETGEAR genie BASIC Settings](#), explains how to set up your Internet connection.

This chapter contains the following sections:

- [Unpack Your Router](#)
- [Hardware Features](#)
- [Insert the SIM Card](#)
- [Install Optional External Antennas](#)
- [Position Your Router](#)

For more information about the topics covered in this manual, visit the support website at <http://support.netgear.com/general/contact/default.aspx>.

Unpack Your Router

Open the box and remove the router, cables, and installation guide.

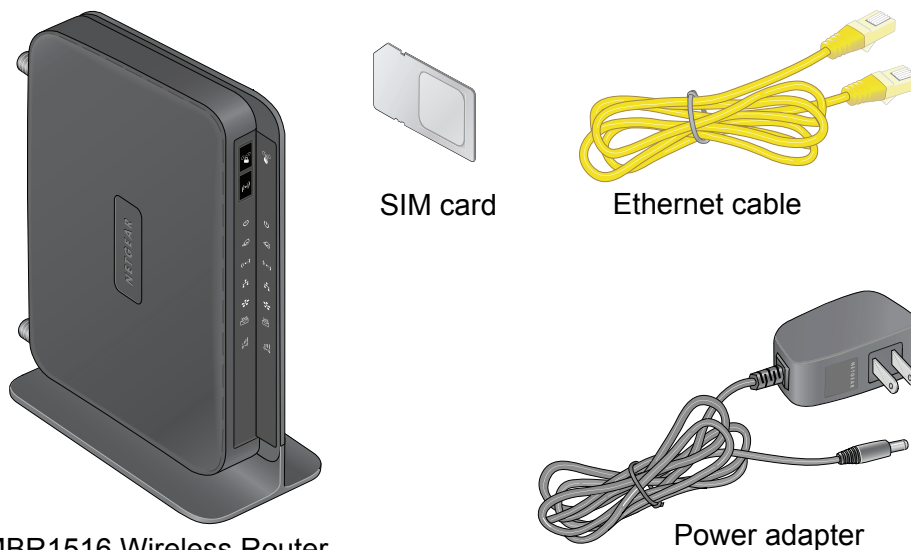


Figure 1. Check the package contents

Your box should contain the following items:

- Mobile LTE Broadband 11n Wireless Router MBR1516
- AC power adapter (plug varies by region)
- Category 5 (Cat 5) Ethernet cable
- Installation guide with cabling and router setup instructions

If any parts are incorrect, missing, or damaged, contact your service provider. Keep the carton and original packing materials, in case you need to return the product for repair.

Hardware Features

Before you cable your router, take a moment to become familiar with the label and the front and back panels. Pay particular attention to the LEDs on the front panel.

Front Panel

The router front panel contains control buttons and status LEDs. Use the LEDs to verify status and connections.

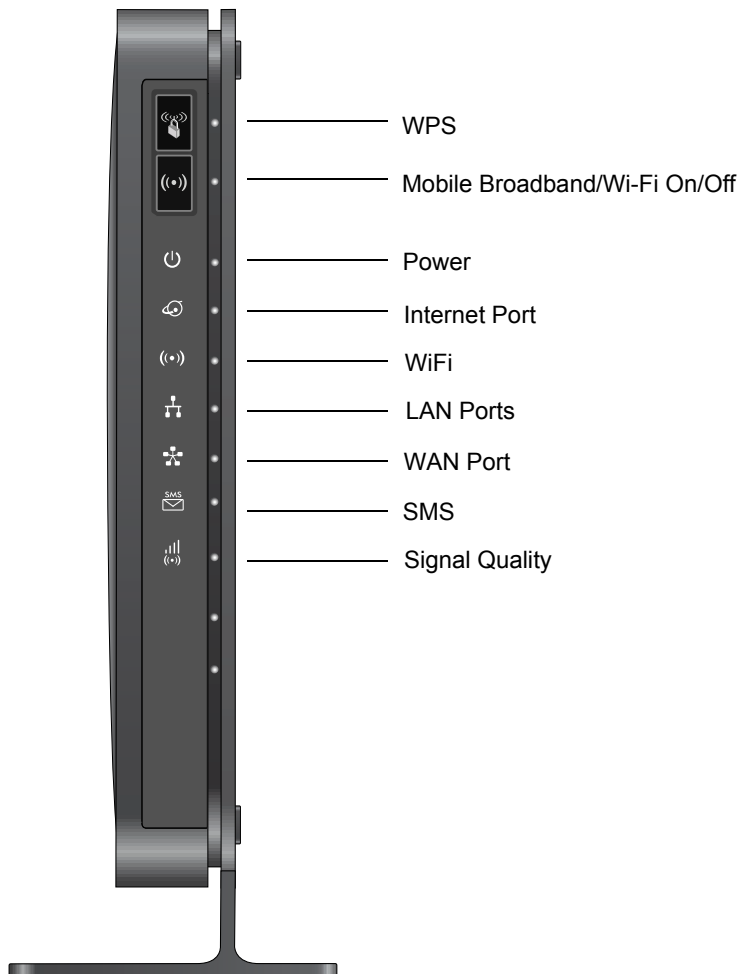


Figure 2. Router, front view

[Table 1](#) describes each LED and button located on the front panel of the router.

Table 1. LED descriptions

LED	Activity	Description
WPS 	Press the WPS button to open a 2-minute window for the router to connect with other WPS-enabled devices. For more information about this function, see Wi-Fi Protected Setup (WPS) Method on page 20.	
WiFi On/Off 	This button can be used to control the WiFi radio or both the WiFi radio and mobile broadband radio. Use the router interface to select the options. The default is set for WiFi radio only.	
Power 	Solid green	The router is turned on and operating normally.
	Solid amber	POST (power-on self-test) is in progress.
	Off	Power is not supplied to the router.
Internet Port 	Solid green	There is an Internet session.
	Solid amber	Traffic meter limit has been reached; traffic is blocked.
	Blinking green	Data is being transmitted over the Internet connection.
	Blinking amber	Traffic meter limit has been reached, but traffic is not blocked.
	Blinking green and amber	Failover from Ethernet WAN to mobile broadband.
	Off	No Internet connection is detected.
WiFi 	Solid blue	The WiFi local port is initialized.
	Blinking blue	Data is being transmitted or received over the WiFi link.
	Off	The wireless access point is turned off.
LAN Ports 	Solid green	The local Ethernet ports have detected wired links with computers.
	Blinking	Data is being transmitted or received.
	Off	No link is detected on these ports.
WAN Port 	Solid green	The Ethernet WAN port has detected an active link.
	Blinking	Data is being transmitted or received.
	Off	No link is detected on these ports.
SMS 	Solid green	SMS messages are waiting.
	Off	There are no unread SMS messages.

Table 1. LED descriptions (continued)

LED	Activity	Description
Signal Quality 	Solid blue	Excellent coverage is detected.
	Solid green	Good coverage is detected.
	Solid amber	Marginal coverage is detected.
	Off	No coverage is detected.

Back Panel

The back panel of the router contains port connections.

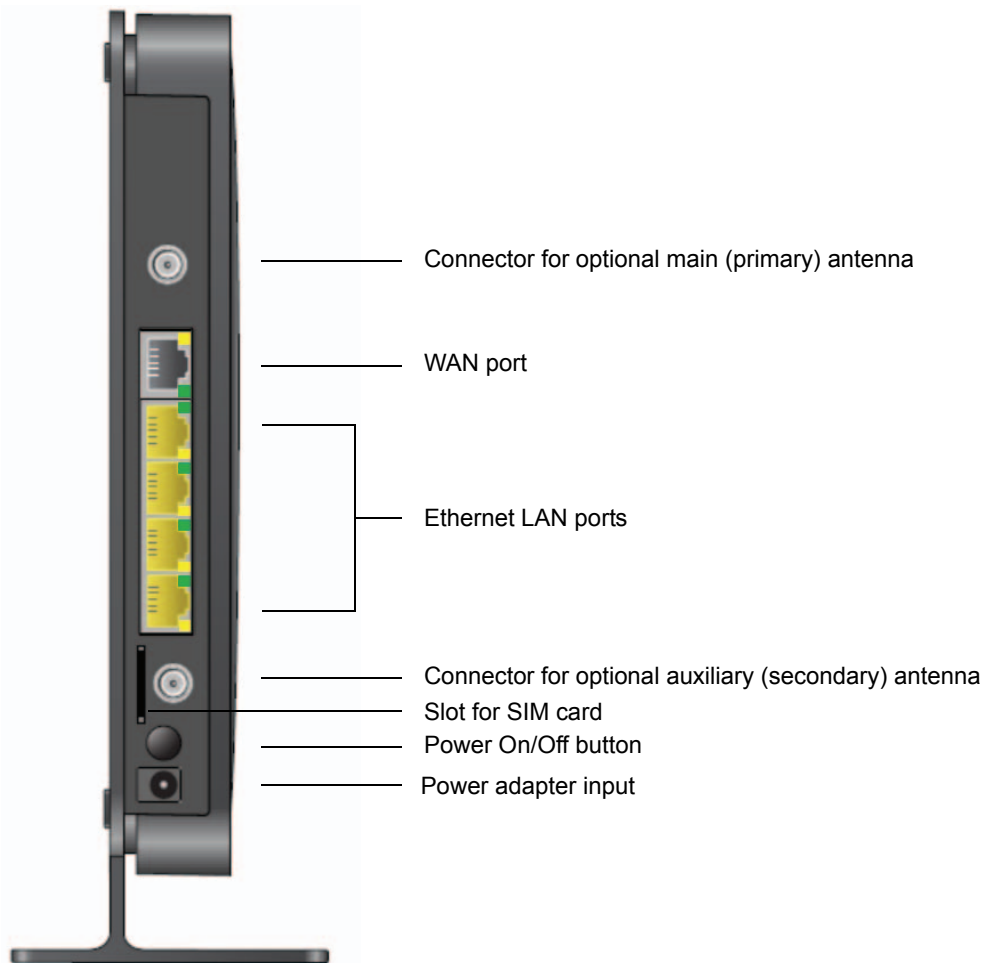


Figure 3. Router, rear view

Label

The label on the side of the router shows the router's MAC address, serial number, security PIN, IMEI or ESN number, and factory default login information. It also contains the SSID and passphrase that are unique to each router.

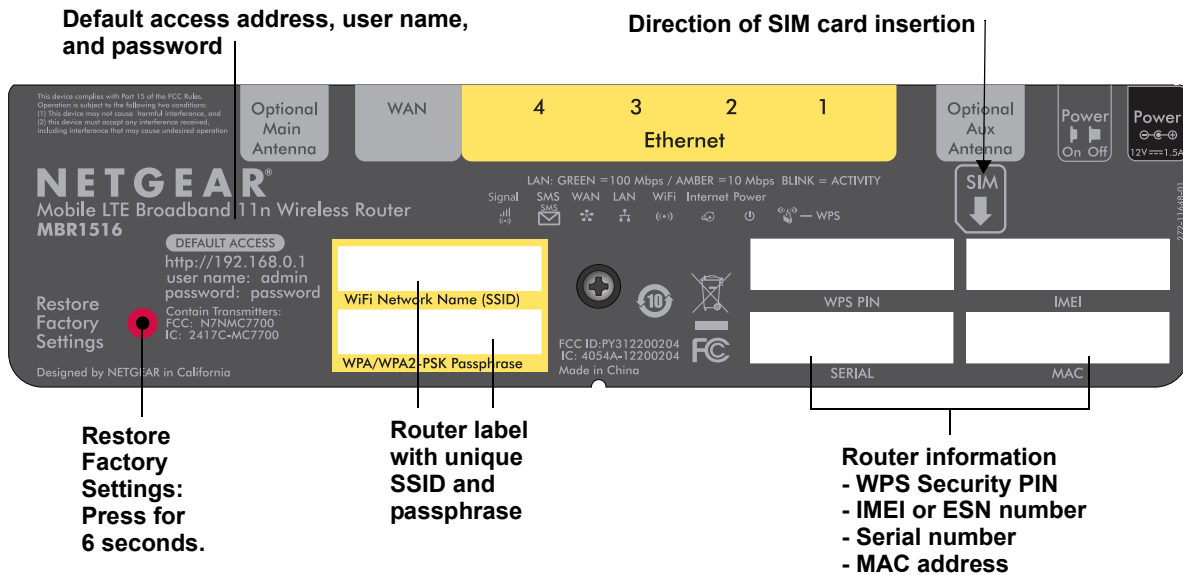


Figure 4. The label shows unique information about your router

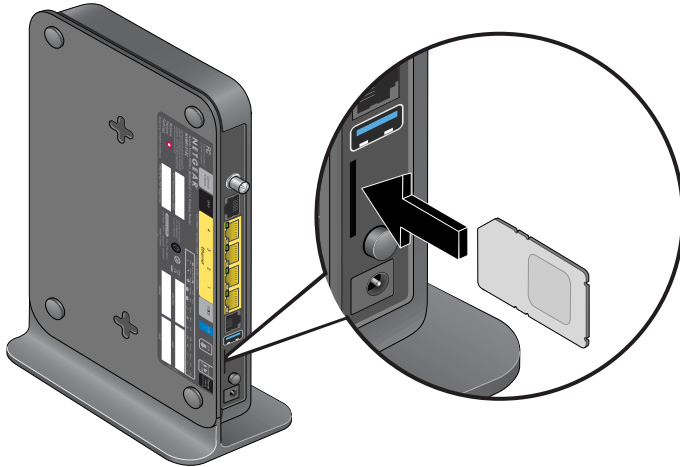
Restore Factory Settings



Locate the small hole outlined in red on the side of the router. Insert a paper clip into the hole and press for 6 seconds. Pressing the Restore Factory Settings button causes the LED to blink briefly. After the button is held down for more than 6 seconds, the Power LED flashes amber, and then turns green as the router resets to the factory defaults. See [Factory Default Settings](#) on page 99 for information about the factory default settings.

Insert the SIM Card

Gently insert the SIM card into the SIM card slot on the back of the router. You should hear a “click” sound when the SIM card has been inserted properly.

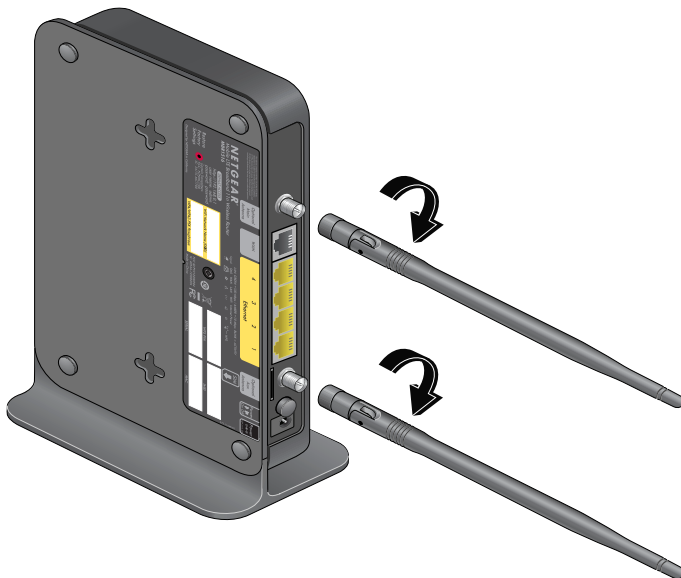


Install Optional External Antennas

For improved performance, connect an external antenna to the main (primary) antenna port. For best 4G LTE performance, connect two external antennas to provide diversity.

➤ **To install the optional external antennas:**

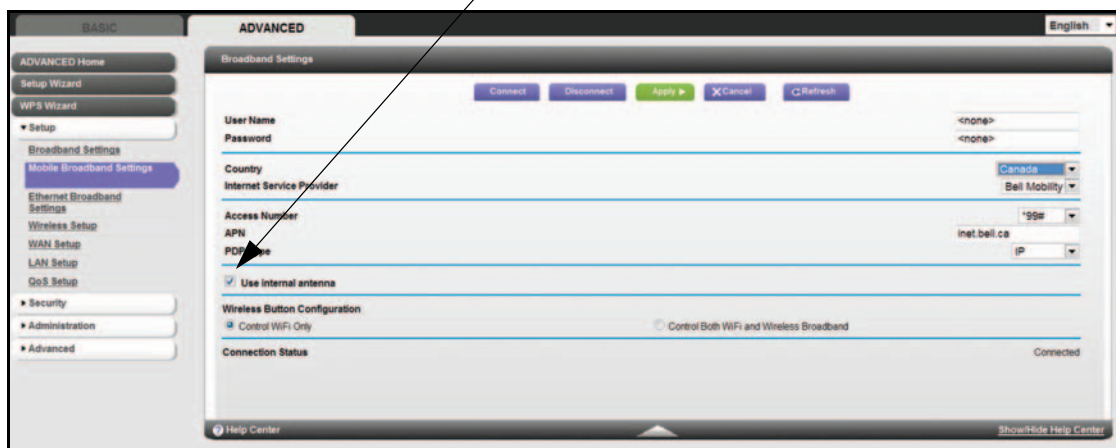
1. To improve signal strength, purchase optional external antennas and install them on the back of the router.



2. Position the antennas so that they are at right angles to each other.



3. After you log in to the router (see [NETGEAR genie Setup](#) on page 16 for more information), clear the **Use Internal Antennas** check box on the Broadband Setting screen and click **Apply**. See [Mobile Broadband Settings](#) on page 36 for more information about this screen.



Position Your Router

The router lets you access your network from virtually anywhere within the operating range of your wireless network. However, the operating distance or range of your wireless connection can vary significantly depending on the physical placement of your router. For example, the thickness and number of walls the wireless signal passes through can limit the range.

Use the Signal Quality LED on the front panel to position the router for best signal strength. Also for best results, place your router:

- On an upper floor of a multi-floor home or office.
- Close to a window but avoiding direct sunlight. A window location gives the best conditions for receiving a strong 4G signal strength.
- Near the center of the area where your computers and other devices operate, and preferably within line of sight to your wireless devices.
- So it is accessible to an AC power outlet and near Ethernet cables for wired computers.
- In an elevated location such as a high shelf, keeping the number of walls and ceilings between the router and your other devices to a minimum.
- Away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, computers, or the base of a cordless phone or 2.4 GHz cordless phone.
- Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.

When you use 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).

Getting Started with NETGEAR genie

2

Connecting to the router

This chapter explains how to use NETGEAR genie to set up your router after you complete cabling as described in the installation guide and in the previous chapter in this book.

This chapter contains the following sections:

- *Router Setup Preparation*
- *Types of Logins and Access*
- *NETGEAR genie Setup*
- *Use NETGEAR genie after Installation*
- *Upgrade Router Firmware*
- *Router Dashboard (BASIC Home Screen)*
- *Add Wireless Devices or Computers to Your Network*

Router Setup Preparation

You can set up your router with the NETGEAR genie automatically, or you can use the NETGEAR genie menus and screens to set up your router manually. However, before you start the setup process, you need to have your ISP information on hand and make sure the laptops, computers, and other devices in the network have the settings described here.

Use Standard TCP/IP Properties for DHCP

If you set up your computer to use a static IP address, you need to change the settings so that it uses Dynamic Host Configuration Protocol (DHCP).

Wireless Devices and Security Settings

Make sure that the wireless device or computer that you are using supports WPA or WPA2 wireless security, which is the wireless security supported by the router.

Types of Logins and Access

There are separate types of logins that have different purposes. It is important that you understand the difference so that you know which login to use when.

- **Router login** logs you in to the router interface from NETGEAR genie. See [Use NETGEAR genie after Installation](#) on page 18 for details about this login.
- **Wireless network key or password.** Your router is preset with a unique wireless network name (SSID) and password for wireless access. This information is on the label located on the bottom of your router.

NETGEAR genie Setup

NETGEAR genie runs on any device with a web browser. It is the easiest way to set up the router because it automates many of the steps and verifies that those steps have been successfully completed. It takes about 15 minutes to complete.

➤ To use NETGEAR genie to set up your router:

1. Turn the router on by pressing the **On/Off** button, if not done yet.
2. Make sure that your device is connected with an Ethernet cable (wired) or wirelessly (with the preset security settings listed on the bottom label) to your router.
3. Launch your Internet browser.
 - If this is the first time you are setting up the Internet connection for your router, the browser automatically goes to <http://192.168.0.1>, and the NETGEAR genie screen displays.

- If you already used the NETGEAR genie, type **http://192.168.0.1** in the address field for your browser to display the NETGEAR genie screen. See [Use NETGEAR genie after Installation](#) on page 18.
4. Follow the onscreen instructions to complete NETGEAR genie setup. NETGEAR genie guides you through connecting the router to the Internet.

If the browser cannot display the web page:

- Make sure that the computer is connected to one of the four LAN Ethernet ports, or wirelessly to the router.
- Make sure that the router is ready to use. Its Power LED should turn on.
- Close and reopen the browser to make sure the browser does not cache the previous page.
- Browse to **http://192.168.0.1**.
- If the computer is set to a static or fixed IP address (this is uncommon), change it to obtain an IP address automatically from the router.

If the router does not connect to the Internet:

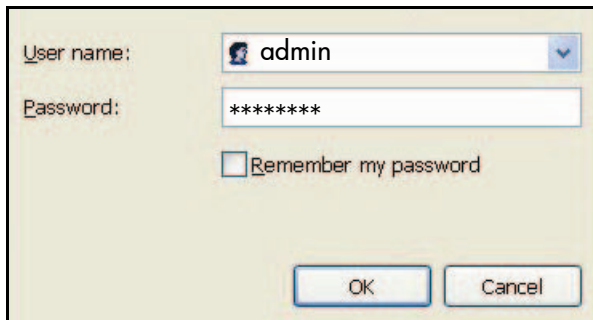
1. Review your settings to be sure that you have selected the correct options and typed everything correctly.
2. Contact your ISP to verify that you have the correct configuration information.
3. Read [Chapter 8, Troubleshooting](#). If problems persist, register your NETGEAR product and contact NETGEAR technical support.

Use NETGEAR genie after Installation

When you first set up your router, NETGEAR genie automatically starts when you launch an Internet browser on a computer that is connected to the router. You can use NETGEAR genie again if you want to view or change settings for the router.

1. Launch your browser from a computer or wireless device that is connected to the router.
2. Type **http://192.168.0.1**.

The login screen displays:

A screenshot of the NETGEAR login screen. It features a light yellow background with a thin black border. At the top left, the text 'User name:' is followed by a text box containing 'admin' and a small blue dropdown arrow. Below this, the text 'Password:' is followed by a text box containing seven asterisks '*****'. Under the password box is a checkbox labeled 'Remember my password'. At the bottom right are two buttons: 'OK' and 'Cancel'.

3. Enter **admin** for the router user name and **password** for the router password, both in lowercase letters.

Note: The router user name and password are different from the user name and password for logging in to your Internet connection. See [Types of Logins and Access](#) on page 16 for more information.

Upgrade Router Firmware

When you set up your router and are connected to the Internet, the router automatically checks for you to see if newer firmware is available. If it is, a message is displayed on the top of the screen. See [Router Upgrade](#) on page 64 for more information about upgrading firmware.

Click the message when it appears, and click **Yes** to upgrade the router with the latest firmware. After the upgrade, the router restarts.



CAUTION:

Do not try to go online, turn off the router, shut down the computer, or do anything else to the router until the router finishes restarting and the Power LED has stopped blinking for several seconds.

Router Dashboard (BASIC Home Screen)

The router BASIC Home screen has a dashboard that lets you see the status of your Internet connection and network at a glance. You can click any of the five sections of the dashboard to view more detailed information. The left column has the menus, and at the top there is an ADVANCED tab that is used to access additional menus and screens.

Menus (Click the ADVANCED tab to view more)

Language

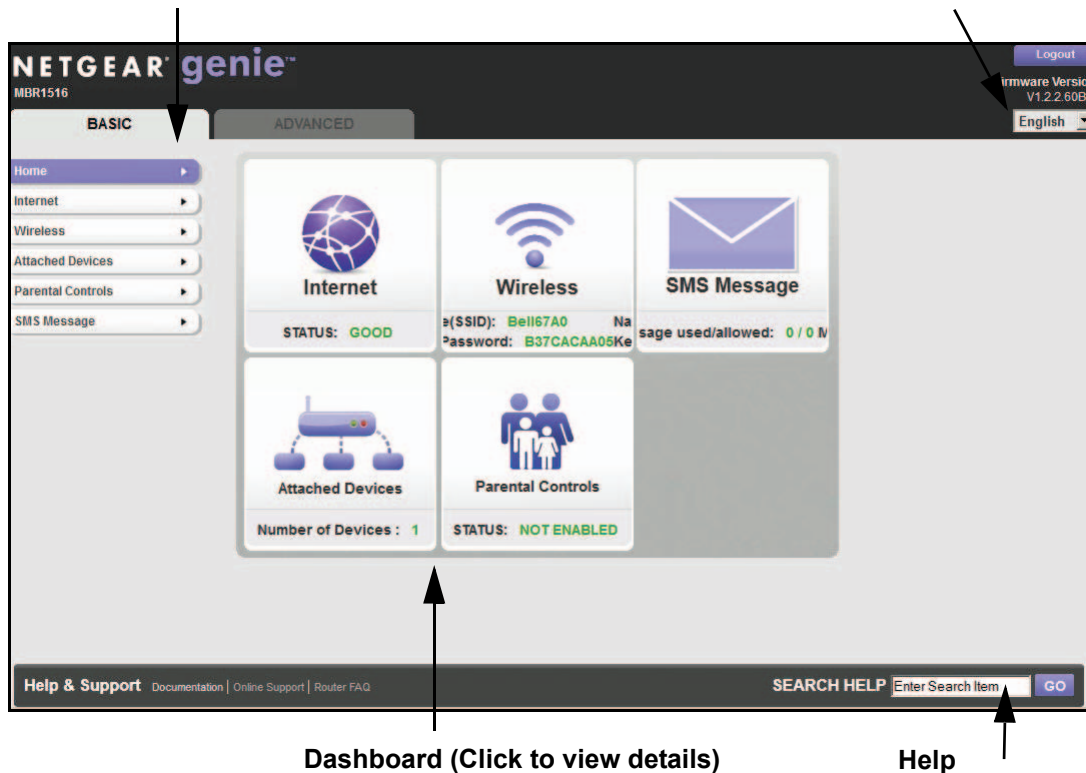


Figure 5. Router BASIC Home screen with dashboard, language, and online help

- **Home.** This dashboard screen displays when you log in to the router.
- **Internet.** Set, update, and check the ISP settings of your router.
- **Wireless.** View or change the wireless settings for your router.
- **Attached Devices.** View the devices connected to your network.
- **Parental Controls.** Download and set up parental controls to prevent objectionable content from reaching your computers.
- **SMS Message.** Send and receive SMS messages.
- **ADVANCED tab.** Set the router up for unique situations such as when remote access by IP or by domain name from the Internet is needed. See [Chapter 7, Advanced Settings](#). Using this tab requires a solid understanding of networking concepts.
- **Help & Support.** Go to the NETGEAR support site to get information, help, and product documentation. These links work once you have an Internet connection.

Add Wireless Devices or Computers to Your Network

Choose either the manual or the WPS method to add wireless devices and other equipment to your wireless network.

Manual Method

➤ **To connect manually:**

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

Wi-Fi Protected Setup (WPS) Method

Wi-Fi Protected Setup (WPS) is a standard for easily adding computers and other devices to a home network while maintaining security. To use WPS, make sure that all wireless devices to be connected to the network are Wi-Fi certified and support WPS. During the connection process, the client gets the security settings from the router so that every device in the network has the same security settings.

➤ **To use WPS to join the wireless network:**

If your wireless device supports WPS (Push 'N' Connect), follow these steps:

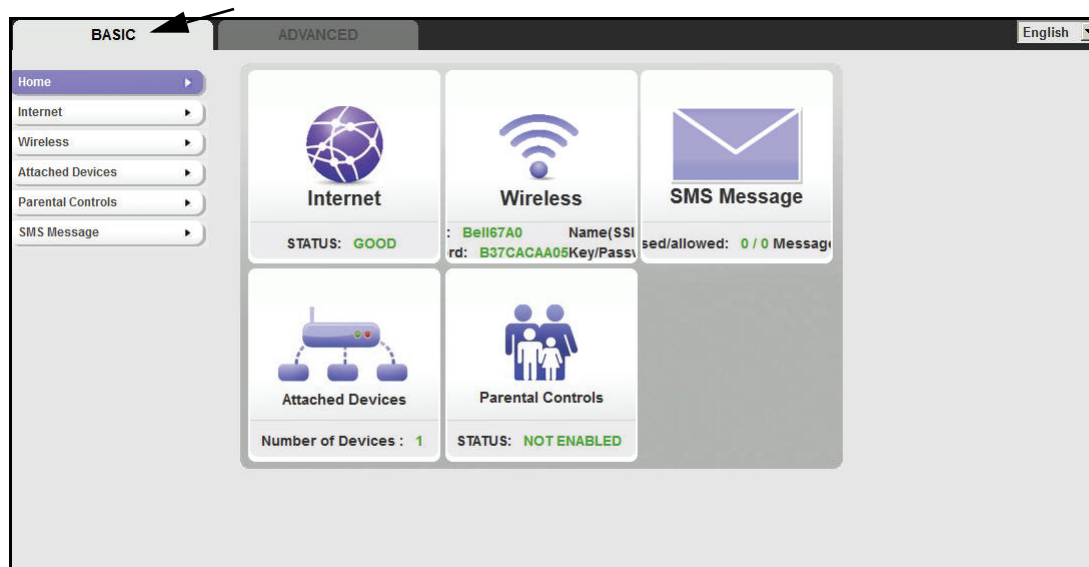
1. Press the **WPS** button on the router front panel.
2. Within 2 minutes, press the **WPS** button on your wireless device, or follow the WPS instructions that came with the device. The device is now connected to your router.
3. Repeat steps 1–2 to add other WPS wireless devices.

NETGEAR genie BASIC Settings

3

Your Internet connection and network

This chapter explains the features available from the NETGEAR genie BASIC Home screen, shown in the following figure:



This chapter contains the following sections:

- [*Internet Setup*](#)
- [*Wireless Settings*](#)
- [*Attached Devices*](#)
- [*Parental Controls*](#)
- [*SMS Message*](#)

Internet Setup

The Internet Setup screen is where you view or change ISP information.

1. From the Home screen, select **Internet**. The following screen displays:

The fields that display in the Internet Setup screen depend on whether or not your Internet connection requires a login.

- **Yes.** Select the encapsulation method and enter the login name. If you want to change the login time-out, enter a new value in minutes.
 - **No.** Enter the account and domain names, only if needed.
2. Enter the settings for the IP address and DNS server. The default settings usually work fine. If you have problems with your connection, check the ISP settings.
 3. Click **Apply** to save your settings.
 4. Click **Test** to test your Internet connection. If the NETGEAR website does not display within 1 minute, see [Chapter 8, Troubleshooting](#).

Internet Setup Screen Fields

The following descriptions explain all of the possible fields in the Internet Setup screen. Note that which fields display in this screen depends on whether or not an ISP login is required.

Does Your ISP Require a Login? Answer either yes or no.

These fields display when no login is required:

- **Account Name (If required).** Enter the account name provided by your ISP. This might also be called the host name.
- **Domain Name (If required).** Enter the domain name provided by your ISP.

These fields display when your ISP requires a login:

- **Internet Service Provider Encapsulation.** ISP types. The choices are PPPoE, PPTP, or L2TP.
- **Login.** The login name provided by your ISP. This is often an email address.
- **Password.** The password that you use to log in to your ISP.
- **Idle Timeout (In minutes).** If you want to change the login time out, enter a new value in minutes. This determines how long the router keeps the Internet connection active after there is no Internet activity from the LAN. Entering a value of 0 (zero) means never log out.

Internet IP Address.

- **Get Dynamically from ISP.** Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
- **Use Static IP Address.** Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP's router to which your router will connect.

Domain Name Server (DNS) Address. The DNS server is used to look up site addresses based on their names.

- **Get Automatically from ISP.** Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
- **Use These DNS Servers.** If you know that your ISP does not automatically transmit DNS addresses to the router during login, select this option, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

Router MAC Address. The Ethernet MAC address used by the router on the Internet port. Some ISPs register the MAC address of the network interface card in your computer when your account is first opened. They will then accept traffic only from the MAC address of that computer. This feature allows your router to use your computer's MAC address (this is also called cloning).

- **Use Default Address.** Use the default MAC address.
- **Use Computer MAC Address.** The router will capture and use the MAC address of the computer that you are now using. You have to use the one computer that is allowed by the ISP.
- **Use This MAC Address.** Enter the MAC address that you want to use.

Wireless Settings

The Wireless Settings screen lets you view or configure the wireless network setup.

The Mobile LTE Broadband 11n Wireless Router comes with preset security. This means that the WiFi network name (SSID), network key (password), and security option (encryption protocol) are preset in the factory. You can find the preset SSID and password on the bottom of the unit.

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

➤ **To view or change basic wireless settings:**

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

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

1. On the BASIC Home screen, select **Wireless** to display the Wireless Settings screen.

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

2. Make any changes that are needed, and click **Apply** to save your settings.
3. Set up and test your wireless devices and computers to make sure that they can connect wirelessly. If they do not, check the following:

- Is your wireless device or computer connected to your network or another wireless network in your area? Some wireless devices automatically connect to the first open network (without wireless security) that they discover.
- Does your wireless device or computer appear on the Attached Devices screen? If it does, then it is connected to the network.
- If you are not sure what the network name (SSID) or password is, look on the label on the bottom of your router.

Wireless Settings Screen Fields

Wireless Network

The b/g/n and a/n notation references the 802.11 standards of conformance. For instance, the 2.4 b/g/n conforms to 802.11b, 802.11g, and 802.11n at 2.4 GHz radio frequency.

Enable SSID Broadcast. This setting allows the router to broadcast its SSID so wireless stations can see this wireless name (SSID) in their scanned network lists. This check box is selected by default. To turn off the SSID broadcast, clear the **Enable SSID Broadcast** check box, and click **Apply**.

Name (SSID). The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. The default SSID is randomly generated, and **NETGEAR strongly recommends that you do not change this.**

Region Selection. The location where the router is used. Select from the countries in the list. Note that in the United States, the region is fixed to United States and is not changeable.

Channel. This setting is the wireless channel used by the gateway. Enter a value from 1 through 13. (For products in the North America market, only Channels 1 through 11 can be operated.) Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which is the best.

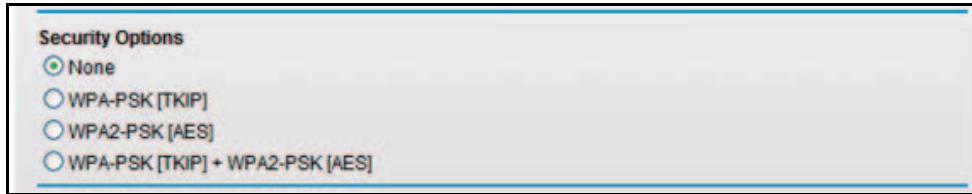
Mode. Up to 217 Mbps is the default and allows 802.11n and 802.11g wireless devices to join the network. g & b supports up to 54 Mbps. The 450 Mbps setting allows 802.11n devices to connect at this speed.

Security Options

The Security Options section of the Wireless Settings screen lets you change the security option and passphrase. Please note that **NETGEAR recommends that you do not change the security option or passphrase**, but if you want to change these settings, the following section explains how. **Do not disable security.**

Change WPA Security Option and Passphrase

1. Under Security Options, select the WPA option you want.



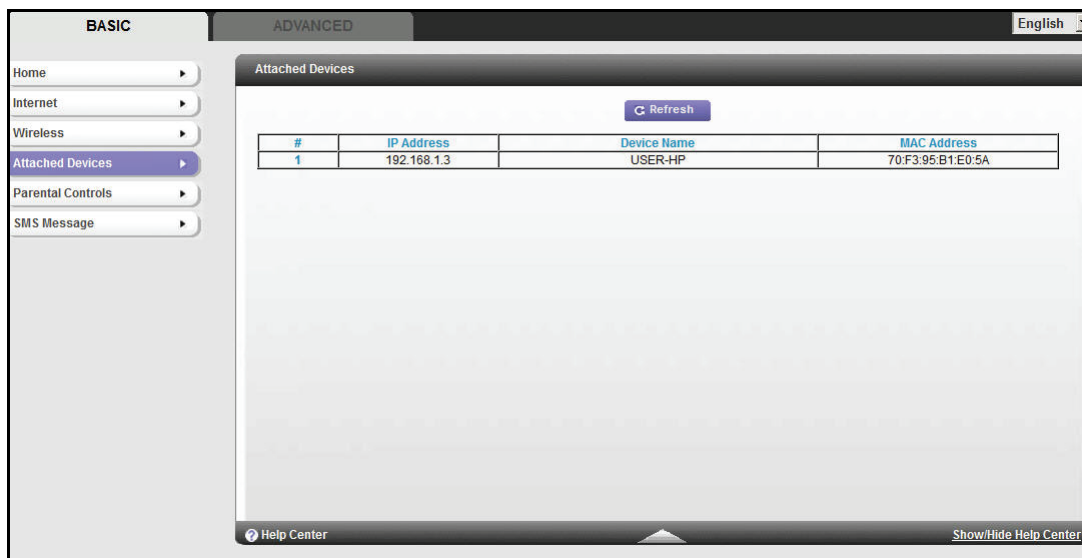
Security Options

- ☒ None
- ☐ WPA-PSK [TKIP]
- ☐ WPA2-PSK [AES]
- ☐ WPA-PSK [TKIP] + WPA2-PSK [AES]

2. In the Passphrase field that displays when you select a WPA security option, enter the network key (passphrase) that you want to use. It is a text string from 8 to 63 characters.

Attached Devices

You can view all computers or devices that are currently connected to your network here. From the BASIC Home screen, select **Attached Devices** to display the following screen:



#	IP Address	Device Name	MAC Address
1	192.168.1.3	USER-HP	70:F3:95:B1:E0:5A

Wired devices are connected to the router with Ethernet cables. Wireless devices have joined the wireless network.

- **#** (number). The order in which the device joined the network.
- **IP Address**. The IP address that the router assigned to this device when it joined the network. Note that this number can change if a device is disconnected and rejoins the network.
- **Device Name**. If the device name is known, it is shown here.
- **MAC Address**. The unique MAC address for each device does not change. The MAC address is typically shown on the product label.

You can click **Refresh** to update this screen.

Parental Controls

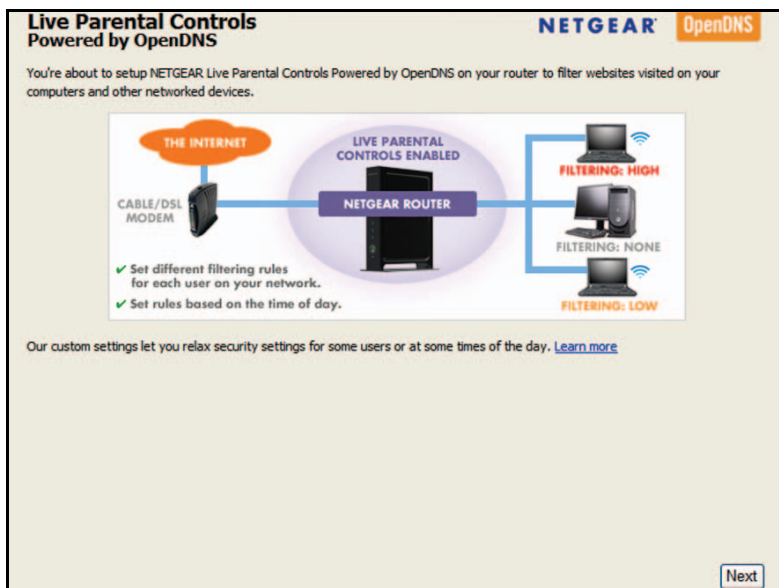
The first time you select Parental Controls from the BASIC Home screen, you are automatically directed to the Internet, where you can learn more about Live Parental Controls or download the application. The following screen displays:

The screenshot shows the 'Parental Controls Center' page. At the top, it says 'NETGEAR' and 'Support | Sign in'. Below the title, there's a message: 'Use OpenDNS Parental Controls with your router to make the Internet safer for your household.' There's an illustration of a router and two desktop computers. The main section is 'Sign in to your OpenDNS account', which includes fields for 'Username' and 'Password', a 'Sign in' button, and a link for 'Forgot your password?'. To the right, an 'Important Note' box states: 'If you have not yet configured the Live Parental Controls feature on your device please do so with the Management Utility found on the CD that came with your router or download it now for [Windows](#) or [Mac](#).' The footer shows the 'OpenDNS' logo and '© 2012 OpenDNS'.

➤ To set up Live Parental Controls:

1. Select **Parental Controls** on the dashboard screen.
2. Click either the **Windows Users** or **Mac Users** button.
3. Follow the onscreen instructions to download and install the NETGEAR Live Parental Controls Management utility.

After installation, Live Parental Controls automatically starts.



4. Click **Next**, read the note, and click **Next** again to proceed.

Because Live Parental Controls uses free OpenDNS accounts, you are prompted to log in or create a free account.

Setting up Live Parental Controls

Welcome, this setup wizard will quickly configure NETGEAR Live Parental Controls Powered by OpenDNS on your NETGEAR router.

In order to use Live Parental Controls, you need a free OpenDNS account. Do you already have one?

☒ Yes, use my existing OpenDNS account.

☐ No, I need to create a free OpenDNS account.

5. Select the radio button that applies to you and click **Next**.
 - If you already have an OpenDNS account, leave the **Yes** radio button selected.
 - If you do not have an OpenDNS account, select the **No** radio button.

If you are creating an account, the following screen displays:

Create a free OpenDNS account

Username

Password

Confirm Password

Email

Confirm Email

- Fill in the fields and click **Next**.

After you log on or create your account, the filtering level screen displays:

Live Parental Controls: choose a filtering level for your network

All computers connected to your router will be protected from the content you select below. You can customize your Live Parental Controls later on our website.

☐ **High**
Protects against all adult-related sites, illegal activity, social networking sites, video sharing sites, phishing attacks and general time-wasters.

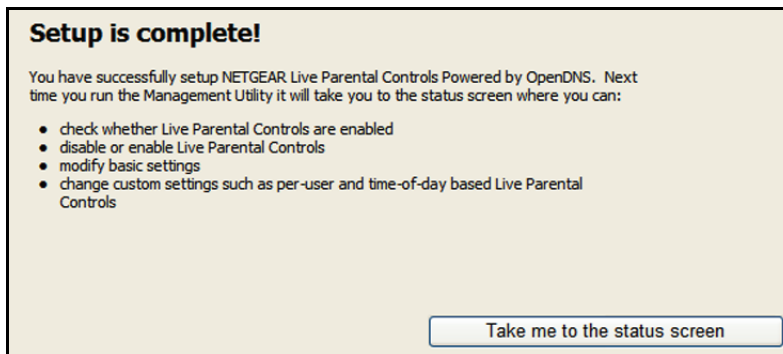
☐ **Moderate**
Protects against all adult-related sites, illegal activity and phishing attacks.

☐ **Low**
Protects against pornography and phishing attacks.

☒ **Minimal**
Protects only against phishing attacks.

☐ **None**
Nothing blocked.

6. Select the radio button for the filtering level that you want and click **Next**.



7. Click the **Take me to the status screen** button.

Parental controls are now set up for the router. The dashboard shows Parental Controls as Enabled.

SMS Message

Short Message Service (SMS) is a text messaging service for communication systems. The SMS screens enable you to perform the tasks that are explained in the following sections:

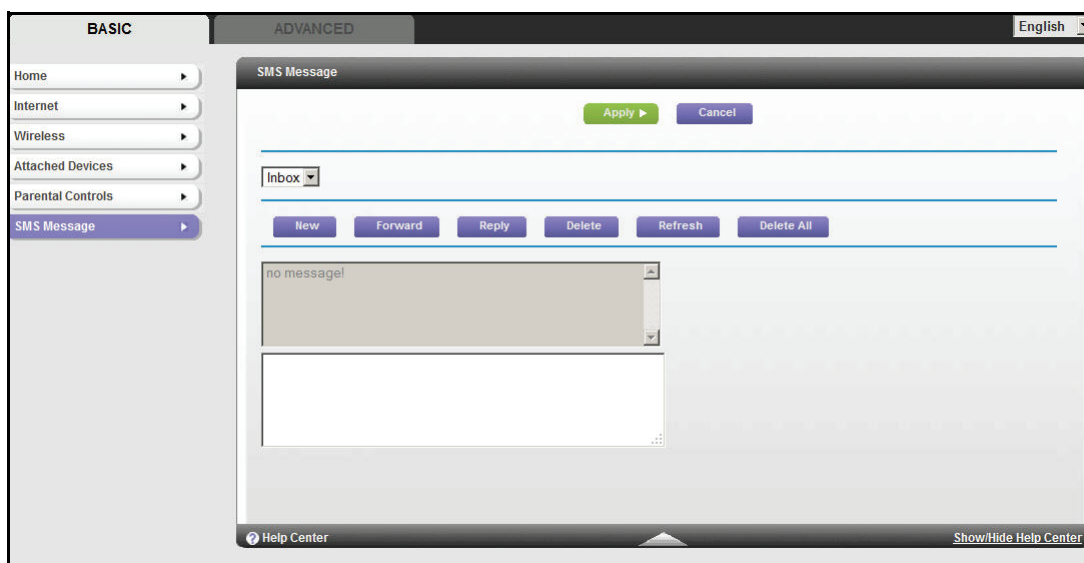
- [View SMS Messages](#)
- [Send SMS Messages](#)

View SMS Messages

New SMS messages are available when the SMS LED on the front panel is solid green.

➤ **To view new SMS messages:**

1. Select **BASIC > SMS Message** to display the following screen:



2. Click a particular message to view it.
 - Click **Forward** or **Reply** to forward or reply to the specified message.
 - Click **Delete** to delete the specified SMS message.
3. Otherwise, do one of the following:
 - Click **Refresh** to redisplay all SMS messages from the SIM card.
 - Click **Delete All** to delete all SMS messages from the SIM card.
 - Click **New** to open a new message. See [Send SMS Messages](#) on page 31 for more information.

Send SMS Messages

You can create a new SMS message or send an SMS message over email.

➤ **To send SMS messages:**

1. Select **BASIC > SMS Message** and then click **New** to display the following screen:

2. In the To field, enter the phone number that you want to send your SMS message to, or the email address to send a SMS message over email.

For multitarget messages, you can send a message to multiple phone numbers. Each phone number has to be separated by a comma (,).

3. In the Content field, enter the content of the SMS message. The length of the message is shown at the bottom of the content box.
4. Click **Send** to send the SMS message.

Alternatively, you can also take one of the following actions:

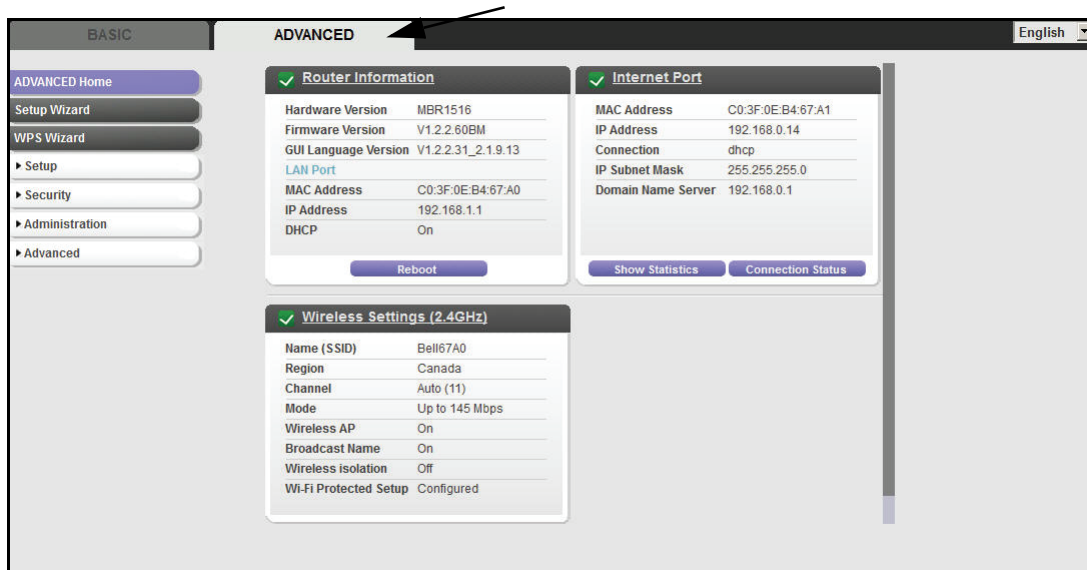
- Click **Clear** to remove the information in the To and Content fields.
- Click **Save** to save a draft of the message.
- Click **Cancel** to return to the Inbox without sending the message.

NETGEAR genie ADVANCED Home

4

Specifying custom settings

This chapter explains the features available from the NETGEAR genie ADVANCED Home screen, shown in the following figure:



This chapter contains the following sections:

- [Setup Wizard](#)
- [WPS Wizard](#)
- [Setup Menu](#)
- [Broadband Settings](#)
- [Mobile Broadband Settings](#)
- [WAN Setup](#)
- [LAN Setup](#)
- [Quality of Service Setup](#)

Some selections on the ADVANCED Home screen are described in separate chapters:

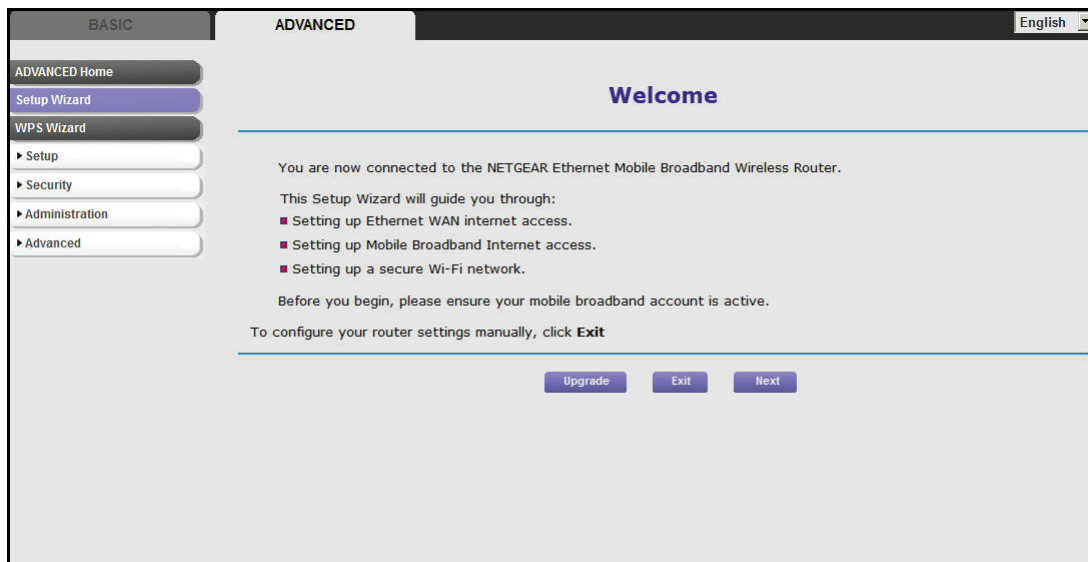
- **Security.** See [Chapter 5, Security](#).
- **Administration.** See [Chapter 6, Administration](#).
- **Advanced Setup.** See [Chapter 7, Advanced Settings](#).

Setup Wizard

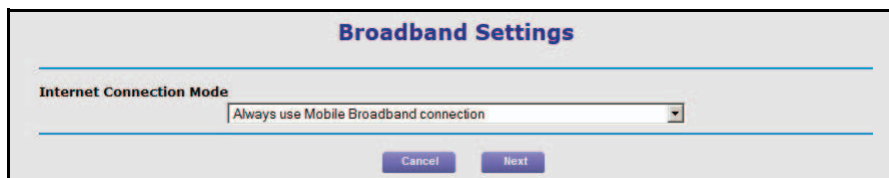
The NETGEAR genie installation process is launched the first time you set up the router. After setting up the router the first time, if you want to perform this task again, you can run Setup Wizard from the ADVANCED tab of the NETGEAR genie.

➤ **To run the Setup Wizard:**

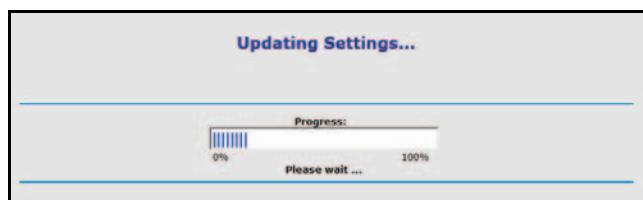
1. Select **ADVANCED > Setup Wizard** to display the following screen:



2. Click **Upgrade** to update the firmware (see [Router Upgrade](#) on page 64). Otherwise, click **Next** to continue.
3. Select your broadband settings (see [Broadband Settings](#) on page 36) and click **Next**.



The router provides you with a update progress indication.



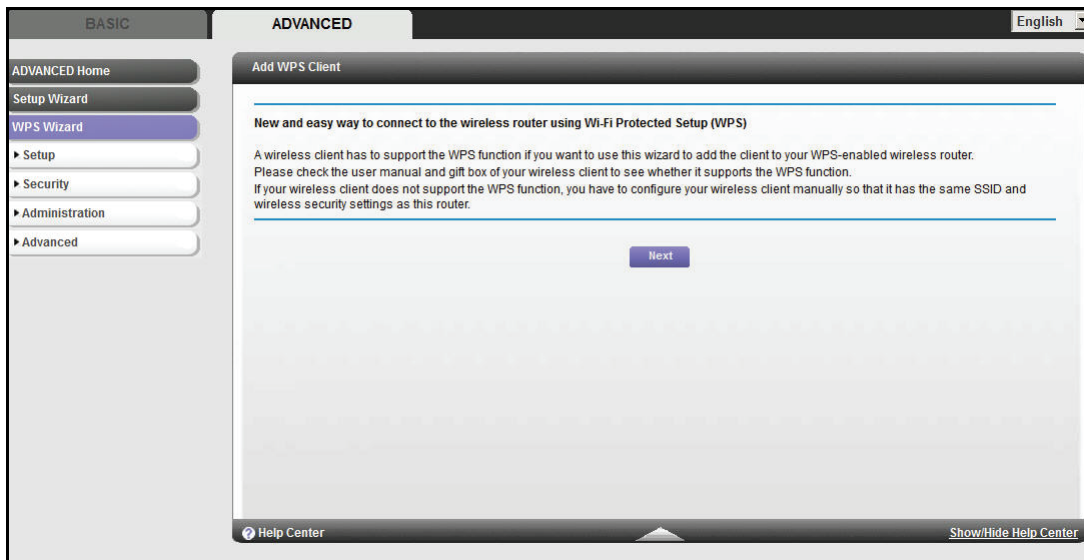
Note: When you run the Setup Wizard from a WiFi connection, you are logged out when the router reboots.

WPS Wizard

The WPS Wizard helps you add a WPS-capable client device (a wireless device or computer) to your network. On the client device you need to either press its WPS button or locate its WPS PIN.

➤ **To use the WPS Wizard:**

1. Select **ADVANCED > WPS Wizard**.
2. Click **Next**. The following screen lets you select the method for adding the WPS client (a wireless device or computer).



You can use either the push button or PIN method.

3. Select either **Push Button** or **PIN Number**.

- To use the push button method, either click the **WPS** button on this screen, or press the **WPS** button located on the side of the router. Within 2 minutes, go to the wireless client and press its **WPS** button to join the network without entering a password.

- To use the PIN method, select the **PIN Number** radio button, enter the client security PIN, and click **Next**.

Within 2 minutes, go to the client device and use its WPS software to join the network without entering a password.

The router attempts to add the WPS-capable device. The WPS LED on the front of the router blinks green. When the router establishes a WPS connection, the LED is solid green, and the router WPS screen displays a confirmation message.

4. Repeat Step 2 and Step 3 to add another WPS client to your network.

Setup Menu

Select **ADVANCED > Setup** to display the Setup menu. The following selections are available:

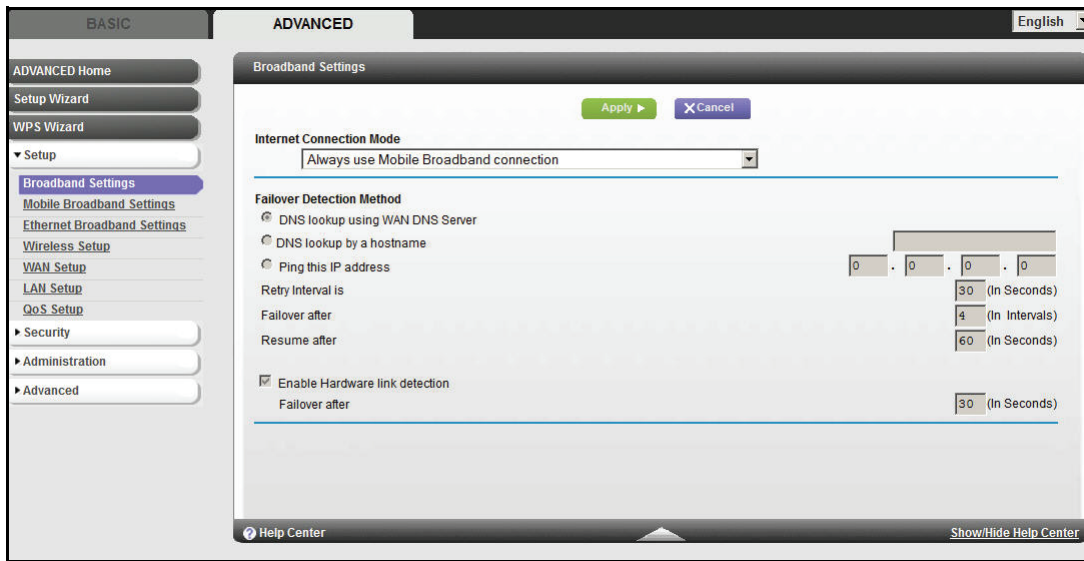
- **Broadband Settings.** Configure the Internet connection mode of your Mobile LTE Broadband 11n Wireless Router MBR1516. See [Broadband Settings](#) on page 36.
- **Mobile Broadband Settings.** Configure the access to your mobile broadband account. See [Mobile Broadband Settings](#) on page 36.
- **Ethernet Broadband Settings.** This is a shortcut to the same Internet Setup screen that you can access from the dashboard on the BASIC Home screen. See [Internet Setup](#) on page 22.
- **Wireless Setup.** This is a shortcut to the same Wireless Settings screen that you can access from the dashboard on the BASIC Home screen. See [Wireless Settings](#) on page 24.
- **WAN Setup.** Internet (WAN) setup. See [WAN Setup](#) on page 38.
- **LAN Setup.** Local area network (LAN) setup. See [LAN Setup](#) on page 41.
- **QoS Setup.** Quality of Service (QoS) setup. See [Quality of Service Setup](#) on page 44.

Broadband Settings

The Broadband Settings screen lets you select the Internet connection mode of your Mobile LTE Broadband 11n Wireless Router MBR1516.

➤ **To select your Internet connection mode:**

1. Select **ADVANCED > Setup > Broadband Settings** to view the following screen:



Your Internet connection choices include the following:

- Use Ethernet connection first and if fail use mobile broadband connection
- Always use Mobile Broadband connection
- Always use Ethernet connection

2. Click **Apply** to save your selection.

Mobile Broadband Settings

The Mobile Broadband Settings screen lets you configure the access to your mobile broadband account.

Note: Connecting to the mobile broadband network requires an active broadband service account.

➤ To configure your mobile broadband account access:

1. Select **ADVANCED > Setup > Mobile Broadband Settings** to view the following screen:

The screenshot displays the 'Mobile Broadband Settings' page. On the left is a navigation menu with options like 'ADVANCED Home', 'Setup Wizard', 'WPS Wizard', 'Setup', 'Broadband Settings', 'Mobile Broadband Settings' (highlighted), 'Ethernet Broadband Settings', 'Wireless Setup', 'WAN Setup', 'LAN Setup', 'GoS Setup', 'Security', 'Administration', and 'Advanced'. The main content area has a 'Broadband Settings' header with 'Connect', 'Disconnect', 'Apply', 'Cancel', and 'Refresh' buttons. Below are input fields for 'User Name', 'Password', 'Country' (set to Canada), 'Internet Service Provider' (set to Bell Mobility), 'Access Number' (set to *99), 'APN' (set to inet.bell.ca), and 'PDP Type' (set to IP). There are checkboxes for 'Use internal antenna' (checked) and 'Wireless Button Configuration' (set to Control WiFi Only). At the bottom, the 'Connection Status' is shown as 'Connected'.

The following settings are provided:

- **User Name.** The account login user name.
 - **Password.** The account password for authentication.
 - **Country.** The country where mobile broadband service is provided.
 - **Internet Service Provider.** The Internet service provider of the 4G network.
 - **PIN code.** The PIN code of the SIM card if the PIN has been enabled.
 - **Access Number.** The phone number of the remote site.
 - **APN.** The access point name.
 - **PDP Type.** The type of packet data protocol.
 - **Use internal antenna.** The Mobile LTE Broadband 11n Wireless Router MBR1516 uses internal antennas unless you choose to boost reception with external antennas.
 - **Wireless Button Configuration.** Choose whether you want the WPS button to control WiFi only or both WiFi and wireless broadband.
 - **Connection Status.** The status of the current WAN port.
2. Click **Apply** to save your settings.
 3. Click **Connect** when you want to connect manually to the network.
 4. Click **Disconnect** when you want to disconnect manually from the current network.

WAN Setup

The WAN Setup screen lets you configure a DMZ (demilitarized zone) server, change the maximum transmit unit (MTU) size, and enable the router to respond to a ping on the WAN (Internet) port. Select **ADVANCED > Setup > WAN Setup** to view the following screen:

- **Disable Port Scan and DoS Protection.** DoS protection protects your LAN against denial of service attacks such as Syn flood, Smurf Attack, Ping of Death, Teardrop Attack, UDP Flood, ARP Attack, Spoofing ICMP, Null Scan, and many others. This should be disabled only in special circumstances.
- **Default DMZ Server.** This feature is sometimes helpful when you are playing online games or videoconferencing. Be careful when using this feature because it makes the firewall security less effective. See [Default DMZ Server](#) on page 39 for more details.
- **Respond to Ping on Internet Port.** If you want the router to respond to a ping from the Internet, select this check box. Use this only as a diagnostic tool because it allows your router to be discovered. Do not select this check box unless you have a specific reason.
- **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. See [Change the MTU Size](#) on page 39.
- **NAT Filtering.** Network Address Translation (NAT) determines how the router processes inbound traffic. Secured NAT provides a secured firewall to protect the computers on the LAN from attacks from the Internet but might prevent some Internet games, point-to-point applications, or multimedia applications from functioning. Open NAT provides a much less secured firewall but allows almost all Internet applications to function.
- **Disable SIP ALG.** Some VoIP applications do not work well with the SIP ALG. Selecting this check box to turn off the SIP ALG helps your VoIP devices create and accept calls through the router.

Default DMZ Server

The default DMZ server feature is helpful when you are using some online games and videoconferencing applications that are incompatible with Network Address Translation (NAT). The router is programmed to recognize some of these applications and to work correctly with them, but there are other applications that might not function well. In some cases, one local computer can run the application correctly if that computer's IP address is entered as the default DMZ server.



WARNING:

DMZ servers pose a security risk. A computer designated as the default DMZ server loses firewall protection from exploits on the Internet. Once compromised, the DMZ server computer attacks other computers on your network.

Incoming traffic from the Internet is usually 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 Port Forwarding/Port Triggering screen. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the default DMZ server.

➤ **To set up a default DMZ server:**

1. On the WAN Setup screen, select the **Default DMZ Server** check box.
2. Type the IP address.
3. Click **Apply**.

Change the MTU Size

The maximum transmission unit (MTU) is the largest data packet a network device transmits. When one network device communicates across the Internet with another, the data packets travel through many devices along the way. If any device in the data path has a lower MTU setting than the other devices, the data packets have to be split or "fragmented" to accommodate the device with the smallest MTU.

The best MTU setting for NETGEAR equipment is often just the default value, and changing the value might fix one problem but cause another. Leave MTU unchanged unless one of these situations occurs:

- You have problems connecting to your ISP or other Internet service, and the technical support of either the ISP or NETGEAR recommends changing the MTU setting. These web-based applications might require an MTU change:
 - A secure website that will not open, or displays only part of a web page
 - Yahoo email
 - MSN portal
 - America Online's DSL service

- You use VPN and have severe performance problems.
- You used a program to optimize MTU for performance reasons, and now you have connectivity or performance problems.

Note: An incorrect MTU setting causes Internet communication problems such as the inability to access certain websites, frames within websites, secure login pages, and FTP or POP servers.

If you suspect an MTU problem, a common solution is to change the MTU to 1400. If you are willing to experiment, you can gradually reduce the MTU from the maximum value of 1500 until the problem goes away. The following table describes common MTU sizes and applications.

Table 2. Common MTU sizes

MTU	Application
1500	The largest Ethernet packet size and the default value. This is the typical setting for non-PPPoE, non-VPN connections and is the default value for NETGEAR routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for ping. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1460	Usable by AOL if you do not have large email attachments, for example.
1436	Used in PPTP environments or with VPN.
1400	Maximum size for AOL DSL.
576	Typical value to connect to dial-up ISPs.

➤ **To change the MTU size:**

1. Select **ADVANCED > Setup > WAN Setup**.
2. In the MTU Size field, enter a new size between 64 and 1500.
3. Click **Apply** to save the settings.

LAN Setup

The LAN Setup screen allows configuration of LAN IP services such as Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP).

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

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

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

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

➤ **To change the LAN settings:**

1. Select **ADVANCED > Setup > LAN Setup** to display the following screen:

The screenshot shows the 'LAN Setup' configuration page in the NETGEAR genie interface. The left sidebar lists various setup categories, with 'LAN Setup' currently selected. The main configuration area includes:

- Device Name:** A text field containing 'MBR1516'.
- LAN TCP/IP Setup:**
 - IP Address:** A four-part numeric field set to 192, 168, 1, 1.
 - IP Subnet Mask:** A four-part numeric field set to 255, 255, 255, 0.
 - RIP Direction:** A dropdown menu set to 'Both'.
 - RIP Version:** A dropdown menu set to 'Disabled'.
- DHCP Server:**
 - Use Router as DHCP Server:** A checked checkbox.
 - Starting IP Address:** A four-part numeric field set to 192, 168, 1, 2.
 - Ending IP Address:** A four-part numeric field set to 192, 168, 1, 254.
- Address Reservation:** A table with columns for '#', 'IP Address', 'Device Name', and 'MAC Address'. Below the table are buttons for '+Add', 'Edit', and 'Delete'.

At the top right of the main area are 'Apply' and 'Cancel' buttons. The bottom of the screen features a 'Help Center' link and a 'Show/Hide Help Center' button.

2. Enter the settings that you want to customize. These settings are described in [LAN Setup Screen Settings](#) on page 42.
3. Click **Apply** to save your changes.

LAN Setup Screen Settings

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 have to be reached through a gateway or router.
- **RIP Direction.** Router Information Protocol (RIP) 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 setting. With the Both or Out Only setting, the router broadcasts its routing table periodically. With the Both or In Only setting, the router incorporates the RIP information that it receives.
- **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, the RIP function is disabled.

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.

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.

- **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

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

Use the Router as a DHCP Server

By default, the router functions as a 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. The router assigns IP addresses to the attached computers from a pool of addresses specified in this screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN. For most applications, the default DHCP and TCP/IP settings of the router are satisfactory.

You can specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the router's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.1.2 and 192.168.1.254, 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 (the router's LAN IP address)
- Primary DNS server (if you entered a primary DNS address in the Internet Setup screen; otherwise, the router's LAN IP address)
- Secondary DNS server (if you entered a secondary DNS address in the Internet Setup screen)

To use another device on your network as the DHCP server, or to manually configure the network settings of all of your computers, clear the **Use Router as DHCP Server** check box and click **Apply**. Otherwise, leave this check box selected. If this service is not enabled and no other DHCP server is available on your network, you need to set your computers' IP addresses manually or they will not be able to access the router.

Address Reservation

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

➤ To reserve an IP address:

1. In the Address Reservation section of the screen, click the **Add** button to display the following screen:

The screenshot shows the 'Address Reservation' window. At the top are buttons for '+ Add', 'X Cancel', and 'G Refresh'. Below is the 'Address Reservation Table' with the following data:

	#	IP Address	Device Name	MAC Address
	1	192.168.1.3	USER-HP	70:13:95:b1:e0:5a

Below the table are input fields for:

- IP Address: 192 . 168 . 1 . []
- MAC Address: []
- Device Name: []

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 192.168.1.x.)
3. Type the MAC address of the computer or server.

Tip: If the computer is already on your network, you can copy its MAC address from the Attached Devices screen and paste it here.

4. Click **Apply** to enter the reserved address into the table.

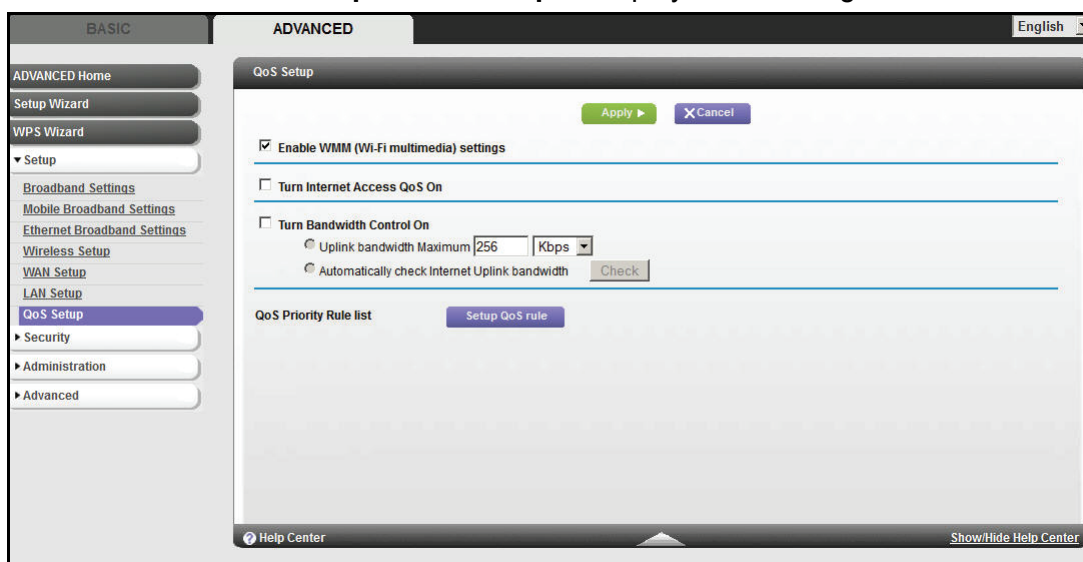
The reserved address is not assigned until the next time the computer contacts the router's DHCP server. Reboot the computer, or access its IP configuration and force a DHCP release and renew.

To edit or delete a reserved address entry, select the radio button next to the reserved address you want to edit or delete. Then click **Edit** or **Delete**.

Quality of Service Setup

Quality of Service (QoS) is an advanced feature that can be used to prioritize some types of traffic ahead of others. The Mobile LTE Broadband 11n Wireless Router can provide QoS prioritization over the wireless link and on the Internet connection. To configure QoS, use the QoS Setup screen.

Select **ADVANCED > Setup > QoS Setup** to display the following screen:



Enable WMM QoS for Wireless Multimedia Applications

WMM (Wireless Multimedia) is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities depending on the type of data. Time-dependent information, such as video and audio, has a higher priority than normal traffic. For WMM to function correctly, wireless clients have to support WMM also.

WMM QoS is enabled by default. You can disable it in the QoS Setup screen by clearing the **Enable WMM (Wi-Fi multimedia) settings** check box and clicking **Apply**.

Turn Internet Access QoS On

Enable this feature for the QoS function to prioritize Internet traffic.

Manage the QoS Priority Rules

Select **ADVANCED > Setup > QoS Setup** and click the **Setup QoS rule button** to display the following screen:

The top screenshot shows the QoS Priority Rule list with the following data:

#	QoS Policy	Priority	Description
1	MSN Messenger	High	MSN Messenger Applications
2	Yahoo Messenger	High	Yahoo Messenger Applications
3	IP Phone	Highest	IP Phone Applications
4	Vonage IP Phone	Highest	Vonage IP Phone Applications
5	NetMeeting	High	NetMeeting Applications
6	AIM	High	AIM Applications
7	Google Talk	Highest	Google Talk Applications
8	Netgear EVA	Highest	Netgear EVA Applications
9	SSH	High	SSH Applications
10	Telnet	High	Telnet Applications
11	VPN	High	VPN Applications
12	FTP	Normal	FTP Applications
13	SMTP	Normal	SMTP Applications
14	WWW	Normal	WWW Applications

The bottom screenshot shows the QoS Priority Rule list with the following data:

#	QoS Policy	Priority	Description
17	eMule / eDonkey	Low	eMule / eDonkey Applications
18	Kazaa	Low	Kazaa Applications
19	Gnutella	Low	Gnutella Applications
20	BT / Azureus	Low	BT / Azureus Applications
21	Counter Strike	High	Online Gaming Counter Strike
22	Ages of Empires	High	Online Gaming Age of Empires
23	Everquest	High	Online Gaming Everquest
24	Quake 2	High	Online Gaming Quake 2
25	Quake 3	High	Online Gaming Quake 3
26	Unreal Tournament	High	Online Gaming Unreal Tournament
27	Warcraft	High	Online Gaming Warcraft

Both screenshots include an 'Apply' button, a 'Cancel' button, and a 'Help Center' link. The bottom screenshot also includes an 'Add Priority Rule' button.

For applications such as online gaming, an Ethernet LAN port, or a specified MAC address that already appears in the list, modify the priority level by selecting it and then clicking **Edit**. Click **Delete** to erase the priority rule.

You can also define the priority policy for each online game, application, LAN port, or the computer's MAC address by clicking **Add Priority Rule**.

For Applications or Online Gaming

- To set up the priority for an application or online gaming:

1. From the Priority Category list, select **Applications** or **Online Gaming**.

2. Select the Internet application or game from one of the lists.

3. Select the priority level: Highest, High, Normal, or Low.
4. In the QoS Policy for field, type the name for this rule.
5. Click **Apply**.

For an Ethernet LAN Port

- **To set up the priority for computers connected to a LAN port:**

1. From the Priority Category list, select **Ethernet LAN Port**.

The screenshot shows the 'QoS - Priority Rules' window. At the top are 'Apply' and 'Cancel' buttons. The 'Priority' section contains the following fields:

- QoS Policy for:** A text box containing 'LAN Port 1'.
- Priority Category:** A dropdown menu set to 'Ethernet LAN Port'.
- LAN Port:** A dropdown menu set to '1'.
- Priority:** A dropdown menu set to 'Normal'.

At the bottom, there is a 'Help Center' icon and a 'Show/Hide Help Center' link.

2. Select the number of the LAN port for which you want to specify the priority level.
3. Select the priority level: Highest, High, Normal, or Low.
4. You can also type the name for this rule in the QoS Policy for field.
5. Click **Apply**.

For a MAC Address

- **To set up the priority for a specified computer through its MAC address:**

1. From the Priority Category list, select **MAC Address**.

The screenshot shows the 'QoS - Priority Rules' window for MAC Address configuration. At the top are 'Apply' and 'Cancel' buttons. The 'Priority' section contains the following fields:

- QoS Policy for:** A text box.
- Priority Category:** A dropdown menu set to 'MAC Address'.

Below this is a 'MAC Device List' table:

	QoS Policy	Priority	Device Name	MAC Address
C	Pri_MAC_B1E05A	Normal	USER-HP	70:F3:95:B1:E0:5A

Below the table are fields for:

- MAC Address:** A series of six boxes for entering the address.
- Device Name:** A text box.
- Priority:** A dropdown menu set to 'Normal'.

At the bottom are buttons for 'Add', 'Edit', 'Delete', and 'Refresh'. The 'Help Center' and 'Show/Hide Help Center' links are at the very bottom.

2. Click **Refresh** to update the list of those computers already connected to the router.
3. Select the entry's radio button in the table.
4. Modify the information in the MAC Address and Device Name fields.
5. Select the priority level: Highest, High, Normal, or Low.
6. You can also type the name for this rule in the QoS Policy for field.
7. Click **Edit** or **Add**.
8. Click **Apply**.

Edit or Delete an Existing QoS Policy

➤ **To edit or delete a QoS policy:**

1. Select **ADVANCED > QoS Setup** to display the QoS Setup screen.
2. Select the radio button next to the QoS policy to be edited or deleted, and do one of the following:
 - Click **Delete** to remove the QoS policy.
 - Click **Edit** to edit the QoS policy. Follow the instructions in the preceding sections to change the policy settings.
3. Click **Apply** in the QoS Setup screen to save your changes.

Security

5

Keeping unwanted content out of your network

This chapter explains how to use the basic firewall features of the router to prevent objectionable content from reaching the computers and other devices connected to your network.

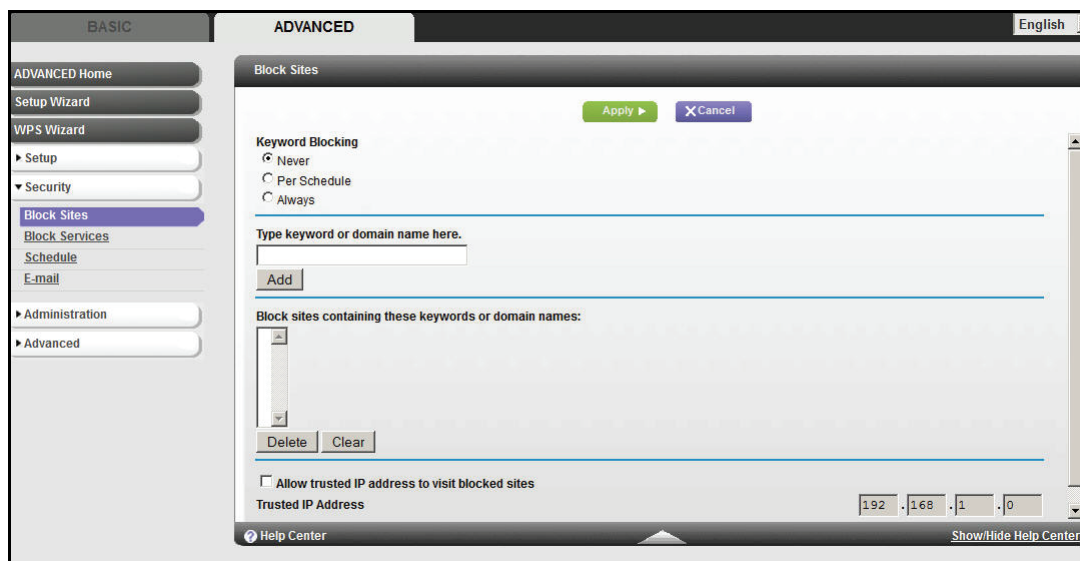
This chapter includes the following sections:

- *Keyword Blocking of HTTP Traffic*
- *Block Services (Port Filtering)*
- *Schedule Blocking*
- *Security Event Email Notifications*

Keyword Blocking of HTTP Traffic

Use keyword blocking to prevent certain types of HTTP traffic from accessing your network. The blocking can be always or according to a schedule.

1. Select **ADVANCED > Security > Block Sites** to display the following screen:



2. Select one of the keyword blocking options:
 - **Per Schedule.** Turn on keyword blocking according to the Schedule screen settings.
 - **Always.** Turn on keyword blocking all the time, independent of the Schedule screen.
3. In the keyword field, enter a keyword or domain, click **Add Keyword**, and click **Apply**.
The keyword list supports up to 32 entries. Here are some sample entries:
 - Specify XXX to block http://www.badstuff.com/xxx.html.
 - Specify .com if you want to allow only sites with domain suffixes such as .edu or .gov.
 - Enter a period (.) to block all Internet browsing access.

➤ **To delete a keyword or domain:**

1. Select the keyword you want to delete from the list.
2. Click **Delete**, and then **Apply** to save your changes.

➤ **To specify a trusted computer:**

You can exempt one trusted computer from blocking and logging. The computer you exempt has to have a fixed IP address.

1. In the Trusted IP Address field, enter the IP address.
2. Click **Apply** to save your changes.

Block Services (Port Filtering)

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 the 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 at <http://www.ietf.org/>) and published in RFC1700, "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. You can often determine port number information by contacting the publisher of the application, by asking user groups or newsgroups, or by searching.

The Block Services screen lets you add and block specific Internet services by computers on your network. This is called service blocking or port filtering. To add a service for blocking, first determine which port number or range of numbers are used by the application.

➤ **To block services:**

1. Select **ADVANCED > Security > Block Services** to display the following screen:

The screenshot shows the 'Block Services' configuration page. On the left is a sidebar with navigation links: ADVANCED Home, Setup Wizard, WPS Wizard, Setup, Security (expanded), Block Sites, Block Services (selected), Schedule, E-mail, Administration, and Advanced. The main content area is titled 'Block Services' and includes an 'Apply' button and a 'Cancel' button. Below these are three radio buttons for 'Services Blocking': 'Never' (selected), 'Per Schedule', and 'Always'. A table with columns '#', 'Service Type', 'Port', and 'IP' is present, with 'Add', 'Edit', and 'Delete' buttons below it. At the bottom, there are links for 'Help Center' and 'Show/Hide Help Center'.

2. Select either **Per Schedule** or **Always** to enable service blocking, and click **Apply**. If you selected **Per Schedule**, specify a time period in the [Schedule](#) screen as described in [Schedule Blocking](#) on page 53.

3. Click **Add** to add a service. The Block Services Setup screen displays:

Block Services Setup

Apply Cancel

Service Type: User Defined

Protocol: TCP

Starting Port: (1~65534)

Ending Port: (1~65534)

Service Type/User Defined:

Filter Services For :

☐ Only This IP Address:

☐ IP Address Range:

☒ All IP Addresses

192 . 168 . 1 . 1

to 192 . 168 . 1 . 1

Help Center Show/Hide Help Center

4. From the Service Type list, select the application or service to allow or block. The list already displays several common services, but you are not limited to these choices. To add any additional services or applications that do not already appear, select **User Defined**.
5. If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select **Both**.
6. Enter the starting and ending port numbers. If the application uses a single port number, enter that number in both fields.
7. Select the radio button for the IP address configuration you want to block, and enter the IP addresses. You can block the specified service for a single computer, a range of computers with consecutive IP addresses, or all computers on your network.
8. Click **Add** to enable your Block Services Setup selections.

Schedule Blocking

You can specify the days and time that you want to block Internet access.

➤ **To schedule blocking:**

1. Select **ADVANCED > Security > Schedule** to display the following screen:

The screenshot shows the 'Schedule' configuration page under the 'ADVANCED' tab. The left sidebar contains a navigation menu with options: ADVANCED Home, Setup Wizard, WPS Wizard, Setup, Security (expanded), Block Sites, Block Services, Schedule (selected), E-mail, Administration, and Advanced. The main content area is titled 'Schedule' and includes an 'Apply' button and a 'Cancel' button. The configuration options are as follows:

- Days to Block:** A list of days with checkboxes: ☒ Every Day, ☒ Sunday, ☒ Monday, ☒ Tuesday, ☒ Wednesday, ☒ Thursday, ☒ Friday, and ☒ Saturday.
- Time of day to block:(use 24-hour clock)**
 - ☒ All Day
 - Start Blocking: 0 Hour 0 Minute
 - End Blocking: 24 Hour 0 Minute
- Time Zone:** A dropdown menu showing '(GMT-05:00) Bogota, Lima, Quito, Eastern Time (US & Canada)'.
- ☒ Automatically adjust for daylight savings time

At the bottom of the page, there is a 'Help Center' link and a 'Show/Hide Help Center' button.

2. Set up the schedule for blocking keywords and services.
 - **Days to Block.** Select days on which you want to apply blocking by selecting the appropriate check boxes, or select **Every Day** to select the check boxes for all days.
 - **Time of day to block.** Select a start and end time in 24-hour format, or select **All Day** for 24-hour blocking.
3. Select your time zone from the list. If you use daylight saving time, select the **Automatically adjust for daylight savings time** check box.
4. Click **Apply** to save your settings.

Security Event Email Notifications

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

➤ **To set up email notifications:**

1. Select **ADVANCED > Security > E-mail** to display the following screen:

The screenshot shows the 'E-mail' configuration screen within the 'ADVANCED' tab. The left sidebar contains a navigation menu with options: ADVANCED Home, Setup Wizard, WPS Wizard, Setup, Security (expanded), Block Sites, Block Services, Schedule, E-mail (selected), Administration, and Advanced. The main content area is titled 'E-mail' and includes an 'Apply' button and a 'Cancel' button. The configuration options are as follows:

- ☐ Turn E-mail Notification On
- Send alerts and logs through e-mail
 - Your Outgoing Mail Server: [Text Field]
 - Send to This E-mail Address: [Text Field]
 - ☐ My mail server requires authentication
 - User Name: [Text Field]
 - Password: [Text Field]
- ☐ Send Alert Immediately
 - When someone attempts to visit a blocked site
- Send logs according to this schedule
 - None [Dropdown]
 - Day [Dropdown]
 - Time [Dropdown] [Radio] a.m. [Radio] p.m.

At the bottom of the screen, there is a 'Help Center' link and a 'Show/Hide Help Center' button.

2. To receive email logs and alerts from the router, select the **Turn E-mail Notification On** check box.
3. In the Your Outgoing Mail Server field, enter the name of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You might be able to find this information in the configuration screen of your email program. If you leave this field blank, log and alert messages are not sent by email.
4. Enter the email address to which logs and alerts are sent in the Send to This E-mail Address field. This email address is also used for the From address. If you leave this field blank, log and alert messages are not sent by email.
5. If your outgoing email server requires authentication, select the **My Mail Server requires authentication** check box. Fill in the User Name and Password fields for the outgoing email server.
6. You can have email alerts sent immediately when someone attempts to visit a blocked site, and you can specify that logs are sent automatically.

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

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

Administration

6

Managing your network

This chapter describes the router settings for administering and maintaining your router and home network. See also [Remote Management](#) on page 85 for information about upgrading or checking the status of your router over the Internet, and [Traffic Meter](#) on page 88 for information about monitoring the volume of Internet traffic passing through your router's Internet port.

This chapter includes the following sections:

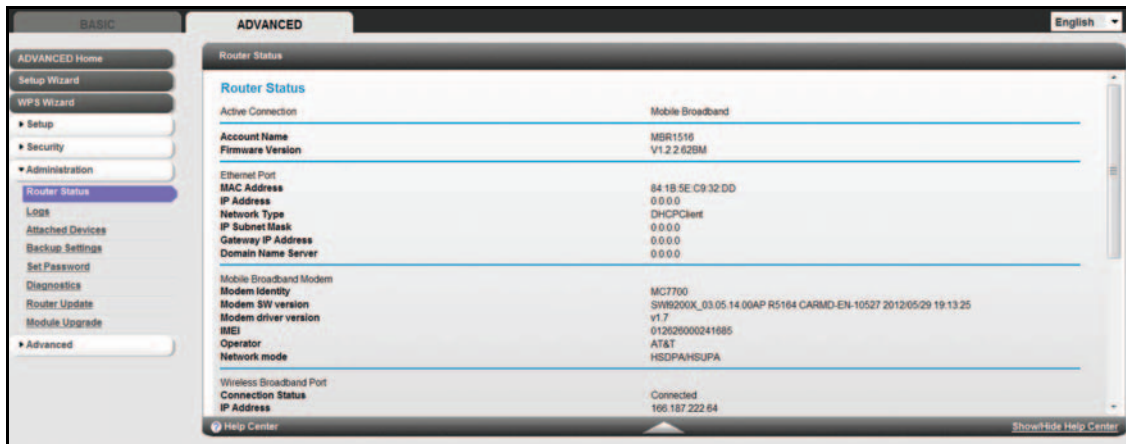
- [Router Status](#)
- [Logs](#)
- [Attached Devices](#)
- [Backup Settings](#)
- [Set Password](#)
- [Diagnostics](#)
- [Router Upgrade](#)
- [Module Upgrade](#)

Router Status

Use the Router Status screen to check the current settings and statistics for your router. This screen shows you the current settings. If something needs to be changed, change it on the relevant screen.

➤ **To view router status and usage information:**

1. Select **ADVANCED > Administration > Router Status** to display the following screen:



The following status information is displayed:

- **Active Connection.** The current WAN interface being used by the router.
- **Account Version.** The router model.
- **Firmware Version.** The version of the router firmware. It changes if you upgrade the router firmware.
- **Ethernet Port.** The current settings of Ethernet broadband port.
 - **MAC Address.** The Media Access Control address. This is the unique physical address being used by the Ethernet (WAN) port of the router.
 - **IP Address.** The IP address being used by the Internet (WAN) port of the router. If no address is shown or the address is 0.0.0, the router cannot connect to the Internet.
 - **Network Type.** This shows if the router is using a fixed IP address on the WAN. If the value is DHCP Client, the router obtains an IP address dynamically from the ISP.
 - **IP Subnet Mask.** The IP subnet mask being used by the Internet (WAN) port of the router.
 - **Gateway IP Address.** The IP address used by the router.
 - **Domain Name Server.** The Domain Name Server addresses being used by the router. A Domain Name Server translates human-language URLs such as www.netgear.com into IP addresses.

- **Mobile Broadband Modem.** This shows the properties of the mobile broadband modem.
 - **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.
 - **IMEI.** International Mobile Equipment Identity. The unique identity of the modem.
 - **Operator.** The ISP for the broadband wireless network.
 - **Network mode.** The mode of the current network the modem is connected to. This is dependent on coverage and distance from the cell site.
- **Wireless Broadband Port.** The current settings of mobile broadband port.
 - **Connection Status.** This shows the status of the wireless broadband connection.
 - **IP Address.** The IP address being used by the Internet (WAN) port of the router. If no address is shown or the address is 0.0.0, the router cannot connect to the Internet.
 - **Protocol.** This shows if the router is using a fixed IP address on the WAN. If the value is DHCP Client, the router obtains an IP address dynamically from the ISP.
 - **IP Subnet Mask.** The IP subnet mask being used by the Internet (WAN) port of the router.
 - **Domain Name Server.** The Domain Name Server addresses being used by the router. A Domain Name Server translates human-language URLs such as www.netgear.com into IP addresses.
- **LAN Port.** These are the current settings, as set in the LAN Setup screen.
 - **MAC Address.** The Media Access Control address. This is the unique physical address being used by the Ethernet (LAN) port of the router.
 - **IP Address.** The IP address being used by the Ethernet (LAN) port of the router. The default is 192.168.0.1.
 - **DHCP.** Identifies whether the router's built-in DHCP server is active for the LAN-attached devices.
 - **IP Subnet Mask.** The subnet mask associated with the LAN IP address.
- **Wireless Port.** These are the current settings, as set in the Wireless Settings screen.
 - **Name (SSID).** The SSID of the router.
 - **Region.** The location (country).
 - **Channel.** The current channel in use.
 - **Wireless AP.** Indicates if the access point feature of the router is enabled or not. If not enabled, the WiFi LED on the front panel is off.
 - **Broadcast Name.** Indicates if the router is broadcasting its SSID.

2. Click **Show Statistics** to see router performance statistics such as the number of packets sent and number of packets received for each port.

Show Statistics

System Up Time 01:22:14

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	100M/Full	922	8930	0	0	123	01:21:43,01:21:45
LAN1	Link Down	---	---	---	---	---	---
LAN2	Link Down	---	---	---	---	---	---
LAN3	Link Down	---	---	---	---	---	---
LAN4	Link Down	---	---	---	---	---	---
WLAN	145M	4004	2987	0	677	62	01:21:57

Poll Interval: (secs)

- **System Up Time.** The time elapsed since the router was last restarted.
- **Port.** The statistics for the WAN (Internet) and LAN (Ethernet) ports. For each port, the screen displays:
 - **Status.** The link status of the port.
 - **TxPkts.** The number of packets transmitted on this port since reset or manual clear.
 - **RxPkts.** The number of packets received on this port since reset or manual clear.
 - **Collisions.** The number of collisions on this port since reset or manual clear.
 - **Tx B/s.** The current transmission (outbound) bandwidth used on the WAN and LAN ports.
 - **Rx B/s.** The current reception (inbound) bandwidth used on the WAN and LAN ports.
 - **Up Time.** The time elapsed since this port acquired the link.
 - **Poll Interval.** The interval at which the statistics are updated in this screen.

To change the polling frequency, enter a time in seconds in the Poll Interval field, and click **Set Interval**.

To stop the polling entirely, click **Stop**.

3. Click **Connection Status** to see information about your current connection.

Mobile Broadband Status	
Connection Status	NO SIM Card Detected
Received Signal Quality(in dbm)	0
Bytes Transmitted	112115
Bytes Received	1735113
Tx B/s	0
Rx B/s	110
System Uptime	01:21:17
Connection Duration	01:20:46

Connection Status	
IP Address	192.168.0.14
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
DHCP Server	192.168.0.1
DNS Server	192.168.0.1
Lease Obtained	1 days,0 Hours,0 minutes.
Lease Expires	0 days,22 Hours,39 minutes.

Poll Interval : (secs)

- Mobile Broadband Status.
 - **Connection Status.** The status of the Internet connection.
 - **Received Signal Quality (in dBm).** Modem radio reception. A small, negative number indicates good signal quality.
 - **Bytes Transmitted.** The number of bytes transmitted in the most recent connection session.
 - **Bytes Received.** The number of bytes received in the most recent connection session.
 - **Tx B/s.** The transmission rate.
 - **Rx B/s.** The receiving rate.
 - **System Uptime.** Time elapsed since the last reboot.
 - **Connection Duration.** Length of the current connection.
- Connection Status.
 - **IP Address.** The IP address that is assigned to the router.
 - **Subnet Mask.** The subnet mask that is assigned to the router.
 - **Default Gateway.** The IP address for the default gateway that the router communicates with.
 - **DHCP Server.** The IP address for the Dynamic Host Configuration Protocol server that provides the TCP/IP configuration for all the computers that are connected to the router.
 - **DNS Server.** The IP address of the Domain Name Service server that provides translation of network names to IP addresses.
 - **Lease Obtained.** The date and time when the lease was obtained.
 - **Lease Expires.** The date and time that the lease expires.

To change the polling frequency, enter a time in seconds in the Poll Interval field, and click **Set Interval**.

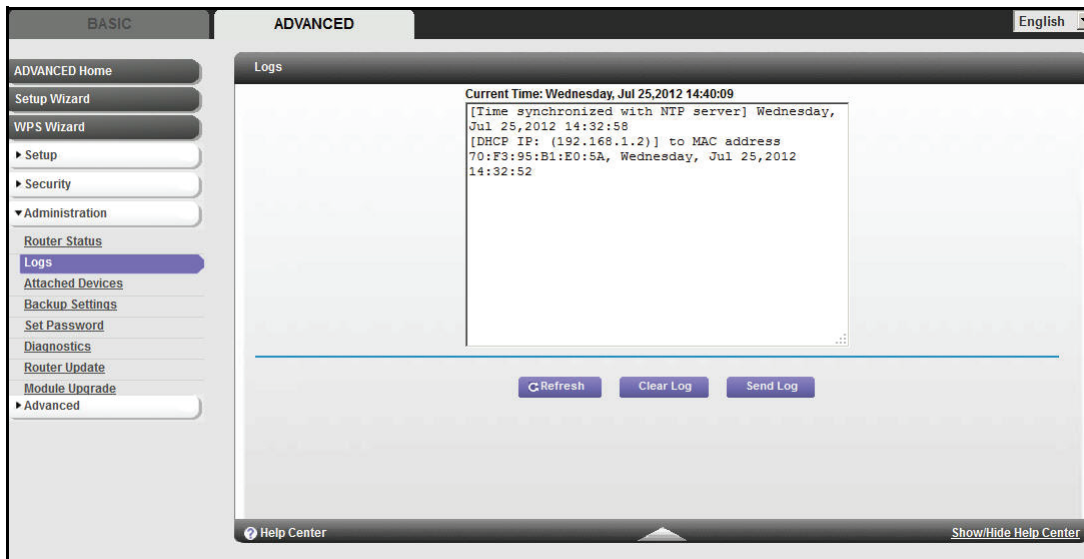
To stop the polling entirely, click **Stop**.

The Close Window button closes the Connection Status screen.

Logs

The log is a detailed record of the websites you have accessed or attempted to access. If you have set up content filtering on the Block Sites screen, the Logs screen shows you when someone on your network tried to access a blocked site. If you have email notification on, you receive these logs in an email message. If you do not have email notification set up, view the logs here.

Select **ADVANCED > Administration > Logs**. The Logs screen displays.



To refresh the log screen, click the **Refresh** button.

To clear the log entries, click the **Clear Log** button.

To email the log immediately, click the **Send Log** button. This feature can be very useful for testing your email settings.

Attached Devices

See [Attached Devices](#) on page 26.

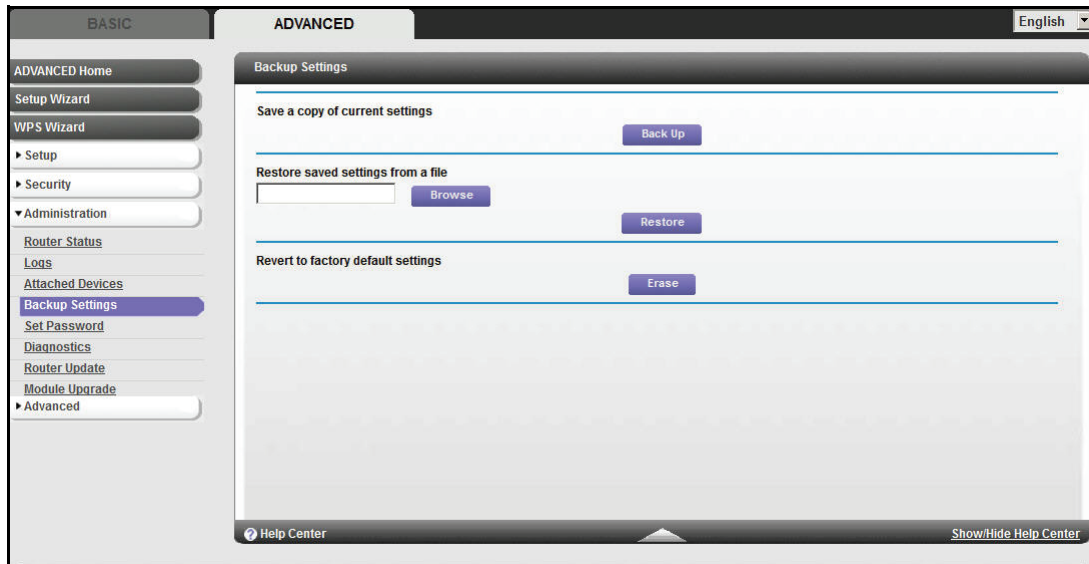
Backup Settings

The configuration settings of the Mobile LTE Broadband 11n Wireless Router are stored within the router in a configuration file. You can back up (save) this file to your computer, restore it, or reset it to the factory default settings.

Back Up Settings

- To back up the router's configuration settings:

1. Select **ADVANCED > Administration > Backup Settings** to display the following screen:



2. Click **Back Up** to save a copy of the current settings.
3. Choose a location to store the .cfg file that is on a computer on your network.

Restore Configuration Settings

- To restore configuration settings that you backed up:

1. Enter the full path to the file on your network, or click the **Browse** button to find the file.
2. When you have located the .cfg file, click the **Restore** button to upload the file to the router.

When the restoration is complete, the router reboots.



WARNING:

Do not interrupt the reboot process.

Erase

Under some circumstances (for example, if you move the router to a different network or if you have forgotten the password), you might want to erase the configuration and restore the factory default settings.

You can either use the Restore Factory Settings button on the back of the router (see [Factory Default Settings](#) on page 99), or you can click the **Erase** button in this screen.

Erase sets the user name to admin, the password to password, and the LAN IP address to 192.168.1.1, and enables the router's DHCP.

Set Password

This feature allows you to change the default password that is used to log in to the router with the user name admin.

This is not the same as changing the password for wireless access. The label on the bottom of your router shows your unique wireless network name (SSID) and password for wireless access (see [Label](#) on page 11).

➤ **To set the password for the user name admin:**

1. Select **ADVANCED > Administration > Set Password** to display the following screen:

2. Type the old password, and type the new password twice in the fields on this screen.
3. If you want to be able to recover the password, select the **Enable Password Recovery** check box.
4. Click **Apply** so that your changes take effect.

Password Recovery

NETGEAR recommends that you enable password recovery if you change the password for the router's user name of admin. Then you will have an easy way to recover the password if it is forgotten. This recovery process is supported in Internet Explorer, Firefox, and Chrome browsers, but not in the Safari browser.

➤ **To set up password recovery:**

1. Select the **Enable Password Recovery** check box.
2. Select two security questions, and provide answers to them.

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

When you use your browser to access the router, the login screen displays. If password recovery is enabled, when you click Cancel, the password recovery process starts. You can then enter the saved answers to the security questions to recover the password.

Diagnostics

Use the Diagnostics screen to perform various diagnostics. For normal operation, these tests are not required.

➤ **To run the diagnostics:**

Select **ADVANCED > Administration > Diagnostics** to display the following screen:

Ping an IP address. Use this test to send a ping packet request to the specified IP address. This procedure is often used to test a connection. If the request times out because no reply is received, this result usually means the destination is unreachable. However, some network devices can be configured not to respond to a ping.

Perform a DNS Lookup. A DNS (Domain Name Server) converts the Internet name (for example, www.netgear.com) to an IP address. If you need the IP address of a web, FTP, mail or other server on the Internet, you can do a DNS lookup to find the IP address.

Display the Routing Table. This operation displays the internal routing table. This information is used by technical support and other staff who understand routing tables.

Reboot the Router. Use this button to perform a remote reboot (restart). You can use this if the router seems to have become unstable or is not operating normally.

Note: Rebooting will break any existing connections either to the router (such as this one) or through the router (for example, LAN users accessing the Internet). However, connections to the Internet are automatically reestablished when possible.

Save diagnostics information. Use this button to view the diagnostics information.

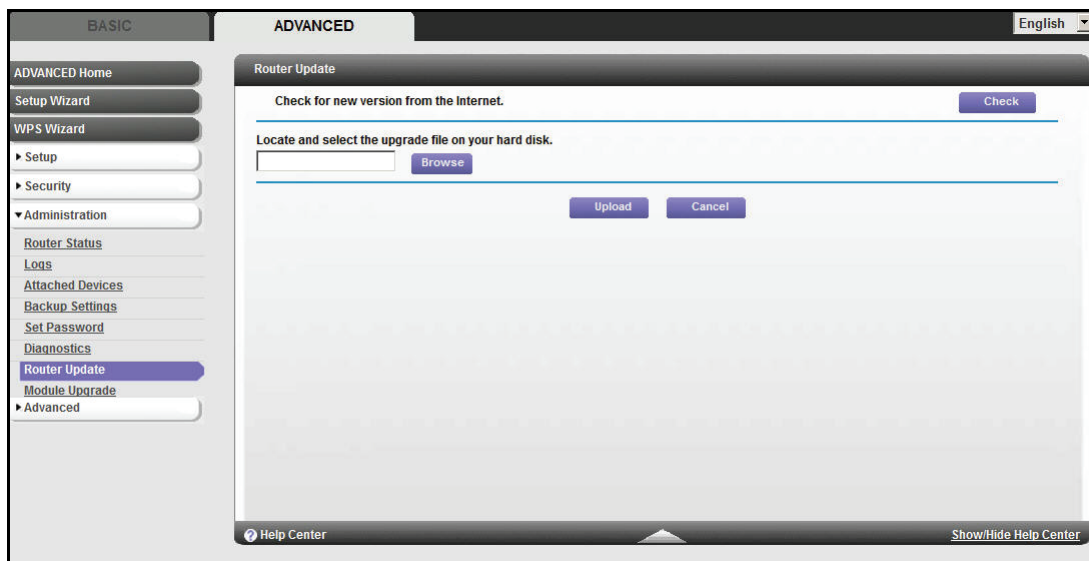
Router Upgrade

The router firmware (routing software) is stored in flash memory. You can update the firmware from the Administration menu on the ADVANCED tab. You might see a message at the top of the NETGEAR genie screens when new firmware is available for your product.

You can use the Check button on the Router Update screen to check and update to the latest firmware for your product if new firmware is available.

➤ **To check for new firmware and update your router:**

1. Select **ADVANCED > Administration > Router Update** to display the following screen:



2. Click **Check**.

The router finds new firmware information if any is available.

3. Click **Yes** to update and locate the firmware you downloaded (the file ends in .img).

**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 could corrupt the firmware.

When the upload is complete, your router restarts. The upgrade process typically takes about 1 minute. Read the new firmware release notes to determine whether or not you need to reconfigure the router after upgrading.

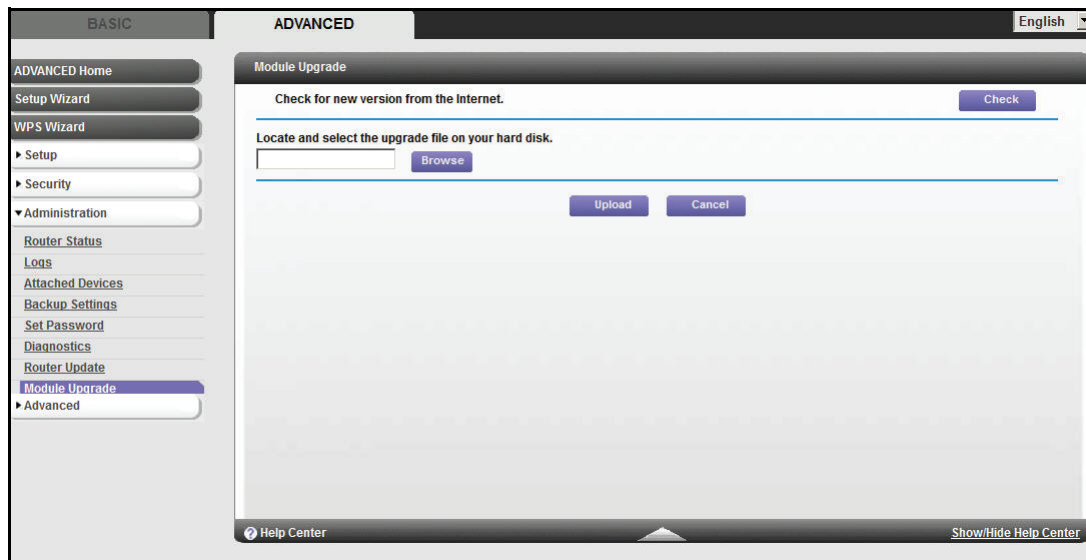
Module Upgrade

The module firmware (broadband mobile software) is stored in flash memory. You can upgrade the firmware from the Administration menu on the ADVANCED tab. You might see a message at the top of the NETGEAR genie screens when new firmware is available for your product.

You can use the Check button on the Module Upgrade screen to check and update to the latest firmware for your product if new firmware is available.

➤ **To check for new firmware and update your router:**

1. Select **ADVANCED > Administration > Module Upgrade** to display the following screen:



2. Click **Check**.

The router finds new firmware information if any is available.

3. Click **Yes** to update and locate the firmware you downloaded (the file ends in .img).



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 could corrupt the firmware.

When the upload is complete, your router restarts. The upgrade process typically takes about 1 minute. Read the new firmware release notes to determine whether or not you need to reconfigure the router after upgrading.

Advanced Settings

7

This chapter describes the advanced features of your router. The information is for users with a solid understanding of networking concepts who want to set the router up for unique situations such as when remote access from the Internet by IP or domain name is needed.

This chapter includes the following sections:

- *SIM Settings*
- *SMS Messages*
- *Wireless Settings*
- *Wireless Repeating*
- *Port Forwarding and Port Triggering*
- *Dynamic DNS*
- *Static Routes*
- *Remote Management*
- *Universal Plug and Play*
- *Traffic Meter*

SIM Settings

Your ISP provides you with a SIM card so that you can access mobile broadband. Use this screen to change your SIM card settings.

➤ **To change your SIM card settings:**

1. Select **ADVANCED > Advanced > SIM Settings** to display the following screen:

2. Change your SIM card settings as necessary:
 - **Enabling or Disabling the PIN Code.** Enable or disable the use of the SIM card PIN code. Enter your current PIN code to authorize this change.
 - **Changing the PIN Code.** The PIN code prevents the use of the SIM card in an unauthorized device. Also, change the PIN code regularly for security reasons. Enter your current PIN code to authorize this change, followed by the new PIN code you have chosen.
3. Click **Apply** so that your changes take effect.

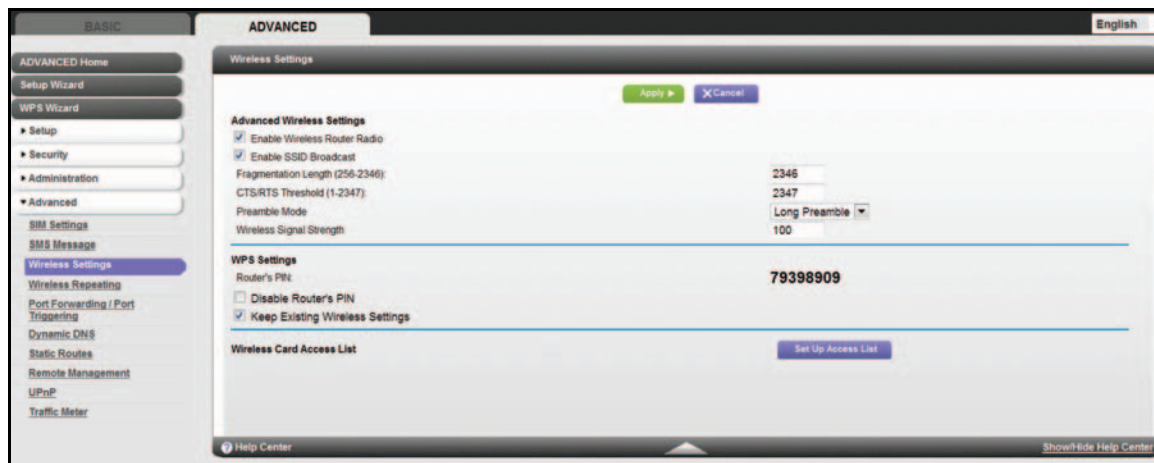
SMS Messages

See [SMS Message](#) on page 30.

Wireless Settings

Note: The wireless router is already configured with the optimum settings. Do not alter these settings unless directed by NETGEAR support. Incorrect settings disable the wireless router.

Select **ADVANCED > Advanced > Wireless Settings** to display the following screen:



The following settings are available in this screen:

Advanced Wireless Settings. Do not change these settings unless directed to do so by NETGEAR support.

- **Enable Wireless Router Radio.** You can completely turn off the wireless portion of the wireless router by clearing this check box. Select this check box again to enable the wireless portion of the router. When the wireless radio is disabled, other members of your household can use the router by connecting their computers to the router with an Ethernet cable.
- **Enable SSID Broadcast.** This setting enables broadcasting of the SSID.

Note: The Fragmentation Length, CTS/RTS Threshold, and Preamble Mode options are reserved for wireless testing and advanced configuration only. Do not change these settings.

- **Wireless Signal Strength.** This setting allows adjusting the power of Wi-Fi from 1% (minimum) to 100% (maximum). Enter an integer ranging from 1 to 100 (default) in this field. Lowering the Wi-Fi power limits the range of Wi-Fi and reduces the Wi-Fi radiation.

WPS Settings. You can add WPS devices to your network.

- **Router's PIN.** This is the PIN number you use on a registrar (for example, from Network Explorer on a Vista Windows PC) to configure the router's wireless settings through WPS. You can also find the PIN on the router's product label.
- **Disable Router's PIN.** You can configure the router's wireless settings or add a wireless client through WPS using the router's PIN only when the PIN is enabled. The router's PIN can be disabled temporarily when the router detects suspicious attempts to break into the router's wireless settings by using the router's PIN through WPS. You can manually enable this function by clearing the check box and clicking the Apply button.
- **Keep Existing Wireless Settings.** This setting shows whether the router is in the WPS configured state. If this option is not selected, adding a new wireless client changes the router's wireless settings to an automatically generated random SSID and security key. In addition, when this option is selected, some external registrars (for example, Network Explorer on Vista Windows) might not see the router.

Configuring the basic wireless settings from the router's web management interface selects this option automatically.

Wireless Card Access List. By default, any wireless computer that is configured with the correct SSID is allowed access to your wireless network. For increased security, restrict access to the wireless network to allow only specific computers based on their MAC addresses. Click the **Set Up Access List** button display the Wireless Card Access List screen. On this screen you can restrict access to your network to specific devices based on their MAC address.

Wireless Card Access List

Apply Cancel

☐ Turn Access Control On

Device Name	MAC Address

+Add Edit X Delete

Click **Add** to add wireless devices to your network based on their MAC addresses.

Wireless Card Access List

+ Add X Cancel Refresh

Available Wireless Cards

Device Name	MAC Address
User-HP	70:13:95:b1:e0:5a

Wireless Card Entry

Device Name:

MAC Address:

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

Wireless Repeating

You can set the Mobile LTE Broadband 11n Wireless Router up to be used as a wireless access point (AP). Doing this enables the router to act as a wireless repeater. A wireless repeater connects to another wireless router as a client where the network to which it connects becomes the ISP service.

Wireless repeating is a type of Wireless Distribution System (WDS). A WDS allows a wireless network to be expanded through multiple access points instead of using a wired backbone to link them. The following figure shows a wireless repeating scenario.

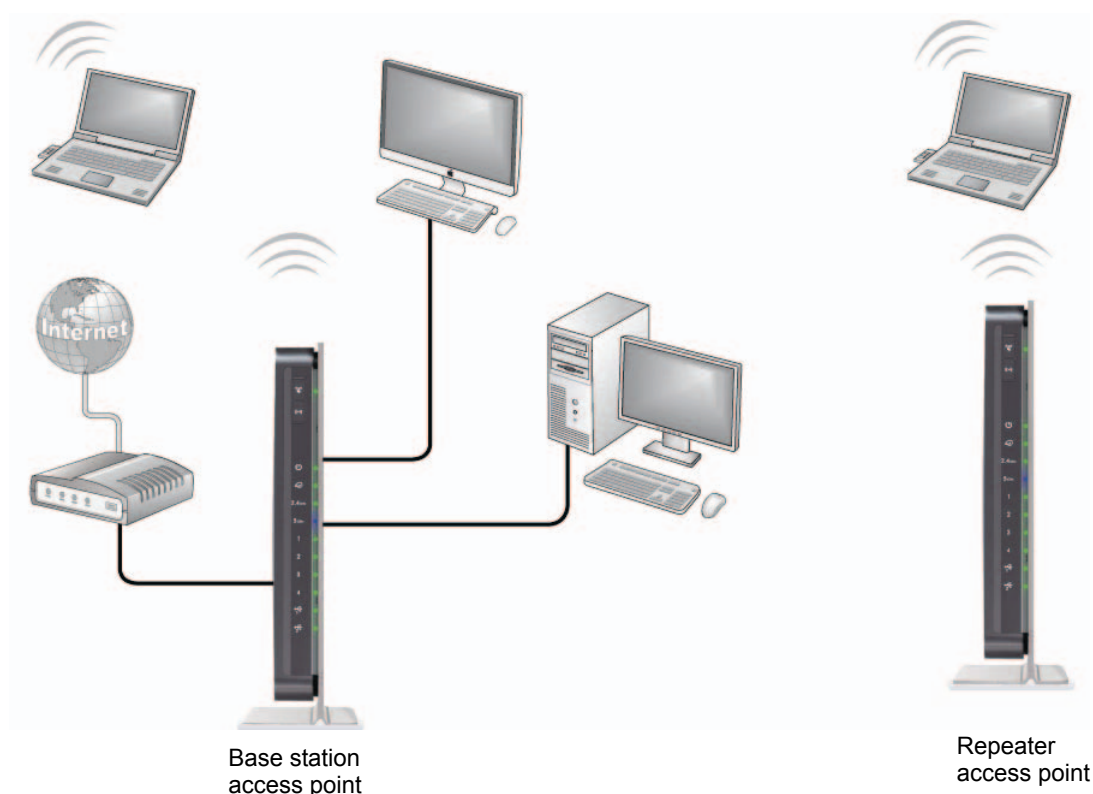


Figure 6. Wireless repeating scenario

Note: If you use the wireless repeating function, you need to select either **WEP** or **None** as a security option in the Wireless Settings screen. The WEP option displays only if you select the wireless mode **Up to 54 Mbps** in the Wireless Settings screen.

Wireless base station. The router acts as the parent access point, bridging traffic to and from the child repeater access point, as well as handling wireless and wired local computers. To configure this mode, you have to know the MAC addresses of the child repeater access point.

Wireless repeater. The router sends all traffic from its local wireless or wired computers to a remote access point. To configure this mode, you have to know the MAC address of the remote parent access point.

The MBR1516 router is always in dual band concurrent mode, unless you turn off one radio. Be aware that if you enable the wireless repeater in either radio band, the wireless base station or wireless repeater cannot be enabled in the other radio band. However, if you enable the wireless base station in either radio band and use the other radio band as a wireless router or wireless base station, dual band concurrent mode is not affected.

For you to set up a wireless network with WDS, the following conditions have to be met for both access points:

- Both access points have to use the same SSID, wireless channel, and encryption mode.
- Both access points have to be on the same LAN IP subnet. That is, all the access point LAN IP addresses are in the same network.
- All LAN devices (wired and wireless computers) have to be configured to operate in the same LAN network address range as the access points.

Wireless Repeating Function

Select **ADVANCED > Advanced > Wireless Repeating** to view or change wireless repeater settings for the router.

The screenshot shows the 'Wireless Repeating Function' configuration page. The interface has a sidebar on the left with a menu including 'ADVANCED Home', 'Setup Wizard', 'WPS Wizard', 'Setup', 'Security', 'Administration', and 'Advanced'. Under 'Advanced', there are links for 'SIM Settings', 'SMS Message', 'Wireless Settings', 'Wireless Repeating' (which is highlighted), 'Port Forwarding / Port Triggering', 'Dynamic DNS', 'Static Routes', 'Remote Management', 'UPnP', and 'Traffic Meter'. The main content area is titled 'Wireless Repeating Function' and contains the following settings:

- ☐ **Enable Wireless Repeating Function**
- Wireless MAC of this router C0:3F:0E:B4:67:A0
- ☒ **Wireless Repeater**
 - Repeater IP Address: 192.168.1.
 - ☐ **Disable Wireless Client Association**
 - Base Station MAC Address:
- ☐ **Wireless Base Station**
 - ☐ **Disable Wireless Client Association**
 - Repeater MAC Address 1:
 - Repeater MAC Address 2:
 - Repeater MAC Address 3:
 - Repeater MAC Address 4:

At the top right of the main area are 'Apply' and 'Cancel' buttons. At the bottom left is a 'Help Center' link, and at the bottom right is a 'Show/Hide Help Center' link.

- **Enable Wireless Repeating Function.** Select the check box for the 2.4 GHz or 5 GHz network to use the wireless repeating function.
- **Wireless MAC of this router.** This field displays the MAC address for your router for your reference. You need to enter this MAC address in the corresponding Wireless Repeating Function screen of the other access point you are using.
- **Wireless Repeater.** If your router is the repeater, select this radio button.

Repeater IP Address. If your router is the repeater, enter the IP address of the other access point.

Disable Wireless Client Association. If your router is the repeater, selecting this check box means that wireless clients cannot associate with it. Only LAN client associations are allowed.

- If you are setting up a point-to-point bridge, select this check box.
- If you want all client traffic to go through the other access point (repeater with wireless client association), leave this check box cleared.

Base Station MAC Address. If your router is the repeater, enter the MAC address for the access point that is the base station.

- **Wireless Base Station.** If your router is the base station, select this radio button.

Disable Wireless Client Association. If your router is the base station, selecting this check box means that wireless clients cannot associate with it. Only LAN client associations are allowed.

Repeater MAC Address (1 through 4). If your router is the base station, it can act as the “parent” of up to 4 other access points. Enter the MAC addresses of the other access points in these fields.

Set Up the Base Station

The wireless repeating function works only in hub and spoke mode. The units cannot be daisy-chained. You have to know the wireless settings for both units. You have to know the MAC address of the remote unit. First, set up the base station, and then set up the repeater.

➤ To set up the base station:

1. Set up both units with exactly the same wireless settings (SSID, mode, channel, and security). Note that the wireless security option has to be set to None or WEP.
2. Select **ADVANCED > Advanced > Wireless Repeating Function** to display the Wireless Repeating Function screen.
3. In the Wireless Repeating Function screen (depending on the frequency you want to use), select the **Enable Wireless Repeating Function** check box and select the **Wireless Base Station** radio button.
4. Enter the MAC address for one or more repeater units.
5. Click **Apply** to save your changes.

Set Up a Repeater Unit

Use a wired Ethernet connection to set up the repeater unit to avoid conflicts with the wireless connection to the base station.

Note: If you are using the MBR1516 base station with a non-NETGEAR router as the repeater, you might need to change additional configuration settings. In particular, you should disable the DHCP server function on the wireless repeater AP.

➤ **To configure the router as a repeater unit:**

1. Log in to the router that will be the repeater. Select **BASIC > Wireless Settings** and verify that the wireless settings match the base unit exactly. The wireless security option has to be set to **WEP** or **None**.
2. Select **ADVANCED > Advanced > Wireless Repeating Function**. Select the **Enable Wireless Repeating Function** check box and the **Wireless Repeater** radio button.
3. Fill in the Repeater IP Address field. This IP address has to be in the same subnet as the base station, but different from the LAN IP address of the base station.
4. Click **Apply** to save your changes.
5. Verify connectivity across the LANs.

A computer on any wireless or wired LAN segment of the router should be able to connect to the Internet or share files and printers with any other wireless or wired computer or server connected to the other access point.

Port Forwarding and Port Triggering

By default, the router blocks inbound traffic from the Internet to your computers except replies to your outbound traffic. You might need to create exceptions to this rule for these purposes:

- To allow remote computers on the Internet to access a server on your local network.
- To allow certain applications and games to work correctly when their replies are not recognized by your router.

Your router provides two features for creating these exceptions: port forwarding and port triggering. The next sections provide background information to help you understand how port forwarding and port triggering work, and the differences between the two.

Remote Computer Access Basics

When a computer on your network needs to access a computer on the Internet, your computer sends your router a message containing the source and destination address and process information. Before forwarding your message to the remote computer, your router has to modify the source information and create and track the communication session so that replies can be routed back to your computer.

Here is an example of normal outbound traffic and the resulting inbound responses:

1. You open a browser, and your operating system assigns port number 5678 to this browser session.
2. You type `http://www.example.com` into the URL field, and your computer creates a web page request message with the following address and port information. The request message is sent to your router.

Source address. Your computer's IP address.

Source port number. 5678, which is the browser session.

Destination address. The IP address of `www.example.com`, which your computer finds by asking a DNS server.

Destination port number. 80, which is the standard port number for a web server process.

3. Your router creates an entry in its internal session table describing this communication session between your computer and the web server at `www.example.com`. Before sending the web page request message to `www.example.com`, your router stores the original information and then modifies the source information in the request message, performing Network Address Translation (NAT):
 - The source address is replaced with your router's public IP address. This is necessary because your computer uses a private IP address that is not globally unique and cannot be used on the Internet.
 - The source port number is changed to a number chosen by the router, such as 33333. This is necessary because two computers could independently be using the same session number.

Your router then sends this request message through the Internet to the web server at `www.example.com`.

4. The web server at `www.example.com` composes a return message with the requested web page data. The return message contains the following address and port information. The web server then sends this reply message to your router.

Source address. The IP address of `www.example.com`.

Source port number. 80, which is the standard port number for a web server process.

Destination address. The public IP address of your router.

Destination port number. 33333.

5. Upon receiving the incoming message, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router then modifies the message to restore the original address information replaced by NAT. Your router sends this reply message to your computer, which displays the web page from `www.example.com`. The message now contains the following address and port information.

Source address. The IP address of `www.example.com`.

Source port number. 80, which is the standard port number for a web server process.

Destination address. Your computer's IP address.

Destination port number. 5678, which is the browser session that made the initial request.

6. When you finish your browser session, your router eventually detects a period of inactivity in the communications. Your router then removes the session information from its session table, and incoming traffic is no longer accepted on port number 33333.

Port Triggering to Open Incoming Ports

In the preceding example, requests are sent to a remote computer by your router from a particular service port number, and replies from the remote computer to your router are directed to that port number. If the remote server sends a reply back to a different port number, your router does not recognize it and discards it. However, some application servers (such as FTP and IRC servers) send replies back to multiple port numbers. Using the port triggering function of your router, you can tell the router to open additional incoming ports when a particular outgoing port originates a session.

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port, but also sends an “identify” message to your computer on port 113. Using port triggering, you can tell the router, “When you initiate a session with destination port 6667, you have to also allow incoming traffic on port 113 to reach the originating computer.” Using steps similar to the preceding example, the following sequence shows the effects of the port triggering rule you have defined:

1. You open an IRC client program to start a chat session on your computer.
2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your router.
3. Your router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.
4. Noting your port triggering rule and having observed the destination port number of 6667, your router creates an additional session entry to send any incoming port 113 traffic to your computer.
5. The IRC server sends a return message to your router using the NAT-assigned source port (as in the previous example, say port 33333) as the destination port. The IRC server also sends an “identify” message to your router with destination port 113.
6. Upon receiving the incoming message to destination port 33333, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router restores the original address information replaced by NAT and sends this reply message to your computer.
7. Upon receiving the incoming message to destination port 113, your router checks its session table and learns that there is an active session for port 113, associated with your computer. The router replaces the message’s destination IP address with your computer’s IP address and forwards the message to your computer.

8. When you finish your chat session, your router eventually senses a period of inactivity in the communications. The router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

To configure port triggering, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

Note: Only one computer at a time can use the triggered application.

Port Forwarding to Permit External Host Communications

In both of the preceding examples, your computer initiates an application session with a server computer on the Internet. However, you might need to allow a client computer on the Internet to initiate a connection to a server computer on your network. Normally, your router ignores any inbound traffic that is not a response to your own outbound traffic. You can configure exceptions to this default rule by using the port forwarding feature.

A typical application of port forwarding can be shown by reversing the client-server relationship from the previous web server example. In this case, a remote computer's browser needs to access a web server running on a computer in your local network. Using port forwarding, you can tell the router, "When you receive incoming traffic on port 80 (the standard port number for a web server process), forward it to the local computer at 192.168.1.123." The following sequence shows the effects of the port forwarding rule you have defined:

1. The user of a remote computer opens a browser and requests a web page from www.example.com, which resolves to the public IP address of your router. The remote computer composes a web page request message with the following destination information:

Destination address. The IP address of www.example.com, which is the address of your router.

Destination port number. 80, which is the standard port number for a web server process.

The remote computer then sends this request message through the Internet to your router.

2. Your router receives the request message and looks in its rules table for any rules covering the disposition of incoming port 80 traffic. Your port forwarding rule specifies that incoming port 80 traffic should be forwarded to local IP address 192.168.1.123. Therefore, your router modifies the destination information in the request message:

The destination address is replaced with 192.168.1.123.

Your router then sends this request message to your local network.

3. Your web server at 192.168.1.123 receives the request and composes a return message with the requested web page data. Your web server then sends this reply message to your router.
4. Your router performs Network Address Translation (NAT) on the source IP address, and sends this request message through the Internet to the remote computer, which displays the web page from www.example.com.

To configure port forwarding, you need to know which inbound ports the application needs. You usually can determine this information by contacting the publisher of the application or the relevant user groups and newsgroups.

How Port Forwarding Differs from Port Triggering

The following points summarize the differences between port forwarding and port triggering:

- Port triggering can be used by any computer on your network, although only one computer can use it at a time.
- Port forwarding is configured for a single computer on your network.
- Port triggering does require that you know the computer's IP address in advance. The IP address is captured automatically.
- Port forwarding requires that you specify the computer's IP address during configuration, and the IP address can never change.
- Port triggering requires specific outbound traffic to open the inbound ports, and the triggered ports are closed after a period of no activity.
- Port forwarding is always active and does not need to be triggered.

Set Up Port Forwarding to Local Servers

Using the port forwarding feature, you can allow certain types of incoming traffic to reach servers on your local network. For example, you might want to make a local web server, FTP server, or game server visible and available to the Internet.

Use the Port Forwarding screen to configure the router to forward specific incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a default DMZ server to which all other incoming protocols are forwarded.

Before starting, you need to determine which type of service, application, or game you want to provide, and the local IP address of the computer that will provide the service. The server computer has to always have the same IP address.

➤ To set up port forwarding:

Tip: To ensure that your server computer always has the same IP address, use the reserved IP address feature of your Mobile LTE Broadband 11n Wireless Router.

1. Select **ADVANCED > Advanced > Port Forwarding/Port Triggering** to display the following screen:

Port Forwarding is selected as the service type.

2. From the Service Name list, select the service or game that you will host on your network. If the service does not appear in the list, see [Add a Custom Service](#) on page 79.
3. In the corresponding Server IP Address field, enter the last digit of the IP address of your local computer that will provide this service.
4. Click **Add**. The service appears in the list in the screen.

Add a Custom Service

To define a service, game, or application that does not appear in the Service Name list, you have to first determine which port number or range of numbers is used by the application. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

➤ To add a custom service:

1. Select **ADVANCED > Advanced > Port Forwarding/Port Triggering**.
2. Select **Port Forwarding** as the service type.
3. Click the **Add Custom Service** button to display the following screen:

4. In the Service Name field, enter a descriptive name.
5. In the Service Type list, select the protocol. If you are unsure, select **TCP/UDP**.

6. In the Starting Port field, enter the beginning port number.
 - If the application uses a single port, enter the same port number in the Ending Port field.
 - If the application uses a range of ports, enter the ending port number of the range in the Ending Port field.
7. In the Server IP Address field, enter the IP address of your local computer that will provide this service.
8. Click **Apply**. The service appears in the list in the Port Forwarding/Port Triggering screen.

Edit or Delete a Port Forwarding Entry

➤ **To edit or delete a port forwarding entry:**

1. In the table, select the radio button next to the service name.
2. Click **Edit Service** or **Delete Service**.

Application Example: Making a Local Web Server Public

If you host a web server on your local network, you can use port forwarding to allow web requests from anyone on the Internet to reach your web server.

➤ **To make a local web server public:**

1. Assign your web server either a fixed IP address or a dynamic IP address using DHCP address reservation. In this example, your router will always give your web server an IP address of 192.168.1.33.
2. In the Port Forwarding screen, configure the router to forward the HTTP service to the local address of your web server at **192.168.1.33**. HTTP (port 80) is the standard protocol for web servers.
3. (Optional) Register a host name with a Dynamic DNS service, and configure your router to use the name as described in [Dynamic DNS](#) on page 82. To access your web server from the Internet, a remote user has to know the IP address that has been assigned by your ISP. However, if you use a Dynamic DNS service, the remote user can reach your server by a user-friendly Internet name, such as mynetgear.dyndns.org.

Set Up Port Triggering

Port triggering is a dynamic extension of port forwarding that is useful in these cases:

- More than one local computer needs port forwarding for the same application (but not simultaneously).
- An application needs to open incoming ports that are different from the outgoing port.

When port triggering is enabled, the router monitors outbound traffic looking for a specified outbound “trigger” port. When the router detects outbound traffic on that port, it remembers the IP address of the local computer that sent the data. The router then temporarily opens the specified incoming port or ports, and forwards incoming traffic on the triggered ports to the triggering computer.

While port forwarding creates a static mapping of a port number or range to a single local computer, port triggering can dynamically open ports to any computer that needs them and can close the ports when they are no longer needed.

Note: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable Universal Plug and Play (UPnP) according to the instructions in [Universal Plug and Play](#) on page 86.

To set up port triggering, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

➤ **To set up port triggering:**

1. Select **ADVANCED > Advanced > Port Forwarding/Port Triggering**.
2. Select the **Port Triggering** radio button to display the port triggering information.

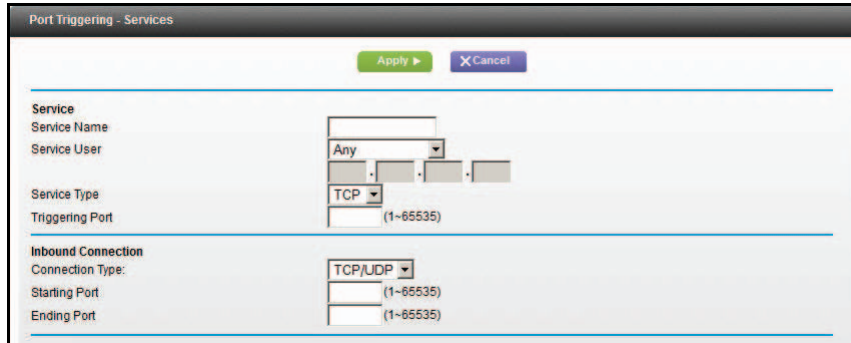
3. Clear the **Disable Port Triggering** check box if it is selected.

Note: If the *Disable Port Triggering* check box is selected after you configure port triggering, port triggering is disabled. However, any port triggering configuration information you added to the router is retained even though it is not used.

4. In the Port Triggering Timeout field, enter a value up to 9999 minutes.

This value controls the inactivity timer for the designated inbound ports. The inbound ports close when the inactivity time expires. This is required because the router cannot be sure when the application has terminated.

5. Click **Add Service** to display the following screen:



6. In the Service Name field, type a descriptive service name.
7. In the Service User list, select **Any** (the default) to allow this service to be used by any computer on the Internet. Otherwise, select **Single address**, and enter the IP address of one computer to restrict the service to a particular computer.
8. Select the service type, either **TCP** or **UDP** or both (**TCP/UDP**). If you are not sure, select TCP/UDP.
9. In the Triggering Port field, enter the number of the outbound traffic port that will cause the inbound ports to be opened.
10. Enter the inbound connection port information in the Connection Type, Starting Port, and Ending Port fields.
11. Click **Apply**. The service appears in the Port Triggering Portmap table.

Dynamic DNS

If your Internet service provider (ISP) gave you 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 do 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. This type of service lets you register your domain to their IP address and forwards traffic directed at your domain to your frequently changing IP address.

If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the Dynamic DNS service will not work because private addresses are not routed on the Internet.

Your router contains a client that can connect to the Dynamic DNS service provided by DynDNS.org. First visit their website at <http://www.dyndns.org> and obtain an account and host name that you configure in the router. Then, whenever your ISP-assigned IP address changes, your router automatically contacts the Dynamic DNS service provider, logs in to your account, and registers your new IP address. If your host name is hostname, for example, you can reach your router at <http://hostname.dyndns.org>.

On the **ADVANCED** tab, select **Advanced > Dynamic DNS** to display the following screen:

The screenshot shows the 'Dynamic DNS' configuration page. The sidebar on the left includes categories like 'SIM Settings', 'SMS Message', 'Wireless Settings', 'Wireless Repeating', 'Port Forwarding / Port Triggering', 'Dynamic DNS' (highlighted), 'Static Routes', 'Remote Management', 'UPnP', and 'Traffic Meter'. The main content area has a title bar 'Dynamic DNS' with 'Apply', 'Cancel', and 'Show Status' buttons. Below is a checkbox 'Use a Dynamic DNS Service'. Underneath, there's a 'Service Provider' dropdown menu showing 'www.DynDNS.org'. Below that are three input fields: 'Host Name', 'User Name', and 'Password'. At the bottom left is a 'Help Center' link, and at the bottom right is a 'Show/Hide Help Center' link.

Figure 7. Forward traffic to a changing IP address

➤ **To set up Dynamic DNS:**

1. Register for an account with one of the Dynamic DNS service providers whose names appear in the Service Provider list.
2. Select the **Use a Dynamic DNS Service** check box.
3. Select the name of your Dynamic DNS service provider. For example, for DynDNS.org, select **www.dyndns.org**.
4. Type the host name (or domain name) that your Dynamic DNS service provider gave you.
5. Type the user name for your Dynamic DNS account. This is the name that you use to log in to your account, not your host name.
6. Type the password (or key) for your Dynamic DNS account.
7. Click **Apply** to save your configuration.

Static Routes

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

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 192.168.1.100.

- Your company's network address is 134.177.0.0.

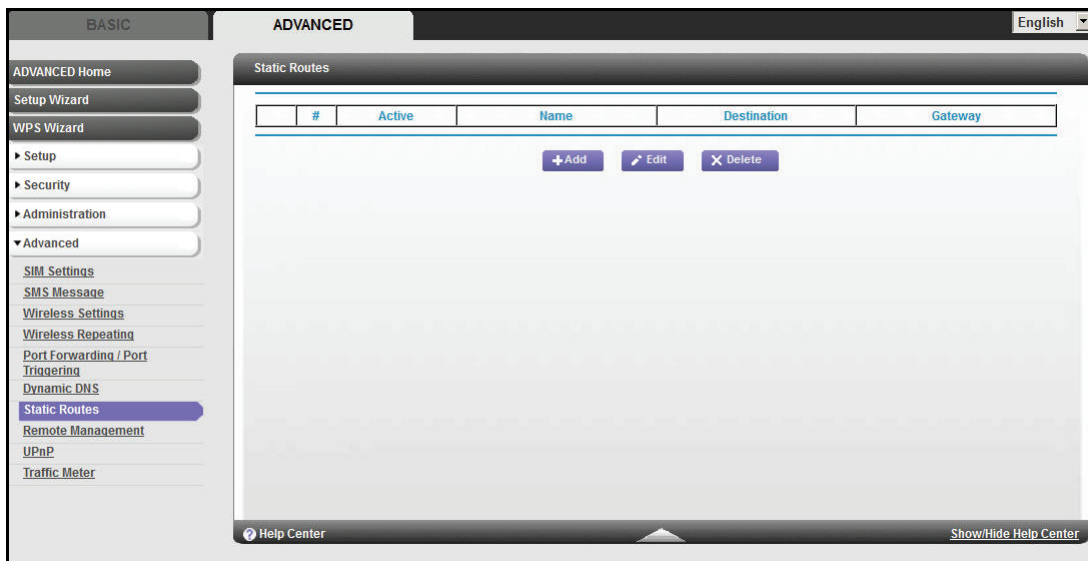
When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.1.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 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 have to define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.1.100. In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Gateway IP Address field specifies that all traffic for these addresses should be forwarded to the ISDN router at 192.168.1.100.
- A metric value of 1 will work since the ISDN router is on the LAN.
- Private is selected only as a precautionary security measure in case RIP is activated.

➤ **To set up a static route:**

1. Select **ADVANCED > Advanced > Static Routes** to display the following screen:



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

3. In the Route Name field, type a name for this static route (for identification purposes only.)
4. Select the **Private** check box if you want to limit access to the LAN only. If Private is selected, the static route is not reported in RIP.
5. Select the **Active** check box to make this route effective.
6. Type the IP address of the final destination.
7. Type the IP subnet mask for this destination. If the destination is a single host, type **255.255.255.255**.
8. Type the gateway IP address, which has to be a router on the same LAN segment as the Mobile LTE Broadband 11n Wireless Router.
9. Type a number between 1 and 15 as the metric value.

This value 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 1.

10. Click **Apply** to add the static route.

Remote Management

The remote management feature lets you upgrade or check the status of your Mobile LTE Broadband 11n Wireless Router over the Internet.

➤ To set up remote management:

1. Select **ADVANCED > Advanced > Remote Management**.

The screenshot displays the 'Remote Management' configuration page. At the top, there are 'Apply' and 'Cancel' buttons. Below them is a checkbox labeled 'Turn Remote Management On'. The 'Remote Management Address' is displayed as 'http://192.168.0.14:8080'. Under the 'Allow Remote Access By:' section, three options are available: 'Only This Computer', 'IP Address Range' (with 'From' and 'To' fields), and 'Everyone' (which is selected). The 'Port Number' field is set to '8080'. The left sidebar contains a list of settings categories, with 'Remote Management' currently selected. The top of the interface shows 'BASIC' and 'ADVANCED' tabs, with 'ADVANCED' being the active tab, and a language selector set to 'English'.

Note: Be sure to change the router's default login password to a very secure password. The ideal password should contain no dictionary words from any language and contain uppercase and lowercase letters, numbers, and symbols. It can be up to 30 characters.

2. Select the **Turn Remote Management On** check box.
3. Under Allow Remote Access By, select the extent of external IP addresses that are to be allowed to access the router's remote management.

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

- To allow access from a single IP address on the Internet, select **Only This Computer**. Enter the IP address that will be allowed access.
 - 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 any IP address on the Internet, select **Everyone**.
4. Specify the port number for accessing the web management interface.

Normal web browser access uses the standard HTTP service port 80. For greater security, enter a custom port number for the remote web management interface. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.
 5. Click **Apply** to have your changes take effect.
 6. When accessing your router from the Internet, type your router's WAN IP address into your browser's 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** in your browser.

Universal Plug and Play

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

Note: If you use applications such as multiplayer gaming, peer-to-peer connections, or real-time communications such as instant messaging or remote assistance (a feature in Windows XP), you should enable UPnP.

➤ **To turn on Universal Plug and Play:**

1. Select **ADVANCED > Advanced > UPnP**. The UPnP screen displays.

2. The available settings and information in this screen are:

Turn UPnP On. UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is disabled. If this check box is not selected, the router does 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 broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations can 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. The time to live hop count is the number of steps a broadcast packet is 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.

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. The UPnP Portmap Table also displays what type of port is open and whether that port is still active for each IP address.

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

Traffic Meter

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

➤ **To monitor Internet traffic:**

1. Click **ADVANCED > Advanced > Traffic Meter** to display the following screen:

2. To enable the traffic meter, select the **Enable Traffic Meter for Internet** check box.
3. If you would like to record and restrict the volume of Internet traffic, select the **Traffic volume control by** radio button. You can select one of the following options for controlling the traffic volume:
 - No limit.** No restriction is applied when the traffic limit is reached.
 - Download only.** The restriction is applied to incoming traffic only.
 - Both directions.** The restriction is applied to both incoming and outgoing traffic.
4. You can limit the amount of data traffic allowed per month by specifying how many Mbytes per month are allowed or by specifying how many hours of traffic are allowed.
5. Set the traffic counter to begin at a specific time and date.
6. Set up traffic control to issue a warning message before the monthly limit of Mbytes or hours is reached. You can select one of the following to occur when the limit is attained:
 - The Internet LED flashes green or amber.
 - The Internet connection is disconnected and disabled.
7. Set up Internet traffic statistics to monitor the data traffic.
8. Click the **Traffic Status** button to get a live update on Internet traffic status on your router.
9. Click **Apply** to save your settings.

This chapter gives information about troubleshooting your Mobile LTE Broadband 11n Wireless Router. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the router on?
Go to [Basic Functioning](#) on page 90.
- Have I connected the router correctly?
Go to [Basic Functioning](#) on page 90.
- I can't access the router's configuration with my browser.
Go to [Troubleshoot Access to the Router Main Menu](#) on page 92.
- I've configured the router but I can't access the Internet.
Go to [Troubleshoot the ISP Connection](#) on page 93.
- I've configured the router but I can't access my local network.
Go to [Troubleshoot a TCP/IP Network Using the Ping Utility](#) on page 95.
- How do I set daylight saving time?
Go to [Problems with Date and Time](#) on page 97.
- I want to clear the configuration and start over again.
Go to [Restore the Default Configuration and Password](#) on page 97.

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 a minute, verify that:
 - a. The Power LED is still solid green. An amber light indicates the unit has failed its power-on self-test (POST).
 - b. The Internet Port LED is lit.
 - c. The WiFi LED is lit. The WiFi radio is on by default.
 - d. The LAN Ports LED is lit when any local ports are connected.

If a LAN Port LED on the back of the unit is lit, a link has been established to the connected device. If a LAN port is connected to a 100 Mbps device, verify that the port's LED is green. If the port is 10 Mbps, the LED is amber.

- e. The WAN Port LED is lit when the router is connected to a wired modem.
- f. The Signal Quality LED is lit when the router has detected a mobile broadband signal.

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

LED		Action
Power 	Power LED is off.	- Make sure that the power cord is correctly connected to your router, and that the power supply adapter is correctly 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 might have a hardware problem and should contact technical support.
	Power LED is amber.	There is a fault within the router. Try to clear the fault as follows: - Cycle the power to see if the router recovers. - Clear the router's configuration to factory defaults. This sets the router's IP address to www.routerlogin.net. This procedure is explained in Restore the Default Configuration and Password on page 97. If the error persists, you might have a hardware problem and should contact technical support.

LED		Action
Internet Port 	Internet Port LED is off.	Be sure the SIM card you received is in the router. SIM cards from other devices will not function in the router, and this SIM card will not function in other devices.
	Internet Port LED is amber.	The router cannot connect to the Internet. Check the Internet connection option being used. - For the mobile broadband connection option, check the Signal Quality LEDs. - For the Ethernet connection option, check the WAN Port LED.
	Internet Port LED is blinking amber and green.	The traffic meter feature is enabled, and the limit set has been reached.
WiFi 	WiFi LED is off.	The WiFi radio has been turned off. If you want a WiFi connection with the router, press the WiFi button to turn the WiFi radio back on.
	WiFi LED is not blinking.	If this LED does not blink when you are attempting to send data over the WiFi link, log in to the router menu using the Ethernet LAN connection, and check your router's wireless (WiFi) configuration.
LAN Ports 	LAN Ports LED is off.	If this LED does not light when an Ethernet connection is made, check the following: - Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation. - Make sure that power is turned on to the connected hub or workstation.
WAN Port 	WAN Port LED is off.	If this LED does not light when an Ethernet connection is made using the Ethernet connection option, check the following: - Make sure that the Ethernet cable connections are secure at the router and at the modem. - Make sure that power is turned on to the modem.
Signal Quality 	Signal Quality LED is off.	If this LED does not light when the mobile broadband connection option is used, check the following: - Check with your ISP to ensure that there is good coverage in the area. - Ensure that your mobile broadband account is active. - Ensure that the SIM card is inserted correctly into the router. - Locate the router near the window or other area of the building. Make sure that one of the Signal Quality LEDs is lit, indicating that there is mobile broadband coverage with the router. - Log in to the router menu and check the Internet configuration. Check that the user name, password, and APN with ISP are set correctly. If you use a PIN to connect to the Internet, make sure it is entered correctly.

Troubleshoot 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.

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 autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router, and reboot your computer.

- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This will set the router's IP address to www.routerlogin.net. This procedure is explained in [Restore the Default Configuration and Password](#) on page 97.
- 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 that 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 management 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.

Troubleshoot the ISP Connection

Check these possible sources of trouble if you are having difficulty connecting to or browsing the Internet.

Connect to the Internet

If unable to connect to Internet, check the following:

1. The Internet account is active.

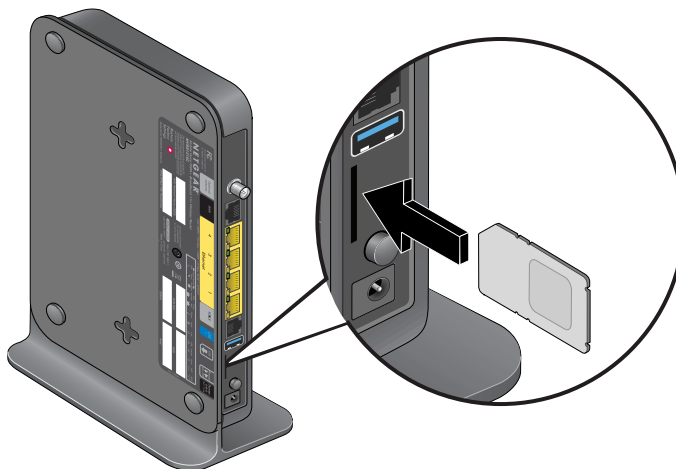
If your ISP has provided you with a SIM card and you have not inserted it into the SIM card slot on the back of the router yet, do so now.

2. Wireless broadband coverage is available where the unit is located.

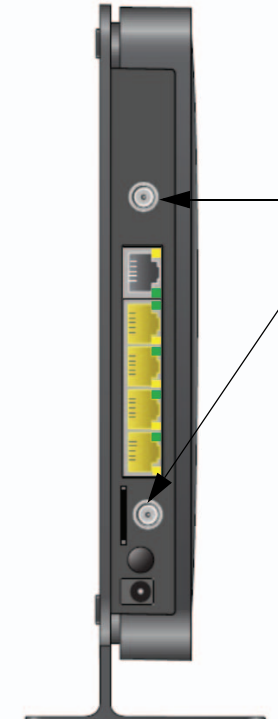
3. Access the router main menu to verify that the broadband settings are correct. Check with your ISP if you are unsure.

4. Check the location of the router.

- a. Move the router closer to a window for better access to the Internet signal. A Signal Quality LED that is off indicates no coverage.
- b. Maintain recommended minimum distances between NETGEAR equipment and household appliances to reduce interference.

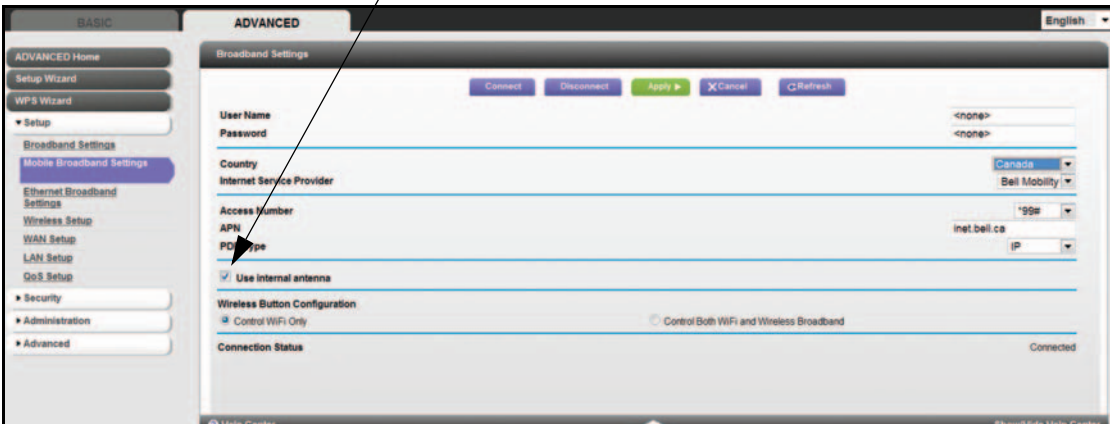


5. Use external antennas for improved signal strength.



Connectors on back panel for optional external antennas

- a. Install external antennas.
(The external antennas are an optional accessory that you can purchase.)
- b. Clear the **Use internal antenna** check box on the Mobile Broadband Settings screen, and then click **Apply**.
- c. Click **Connect** to connect to the Internet.



The screenshot shows the 'ADVANCED' tab of the router's web interface. The 'Mobile Broadband Settings' section is active. It includes fields for User Name, Password, Country (set to Canada), Internet Service Provider (set to Bell Mobility), Access Number, APN (set to inet.bell.ca), and PDP Type (set to IP). The 'Use internal antenna' checkbox is checked. Below this is the 'Wireless Button Configuration' section with two options: 'Control WiFi Only' (selected) and 'Control Both WiFi and Wireless Broadband'. At the bottom, the 'Connection Status' is shown as 'Connected'. A 'Help Center' link is visible at the bottom left.

Troubleshoot Internet Browsing

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

- The traffic meter is enabled, and the limit might have been reached.

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

- Your computer might not recognize any DNS server addresses.

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

Troubleshoot a TCP/IP Network Using the Ping Utility

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

Test the LAN Path to Your Router

You can ping the router from your computer to verify that the LAN path to your router is set up correctly.

➤ To ping the router from a PC running Windows 95 or later:

1. From the Windows toolbar, click the **Start** button, and select **Run**.
2. In the field provided, type **ping** followed by the IP address of the router, as in this example:
`ping 192.168.0.1`
3. Click **OK**.

You should see a message like this one:

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

If the path is working, you see this message:

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

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

Request timed out

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

- Wrong physical connections
 - Make sure that the LAN Ports LED is on. If the LED is off, follow the instructions in [Connect to the Internet](#) on page 93.
 - Check that the corresponding link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
- Wrong network configuration
 - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer or workstation.
 - Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Test the Path from Your Computer to a Remote Device

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

➤ To test the path:

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 computer has the IP address of your router listed as the default router. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer's Network Control Panel. Verify that the IP address of the router is listed as the default router.
- Make sure that the network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your computer, enter that host name as the account name in the Basic Settings screen.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your computers. Many broadband ISPs restrict access by allowing only traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If this is the case, you need to configure your router to clone or spoof the MAC address from the authorized computer.

Problems with Date and Time

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

- Date shown is January 1, 2000.
Cause: The router has not yet successfully reached a network time server. Check that your Internet access settings are configured correctly. If you have just completed configuring the router, wait at least 5 minutes, and check the date and time again.
- Time is off by one hour.
Cause: The router does not automatically sense daylight saving time. On the E-mail screen, select or clear the **Automatically adjust for Daylight Savings Time** check box.

Restore the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router's admin password to **password** and the IP address to **www.routerlogin.net**. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase feature (see [Erase](#) on page 61).
- Press the **Restore Factory Settings** button on the bottom of the router for 6 seconds.
Use this method for cases when the administration password or IP address is not known.

The factory default settings are shown in [Factory Default Settings](#) on page 99.

Supplemental Information



This appendix provides the following information:

- *Factory Default Settings*
- *Technical Specifications*

Factory Default Settings

Use the Restore Factory Settings button located on the bottom of your router to reset all settings to their original factory default settings. This is called a hard reset. To perform a hard reset, press and hold the **Restore Factory Settings** button for 6 seconds. Your router returnx to the factory configuration settings that are shown in the following table.

Feature		Default Behavior
Router login	User login URL	http://192.168.0.1
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Internet connection	WAN MAC address	Use default address
	WAN MTU size	1500
	Port speed	AutoSense
Local network (LAN)	LAN IP	www.routerlogin.net
	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
	Daylight saving time adjustment	Enabled
Firewall	Inbound communication from the Internet	Disabled (except traffic on port 80, the HTTP port)
	Outbound communication to the Internet)	Enabled (all)
	Source MAC filtering	Disabled

Mobile LTE Broadband 11n Wireless Router MBR1516

Feature (continued)		Default Behavior (continued)
Mobile broadband	Internet service provider	Bell Mobility
	APN	inet.bell.ca
	Access Number	*99#
	PDP type	IP
	User name	None required
WiFi	Wireless communication	Enabled
	SSID name	See label on the bottom of router
	Security	WPA-PSK/WPA2-PSK mixed mode
	Broadcast SSID	Enabled
	Transmission speed	Auto (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.)
	Country/region	Canada
	RF channel	Auto
	Operating mode	Up to 145 Mbps
	Data rate	Best
	Output power	Full
	Access point	Enabled
	Authentication type	Open system
	Wireless Card Access List	All wireless stations allowed

Technical Specifications

Technical Specifications	
Network protocol and standards compatibility	TCP/IP, DHCP
Power adapter	• North America: 120V AC, 60 Hz, input • 12V DC @ 2.5A output
Physical specifications	• Dimensions: 6.8 in. x 5.03 in. x 1.28 in. (173 mm x 128 mm x 33 mm) • Weight: 0.65 lbs without the stand (0.29 kg)
Environmental specifications	• Operating temperature: 0° to 40°C (32° to 104°F) • Operating humidity: 90% maximum relative humidity, noncondensing
Electromagnetic emissions	FCC Part 15 Class B; IC; EN 55 022 (CISPR 22), Class B
Interface specifications	• LAN: 10BASE-T or 100BASE-Tx, RJ-45 • WAN: 10BASE-T or 100BASE-TX, RJ-45
Antenna connection (optional)	• SMA connector

Notification of Compliance



NETGEAR Wireless Routers, Gateways, APs

Regulatory Compliance Information

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

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

FCC Requirements for Operation in the United States

FCC Information to User

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

FCC Guidelines for Human Exposure

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

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

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the Mobile LTE Broadband 11n Wireless Router MBR1516 complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

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

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

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

FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Mobile LTE Broadband 11n Wireless Router MBR1516) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

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

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

Industry Canada

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE: Radiation Exposure Statement:

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

Caution:

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

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

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

Interference Reduction Table

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

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

Index

A

- access
 - remote **85**
 - viewing logs **60**
- access points **71**
- accessing remote computer **74**
- address reservation **43**
- advertisement period **87**
- alerts, emailing **54**
- antenna **12**
- attached devices **26**
- authentication, required by mail server **54**
- automatic firmware checking **64, 65**

B

- back panel **10**
- backing up configuration **61**
- base station, setting up **73**
- blocking
 - inbound traffic **74**
 - keywords **50**
 - services **51**
 - sites **50**
- box contents **7**
- broadband settings **36**

C

- compliance **102**
- configuration file **60, 61**
- configuring
 - DMZ server **39**
 - Dynamic DNS **83**
 - NAT **38**
 - port forwarding **78**
 - port triggering **80**
 - repeater unit **74**
 - user-defined services **51**
- connecting wirelessly **14**
- control buttons **8**
- country setting **33**
- CTS/RTS Threshold **69**

- custom service (port forwarding) **79**

D

- dashboard **19**
- data packets, fragmented **39**
- date and time **97**
- daylight savings time **97**
- default DMZ server **39**
- default factory settings, restoring **61**
- default gateway **59**
- denial of service (DoS) protection **49**
- DHCP server **42, 59**
- DHCP setting **57**
- DMZ server **39**
- DNS servers **75**
- Domain Name Server (DNS) addresses **23, 56, 57**
- Dynamic DNS **82**
- DynDNS.org **82**

E

- email notices **54**
- erasing configuration **61**

F

- factory default settings, restoring **61**
- factory defaults **11, 99**
- firewall settings **49**
- firmware version **56**
- firmware, upgrading **18, 64, 65**
- fragmentation length **69**
- fragmented data packets **39**
- front panel **8, 90**

G

- gateway IP address **23**
- gateway, default **59**
- genie, NETGEAR **16**

H

host name [22](#)
 host, trusted [50](#)

I

inbound traffic, allowing or blocking [74](#)
 installing NETGEAR genie [16](#)
 installing with the Setup Wizard [33](#)
 Internet connection, setting up [22](#)
 Internet Port LED [9](#), [91](#)
 Internet Relay Chat (IRC) [76](#)
 Internet service provider (ISP)
 Internet Setup screen [22](#)
 Internet services, blocking access [51](#)
 interval, poll [58](#)
 IP addresses
 auto-generated [92](#)
 current [56](#), [57](#)
 DHCP [16](#)
 dynamic [82](#)
 reserved [43](#)
 IP subnet mask [56](#), [57](#)

K

keywords [50](#)

L

label, product [11](#)
 LAN setup [41](#)
 language setting [33](#)
 lease, DHCP [59](#)
 LED descriptions [9](#)
 local servers, port forwarding to [78](#)
 logging in [16](#), [18](#)
 logs
 emailing [54](#)
 viewing [60](#)

M

MAC address [96](#)
 mail server, outgoing [54](#)
 maintenance settings [55](#)
 managing router remotely [85](#)
 menus, described [19](#)
 metric value [85](#)
 mobile broadband settings [36](#)
 MTU size [39](#)

multicasting [42](#)

N

NAT (Network Address Translation) [38](#), [39](#), [75](#)
 NETGEAR genie [16](#)
 Network Time Protocol (NTP) [97](#)

O

outgoing mail server [54](#)

P

packets, fragmented [39](#)
 Parental Controls [27](#)
 passphrases, changing [26](#)
 password recovery, admin [62](#)
 password, restoring [97](#)
 poll interval [58](#)
 port filtering [51](#)
 port forwarding [74](#), [77](#), [78](#)
 port numbers [51](#)
 port status [58](#)
 port triggering [74](#), [76](#), [78](#), [80](#)
 ports, LAN and WAN [9](#), [91](#)
 positioning the router [14](#)
 Power LED [9](#), [90](#)
 Preamble mode [69](#)
 preset security
 about [24](#)
 passphrase [26](#)
 primary DNS addresses [23](#)
 prioritizing traffic [44](#)
 Push 'N' Connect [20](#)

Q

QoS (Quality of Service) [44](#)

R

radio, wireless [69](#)
 range of wireless connections [14](#)
 recovering admin password [62](#)
 remote management [85](#)
 repeater units [73](#)
 reserved IP addresses [43](#)
 restoring
 configuration file [61](#)
 default factory settings [11](#), [61](#)

router interface, described **19**
 router status, viewing **56**

S

scheduling keyword and service blocking **53**
 secondary DNS **23**
 security **24, 49**
 security PIN **34**
 sending logs by email **54**
 services, blocking **51**
 Setup Wizard **33**
 signal quality **10, 91**
 SIM card **12**
 sites, blocking **50**
 SMS (Short Message Service), configuring **31**
 SMS LED **9**
 SMTP server **54**
 SSID, described **25**
 static routes **83**
 status LEDs **8, 90**
 status, router, viewing **56**
 subnet mask **56, 57**
 system up time **58**

T

TCP/IP network, troubleshooting **95**
 technical support **2**
 time of day **97**
 time to live, advertisement **87**
 time-out, port triggering **81**
 trademarks **2**
 traffic metering **88**
 traffic, prioritizing **44**
 troubleshooting **89**
 trusted host **50**

U

Universal Plug and Play (UPnP) **86**
 up time, system **58**
 upgrading firmware **18, 64, 65**
 user-defined services **51**

V

viewing
 logs **60**
 router status **56**

W

WAN Port LED **9, 91**
 WAN setup **38**
 WiFi button **9, 91**
 WiFi LED **9**
 Wi-Fi Protected Setup (WPS) **20, 34**
 wireless channel **25**
 wireless connections **14**
 wireless devices, adding to the network **20**
 Wireless Distribution System (WDS) **71, 72**
 wireless mode **25**
 wireless network name (SSID)
 broadcast **25**
 described **25**
 wireless network settings **25**
 wireless radio **69**
 wireless repeating **71, 72**
 base station **73**
 repeater unit **73**
 wireless settings **24**
 SSID broadcast **25**
 WMM (Wi-Fi Multimedia) **44**
 WPS button **9, 20**

© NETGEAR, Inc., 2012. Tous droits réservés.

Aucune partie de cette publication ne peut être reproduite, transmise, transcrite, stockée dans un système d'extraction ou traduite dans une autre langue, sous quelque forme et à quelque fin que ce soit, sans le consentement écrit de NETGEAR, Inc.

Soutien technique

Nous vous remercions d'avoir choisi NETGEAR. Pour enregistrer votre produit, vous procurer les mises à jour les plus récentes ou obtenir un soutien technique en ligne, rendez-vous sur le site <http://support.netgear.com/general/contact/default.aspx>.

Téléphone (Canada et États-Unis seulement) : 1-888-NETGEAR

Téléphone (autres pays) : reportez-vous à la carte d'information sur le soutien technique.

Marques commerciales

NETGEAR, le logo NETGEAR et Connect with Innovation sont des marques de commerce ou des marques déposées de NETGEAR, Inc. ou de ses sociétés affiliées aux États-Unis et dans d'autres pays. Ces informations sont susceptibles d'être modifiées sans préavis. Les autres marques et noms de produits sont des marques de commerce ou des marques déposées de leurs détenteurs respectifs. © NETGEAR, Inc., 2012. Tous droits réservés.

Conditions

Afin d'améliorer la conception, les fonctions opérationnelles ou la fiabilité de l'équipement, NETGEAR se réserve le droit de modifier sans préavis les produits décrits dans ce document. NETGEAR décline toute responsabilité quant aux conséquences de l'utilisation des produits ou des configurations de circuits décrits dans ce document.

Sommaire

Chapitre 1 Configuration matérielle

Déballez votre routeur	113
Caractéristiques matérielles	114
Panneau avant	114
Panneau arrière	116
Étiquette	117
Réinitialisation des paramètres d'usine	117
Insérer la carte SIM	118
Installer des antennes externes en option	118
Placer votre Routeur	120

Chapitre 2 Pour démarrer avec NETGEAR Genie

Préparation de la configuration du Routeur	122
Utilisation des propriétés TCP/IP standard pour DHCP	122
Périphériques sans fil et paramètres de sécurité	122
Types de connexions et d'accès	122
Configuration de NETGEAR Genie	122
Utilisation de NETGEAR Genie après l'installation	124
Mise à niveau du micrologiciel (firmware) du Routeur	124
Tableau de bord du Routeur (écran d'accueil DE BASE)	125
Ajout de périphériques sans fil ou d'ordinateurs à votre réseau	126
Méthode manuelle	126
Méthode WPS (Wi-Fi Protected Setup)	126

Chapitre 3 Paramètres DE BASE de NETGEAR Genie

Configuration Internet	128
Champs de l'écran de configuration Internet	128
Paramètres sans fil	130
Champs de l'écran Paramètres sans fil	131
Changer l'option de sécurité WPA et la phrase d'authentification	132
Dispositifs connectés	132
Contrôles parentaux	133
Message SMS	136
Affichage de messages SMS	136
Envoi de messages SMS	137

Chapitre 4 Écran d'accueil AVANCÉ de NETGEAR Genie

Assistant de configuration	139
Assistant WPS	140
Menu Configuration	141
Paramètres haut débit	142
Paramètres haut débit mobile	142
Paramètres WAN	144
Serveur DMZ par défaut	145
Modification de la taille de la MTU	145
Paramétrage LAN	147
Paramètres de l'écran Paramétrage LAN	148
Utilisation du Routeur comme serveur DHCP	149
Réservation d'adresses	150
Paramétrage QoS (Qualité de service)	151

Chapitre 5 Sécurité

Blocage par mot clef du trafic HTTP	157
Blocage de services (filtrage de port)	158
Calendrier de blocage	160
Notifications d'événements de sécurité par courriel	161

Chapitre 6 Administration

Statut du Routeur	163
Journaux	167
Dispositifs connectés	167
Paramètres de sauvegarde	167
Paramètres de sauvegarde	168
Restaurer les paramètres de configuration	168
Effacer	168
Définition du mot de passe	169
Récupération du mot de passe	169
Diagnostic	170
Mise à niveau du routeur	171
Mise à niveau du module	172

Chapitre 7 Paramètres avancés

Paramètres de carte SIM	175
Messages SMS	175
Paramètres sans fil	176
Répéteur sans fil	178
Fonction Répéteur de réseau sans fil	179
Configurer la station du réseau	180
Configuration d'un répéteur	181

Ouverture de port et déclenchement de port	181
Les bases de l'accès à un ordinateur distant	182
Du port de déclenchement aux ports entrants ouverts	183
Ouverture de port pour permettre des communications d'accueil externes	185
En quoi l'ouverture de port diffère-t-elle du déclenchement de port?	186
Configurer l'ouverture de port pour les serveurs locaux	186
Configurer un déclenchement de port	188
DNS dynamique	191
Routes statiques	192
Gestion à distance	194
Service UPnP	195
Mesure de trafic	196

Chapitre 8 Dépannage

Fonctionnement de base	199
Dépannage de l'accès au menu principal du routeur	201
Dépannage de la connexion au FAI	202
Connexion à Internet	202
Dépannage de la navigation Internet	204
Dépannage d'un réseau TCP/IP à l'aide de l'utilitaire Ping	204
Vérification de la connexion entre le réseau local et votre routeur	204
Vérification de la connexion entre l'ordinateur et un périphérique distant	205
Problèmes de date et d'heure	206
Rétablissement du mot de passe et de la configuration par défaut	206

Annexe A Informations complémentaires

Paramètres par défaut d'usine	208
Caractéristiques techniques	210

Annexe B Avis de conformité

Index

Configuration matérielle

1

Se familiariser avec le routeur

Le Routeur sans fil 11n LTE à haut débit mobile MBR1516 vous propose un moyen facile et sûr de configurer un réseau domestique sans fil avec un accès rapide à l'Internet par l'intermédiaire du réseau sans fil haute vitesse 4G (LTE/HSPA+). Il vous permet de bloquer des applications et contenus Internet dangereux et protège les périphériques (ordinateurs, consoles de jeux, etc.) que vous connectez à votre réseau domestique.

Si vous n'avez pas déjà configuré votre nouveau routeur en utilisant le guide d'installation fourni dans l'emballage, ce chapitre vous guide à travers la configuration matérielle. [Chapitre 3, Paramètres DE BASE de NETGEAR Genie](#), explique comment configurer votre connexion Internet.

Ce chapitre comprend les sections suivantes :

- [Déballez votre routeur](#)
- [Caractéristiques matérielles](#)
- [Insérer la carte SIM](#)
- [Installer des antennes externes en option](#)
- [Placer votre Routeur](#)

Pour plus d'information à propos des sujets traités dans ce manuel, visitez le site web du soutien à l'adresse <http://support.netgear.com/general/contact/default.aspx>.

Déballer votre routeur

Ouvrez la boîte et retirez le routeur, les câbles et le guide d'installation.

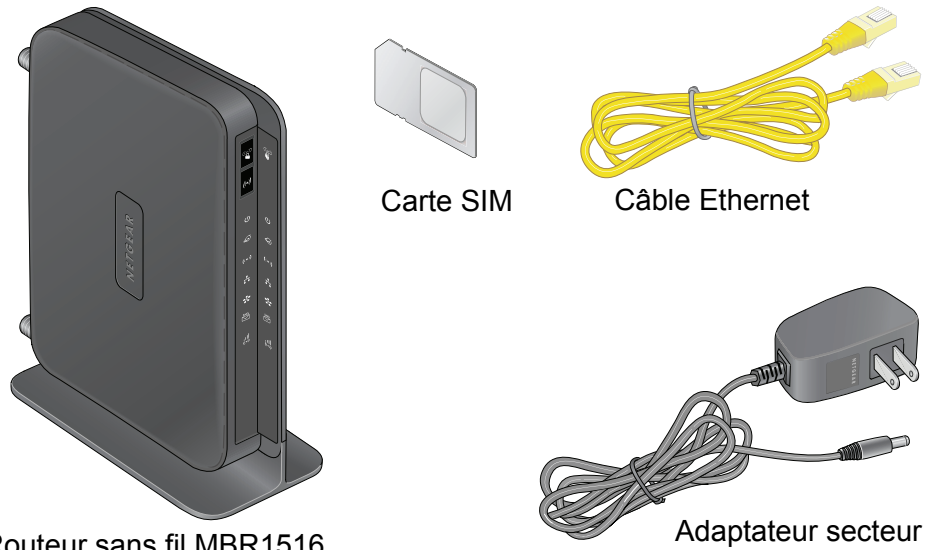


Figure 1. Vérifier le contenu de la boîte

Votre emballage devrait contenir les éléments suivants :

- Routeur sans fil 11n LTE à haut débit mobile MBR1516
- Adaptateur secteur CA (la prise varie selon les régions)
- Câble Ethernet catégorie 5 (Cat 5)
- Guide d'installation et instructions de câblage et de configuration du routeur

Si des pièces sont inadéquates, manquantes ou endommagées, contactez votre fournisseur de services. Conservez le carton et les matériaux d'emballage d'origine, au cas où vous devriez renvoyer le produit pour réparation.

Caractéristiques matérielles

Avant d'installer le câblage sur votre routeur, prenez un moment pour vous familiariser avec l'étiquette et les panneaux avant et arrière. Portez une attention particulière aux voyants sur le panneau avant.

Panneau avant

Le panneau avant du routeur comporte des boutons de commande et des voyants d'état. Les voyants vous permettent de vérifier l'état de l'appareil et les connexions en cours.

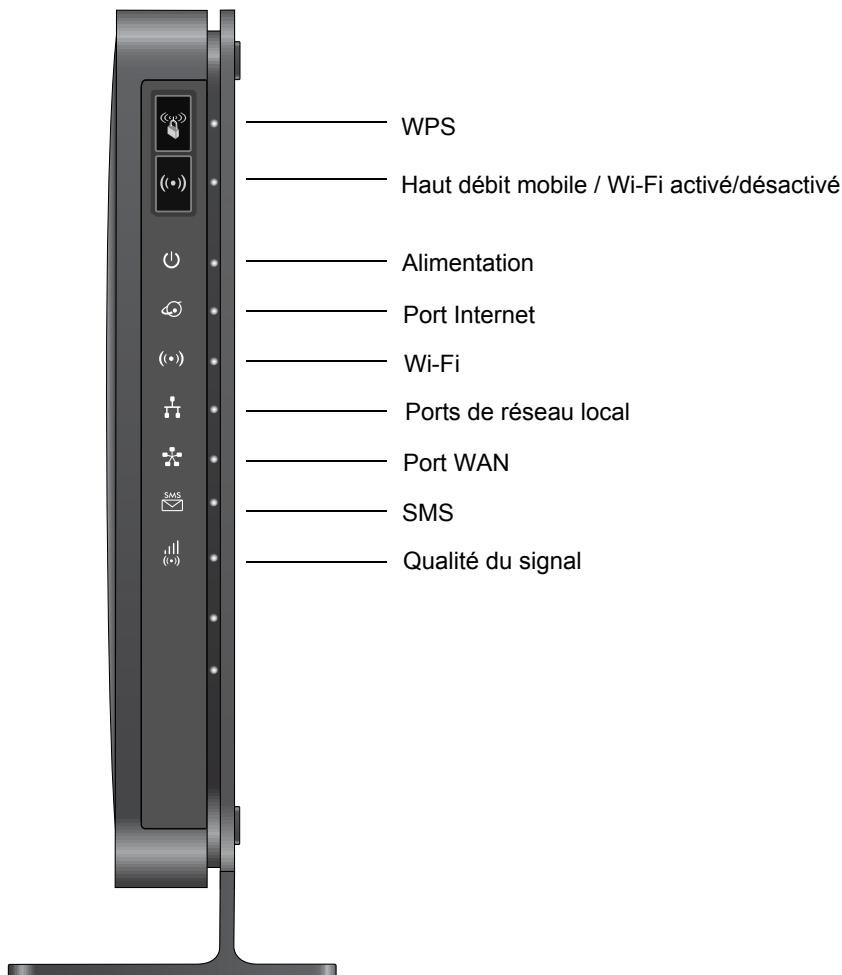


Figure 2. Router, vue avant

Le [Tableau 1](#) présente une description de tous les voyants et boutons situés sur le panneau avant du routeur.

Tableau 1. Description des voyants

Voyant	Activité	Description
WPS 		Appuyez sur le bouton WPS pendant deux minutes pour tenter de connecter le routeur à d'autres périphériques WPS. Pour en savoir plus sur cette fonction, consultez la section Méthode WPS (Wi-Fi Protected Setup) à la page 126.
Bouton marche/arrêt Wi-Fi 		Ce bouton permet de contrôler seulement la liaison radio Wi-Fi ou bien la liaison radio Wi-Fi et la liaison radio haut débit mobile. Utilisez l'interface pour sélectionner les options désirées. Le paramètre par défaut est activé pour la liaison radio Wi-Fi seulement.
Alimentation 	Vert continu	Le routeur est sous tension et fonctionne normalement.
	Orange continu	Le routeur effectue un test d'autodiagnostic.
	Éteint	Le routeur est hors tension.
Port Internet 	Vert continu	Une session Internet est en cours.
	Orange continu	La limite de trafic est atteinte et le trafic est bloqué.
	Vert clignotant	Des données sont transmises par connexion Internet.
	Orange clignotant	La limite de trafic est atteinte, mais le trafic n'est pas bloqué.
	Clignotant vert et orange	Basculement du réseau étendu Ethernet à la connexion haut débit mobile.
	Éteint	Aucune connexion Internet détectée.
Wi-Fi 	Bleu continu	Le port Wi-Fi local est initialisé.
	Bleu clignotant	Des données sont reçues ou transmises par liaison Wi-Fi.
	Éteint	Le point d'accès sans fil est désactivé.
Ports de réseau local 	Vert continu	Des liaisons filaires avec des ordinateurs ont été détectées sur les ports Ethernet locaux.
	Clignotant	Les données sont en cours de transmission ou de réception.
	Éteint	Aucune liaison n'a été détectée sur ces ports.
Port WAN 	Vert continu	Liaison active détectée sur le port Ethernet de réseau étendu.
	Clignotant	Les données sont en cours de transmission ou de réception.
	Éteint	Aucune liaison n'a été détectée sur ces ports.

Tableau 1. Description des voyants (suite)

Voyant	Activité	Description
	Vert continu	Messages SMS en attente.
	Éteint	Aucun message SMS non lu.
	Bleu continu	Une excellente couverture est détectée.
	Vert continu	Une bonne couverture est détectée.
	Orange continu	Une couverture partielle est détectée.
	Éteint	Aucune couverture n'est détectée.

Panneau arrière

Le panneau arrière du routeur comporte des ports de connexion.

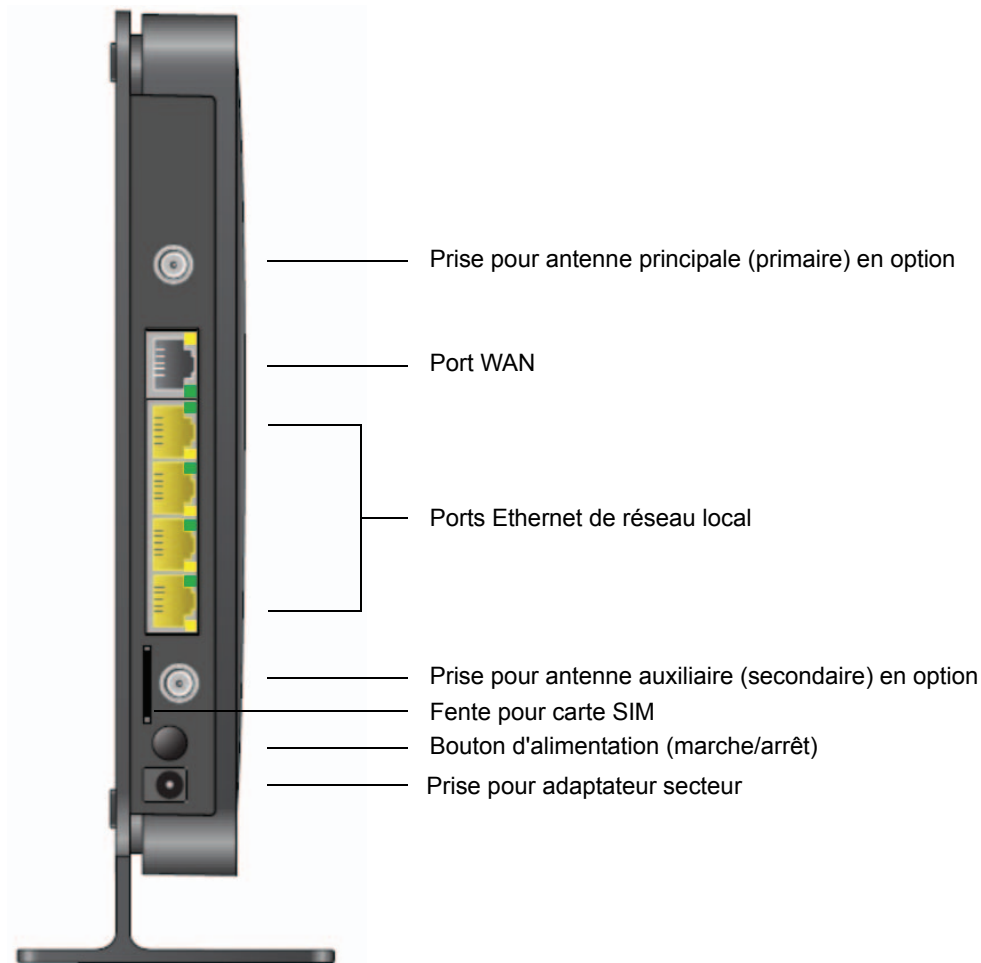


Figure 3. Routeur, vue arrière

Étiquette

L'étiquette située sur le côté du routeur mentionne son adresse MAC, son numéro de série, le code PIN de sécurité, le numéro IMEI ou NSE et les renseignements de connexion par défaut. Cette étiquette comporte également le numéro SSID et la phrase d'authentification qui sont propres à chaque routeur.

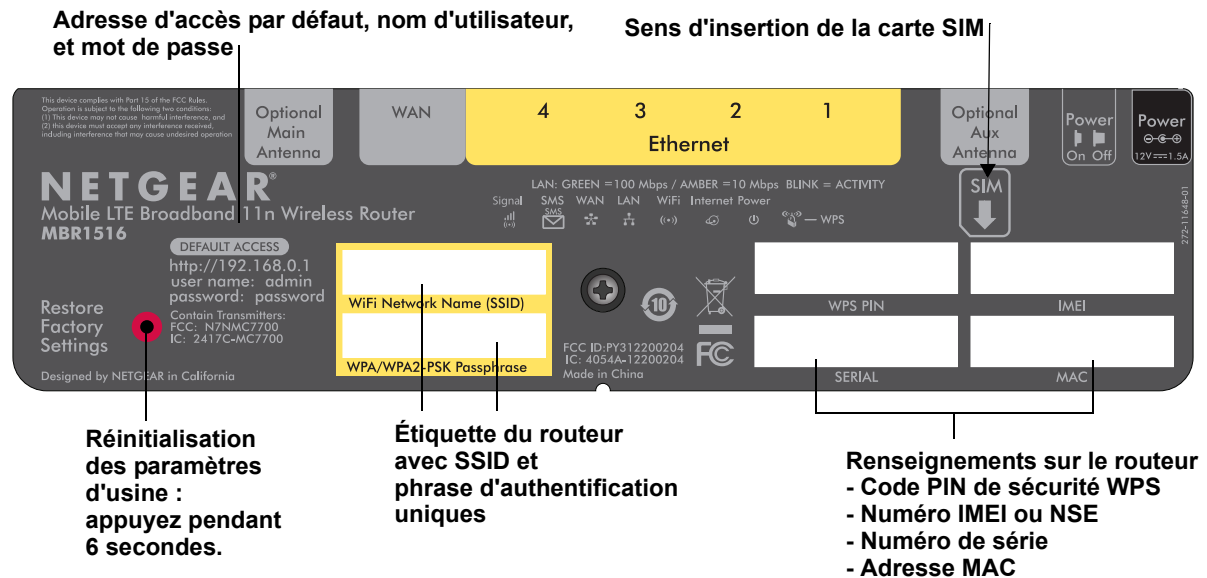


Figure 4. L'étiquette indique des informations uniques se rapportant à votre routeur

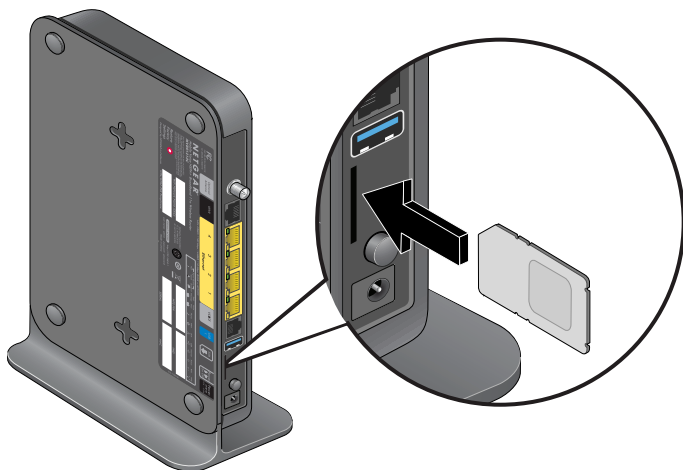
Réinitialisation des paramètres d'usine



Repérez le petit trou cerclé de rouge sur le côté du routeur. Insérez l'extrémité d'un trombone dans le trou et appuyez pendant six secondes. Le fait d'appuyer sur le bouton de réinitialisation des paramètres d'usine fait clignoter brièvement le voyant. Une fois que vous avez enfoncé le bouton pendant plus de six secondes, le voyant d'alimentation clignote en orange, puis il devient vert lorsque le routeur a réinitialisé les paramètres par défaut. Voir [Paramètres par défaut d'usine](#) à la page 208 pour de plus amples informations sur les paramètres par défaut d'usine.

Insérer la carte SIM

Insérez doucement la carte SIM dans la fente pour carte SIM à l'arrière du routeur. Vous devriez entendre un « clic » lorsque la carte SIM est insérée correctement.

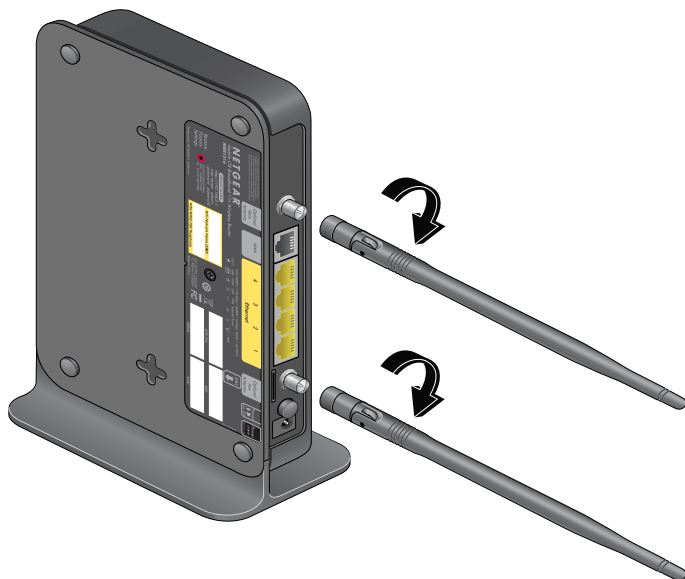


Installer des antennes externes en option

Pour améliorer le rendement, connectez une antenne externe au port de l'antenne principale (primaire). Pour le meilleur rendement du 4G LTE, connectez deux antennes externes pour assurer une diversité.

➤ Pour installer des antennes externes en option :

1. Pour améliorer la puissance du signal, procurez-vous des antennes externes en option et installez-les à l'arrière du routeur.



- Placez les antennes pour qu'elles soient à angle droit l'une par rapport à l'autre.



- Après vous être connecté au routeur (voir la section [Configuration de NETGEAR Genie](#) à la page 122 pour plus d'informations), décochez la case **Utiliser l'antenne interne** dans l'écran Paramètres haut débit et cliquez sur **Appliquer**. Consultez la section [Paramètres haut débit mobile](#) à la page 142 pour obtenir de plus amples informations sur cet écran.

The screenshot shows the 'Paramètres haut débit' (High Speed Settings) page. On the left is a navigation menu with options like 'Accueil AVANCÉ', 'Assistant de configuration', 'Assistant WPS', 'Configuration', 'Paramètres haut débit', 'Paramètres haut débit mobile', 'Paramètres haut débit Ethernet', 'Configuration sans fil', 'Paramètres WAN', 'Paramétrage LAN', 'Paramétrage QoS (Qualité de service)', 'Sécurité', 'Administration', and 'Avancé'. The main area is titled 'Paramètres haut débit' and contains several sections:

- Connecter / Déconnecter / Appliquer / Annuler / Actualiser** buttons at the top.
- Identifiant** and **Mot de passe** fields, both set to '<none>'.
- Pays** dropdown menu set to 'Canada'.
- Fournisseur d'accès Internet** dropdown menu set to 'Bell Mobility'.
- Code PIN** field with four dots.
- Numéro d'accès** dropdown menu set to '*99#'.
- Nom du point d'accès 3G** field set to 'inet.bell.ca'.
- Type de PDP** dropdown menu set to 'IP'.
- Utiliser l'antenne interne** checkbox, which is unchecked.
- Configuration du bouton sans fil** section with two radio buttons: 'Contrôler le Wi-Fi uniquement' (selected) and 'Contrôler le Wi-Fi et le haut débit sans fil'.
- Statut de la connexion** field showing 'Connecté'.
- At the bottom, there is a 'Centre d'aide' link and an 'Afficher/cacher le centre d'aide' button.

Placer votre Routeur

Le routeur permet d'accéder au réseau depuis n'importe où dans le champ de fonctionnement du réseau sans fil. Toutefois, la distance de fonctionnement ou la portée de votre connexion sans fil peut varier considérablement en fonction de l'endroit où se trouve le routeur. Par exemple, l'épaisseur et le nombre de murs que doit traverser le signal sans fil peuvent limiter sa portée.

Utilisez le voyant de qualité du signal sur le panneau avant pour placer le routeur de manière à obtenir la puissance de signal optimale. Également, pour obtenir les meilleurs résultats, placez le routeur :

- À un étage supérieur dans une maison ou un bureau à plusieurs étages.
- Près d'une fenêtre, mais en évitant de l'exposer aux rayons directs du soleil. Un emplacement près d'une fenêtre offre les meilleures conditions pour recevoir un puissant signal 4G.
- Près du centre de la zone de fonctionnement des ordinateurs et autres périphériques, de préférence dans la ligne de mire de vos périphériques sans fil.
- De manière à ce qu'il soit près d'une prise d'adaptateur secteur CA et proche des câbles Ethernet des ordinateurs câblés.
- En hauteur (sur une étagère, par exemple), en limitant au maximum le nombre de murs et de plafonds entre le routeur et les autres périphériques.
- Loin des appareils électriques qui peuvent être source d'interférences, comme les ventilateurs de plafond, les systèmes de sécurité à domicile, les fours micro-ondes, les ordinateurs ou la base d'un téléphone sans fil à 2,4 GHz ou d'un téléphone sans fil.
- Loin des grandes surfaces métalliques, comme une porte en acier ou des plots en aluminium. De grandes étendues de matériaux divers tels que le verre, les murs isothermes, les aquariums, les miroirs, la brique et le béton peuvent également influencer sur le signal sans fil.

Lorsque vous utilisez plusieurs points d'accès, il est préférable que chacun utilise un canal de fréquences radio différent pour réduire les interférences. Le nombre de canaux recommandés entre chaque point d'accès est 5 (par exemple, utilisez les canaux 1 et 6 ou 6 et 11, etc.).

Pour démarrer avec NETGEAR Genie

2

Connexion au routeur

Ce chapitre explique comment utiliser NETGEAR Genie pour configurer votre routeur après avoir terminé le câblage, tel que décrit dans le guide d'installation et dans le chapitre précédent du présent guide.

Ce chapitre comprend les sections suivantes :

- *Préparation de la configuration du Routeur*
- *Types de connexions et d'accès*
- *Configuration de NETGEAR Genie*
- *Utilisation de NETGEAR Genie après l'installation*
- *Mise à niveau du micrologiciel (firmware) du Routeur*
- *Tableau de bord du Routeur (écran d'accueil DE BASE)*
- *Ajout de périphériques sans fil ou d'ordinateurs à votre réseau*

Préparation de la configuration du Routeur

Vous pouvez configurer automatiquement votre routeur au moyen de NETGEAR Genie ou utiliser les menus et écrans de NETGEAR Genie pour une configuration manuelle. Cependant, avant de commencer le processus de configuration, vous devez avoir à proximité les informations sur votre FAI et vous assurer que les ordinateurs portables ou de bureau et autres périphériques du réseau utilisent les paramètres décrits dans le présent chapitre.

Utilisation des propriétés TCP/IP standard pour DHCP

Si vous configurez votre ordinateur afin qu'il utilise une adresse IP statique, vous devez modifier les paramètres de sorte que l'ordinateur utilise le protocole DHCP (Dynamic Host Configuration Protocol).

Périphériques sans fil et paramètres de sécurité

Assurez-vous que votre périphérique sans fil ou ordinateur prend en charge la sécurité sans fil WPA ou WPA2, ce qui correspond au type de sécurité sans fil pris en charge par le routeur.

Types de connexions et d'accès

Il existe divers types de connexions servant à différentes fins. Il est essentiel de connaître les différences entre ces types de connexion, afin de savoir lequel utiliser et quand.

- **La connexion au.** Routeur vous permet de vous connecter à l'interface du routeur depuis NETGEAR Genie. Consultez la section *Utilisation de NETGEAR Genie après l'installation* à la page 124 pour obtenir plus d'information sur ce type de connexion.
- **Clé réseau sans fil ou mot de passe.** Votre routeur comprend un nom de réseau sans fil (SSID) et un mot de passe uniques prédéfinis pour l'accès sans fil. Vous trouverez ces renseignements sur l'étiquette située sous votre routeur.

Configuration de NETGEAR Genie

NETGEAR Genie est compatible avec tout périphérique doté d'un navigateur Web. Il s'agit de la façon la plus simple de configurer le routeur, car il automatise de nombreuses étapes et s'assure de leur bon déroulement. La configuration dure environ 15 minutes.

➤ Pour utiliser NETGEAR Genie afin de configurer votre routeur :

1. Mettez sous tension le routeur en appuyant sur le bouton d'alimentation (**marche/arrêt**), si ce n'est déjà fait.
2. Assurez-vous que votre périphérique est connecté à votre routeur au moyen d'un câble Ethernet ou d'une liaison sans fil (à partir des paramètres de sécurité prédéfinis indiqués sur l'étiquette située sous le routeur).

3. Lancez votre navigateur Web.
 - Si vous configurez la connexion Internet de votre routeur pour la première fois, le navigateur accède automatiquement à l'adresse <http://192.168.0.1>, puis l'écran de NETGEAR Genie s'affiche.
 - Si vous avez déjà utilisé NETGEAR Genie, entrez **<http://192.168.0.1>** dans la barre d'adresse de votre navigateur, afin d'accéder à l'écran de NETGEAR Genie. Consultez la section *Utilisation de NETGEAR Genie après l'installation* à la page 124.
4. Suivez les instructions à l'écran pour effectuer la configuration au moyen de NETGEAR Genie. NETGEAR Genie vous guide lors de la connexion du routeur à Internet.

Si le navigateur ne peut afficher la page Web :

- Assurez-vous que l'ordinateur utilise une connexion sans fil ou qu'il est connecté en réseau local à l'un des quatre ports Ethernet du routeur.
- Assurez-vous que le routeur est prêt à l'emploi. Son voyant d'alimentation devrait s'allumer.
- Fermez et rouvrez le navigateur pour vous assurer qu'il n'a pas mis en cache la page précédente.
- Allez à l'adresse **<http://192.168.0.1>**.
- Si l'ordinateur est configuré de manière à utiliser une adresse IP statique ou fixe (ce qui est rare), modifiez le paramètre pour obtenir automatiquement une adresse IP auprès du routeur.

Si le routeur ne peut se connecter à Internet :

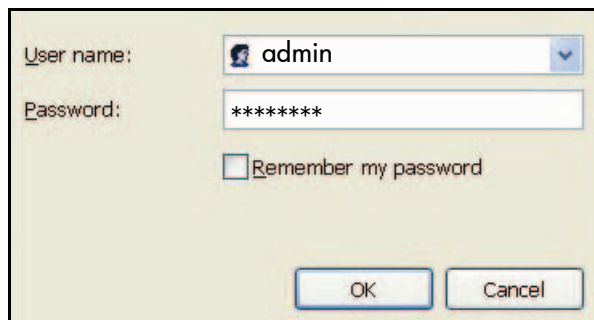
1. Vérifiez vos paramètres et assurez-vous d'avoir sélectionné les bonnes options et que les renseignements entrés sont corrects.
2. Communiquez avec votre FAI afin de confirmer que vous disposez des bonnes données de configuration.
3. Lisez le *Chapitre 8, Dépannage*. Si les problèmes persistent, enregistrez votre produit NETGEAR et communiquez avec le soutien technique de NETGEAR.

Utilisation de NETGEAR Genie après l'installation

Lorsque vous configurez votre routeur pour la première fois, NETGEAR Genie démarre automatiquement au lancement d'un navigateur Web sur un ordinateur connecté au routeur. Vous pouvez utiliser NETGEAR Genie de nouveau si vous désirez consulter ou modifier les paramètres du routeur.

1. Lancez le navigateur depuis un ordinateur ou périphérique sans fil connecté au routeur.
2. Entrez l'adresse **http://192.168.0.1**.

L'écran de connexion s'affiche :



3. Entrez le nom d'utilisateur du routeur (**admin**) et le mot de passe du routeur (**password**), tous deux en minuscules.

Remarque : Le nom d'utilisateur et le mot de passe du routeur ne sont pas les mêmes que ceux utilisés pour vous connecter à Internet. Consultez la section [Types de connexions et d'accès](#) à la page 122 pour obtenir plus d'information.

Mise à niveau du micrologiciel (firmware) du Routeur

Lorsque vous configurez votre routeur et que vous êtes connecté à Internet, le routeur vérifie automatiquement si une nouvelle version du micrologiciel (firmware) est disponible. Le cas échéant, un message s'affiche dans le haut de l'écran. Consultez la section [Mise à niveau du routeur](#) à la page 171 pour obtenir plus d'information sur la mise à jour du micrologiciel (firmware).

Cliquez sur le message lorsqu'il apparaît puis sur **Oui** pour mettre à niveau le routeur au moyen du plus récent micrologiciel (firmware). Une fois la mise à niveau terminée, le routeur redémarrera.



ATTENTION:

N'essayez pas de vous connecter à Internet, d'éteindre le routeur ou l'ordinateur ou d'utiliser autrement le routeur, jusqu'à ce que le routeur ait fini de redémarrer et que le voyant d'alimentation ait cessé de clignoter depuis plusieurs secondes.

Tableau de bord du Routeur (écran d'accueil DE BASE)

L'écran d'accueil DE BASE du routeur est doté d'un tableau de bord qui vous permet de consulter l'état de votre connexion Internet et de votre réseau en un coup d'œil. Vous pouvez cliquer sur une des cinq sections du tableau de bord pour accéder à des informations détaillées. La colonne à gauche contient des menus et vous trouverez dans le haut l'onglet AVANCÉ, qui vous permet d'accéder à des menus et écrans supplémentaires.

Menus (Cliquer sur l'onglet AVANCÉ pour accéder à d'autres menus)

Langue



Tableau de bord (Cliquer pour accéder à un affichage détaillé)

Aide

Figure 5. Écran d'accueil DE BASE du Routeur, avec tableau de bord, sélection de la langue et aide en ligne

- **Accueil.** Cet écran du tableau de bord s'affiche lorsque vous vous connectez au routeur.
- **Internet.** Configurez, mettez à jour et vérifiez les paramètres du FAI pour votre routeur.
- **Sans-fil.** Consultez ou modifiez les paramètres sans fil de votre routeur.
- **Dispositifs connectés.** Consultez les dispositifs connectés à votre réseau.
- **Contrôles parentaux.** Téléchargez et définissez des contrôles parentaux afin d'empêcher le chargement de contenu inapproprié sur votre ordinateur.
- **Message SMS.** Envoyez et recevez des messages SMS.
- **Onglet AVANCÉ.** Configurez le routeur pour des situations uniques, par exemple lorsqu'un accès distant par adresse IP ou nom de domaine Internet est requis. Consultez la section [Chapitre 7, Paramètres avancés](#). L'utilisation de cet onglet requiert une bonne compréhension des concepts du réseautage.

- **Aide et soutien.** Accédez au site de soutien de NETGEAR pour obtenir de l'information, de l'aide et de la documentation sur votre produit. Ces liens fonctionneront une fois votre connexion Internet établie.

Ajout de périphériques sans fil ou d'ordinateurs à votre réseau

Choisissez la méthode manuelle ou WPS pour ajouter des périphériques sans fil et autres appareils à votre réseau sans fil.

Méthode manuelle

➤ **Pour vous connecter manuellement :**

1. Lancez le logiciel qui gère vos connexions sans fil sur le périphérique sans fil (ordinateur portable, console de jeu, iPhone) que vous voulez connecter à votre routeur. Ce logiciel recherche tous les réseaux sans fil de votre secteur.
2. Recherchez votre réseau et sélectionnez-le. Si vous n'avez pas modifié le nom de votre réseau pendant le processus de configuration, recherchez le nom par défaut du réseau Wi-Fi (SSID) et sélectionnez-le. Le SSID par défaut est indiqué sur l'étiquette du produit, située sous le routeur.
3. Entrez le mot de passe du routeur et cliquez sur **Connexion**. La phrase d'authentification par défaut du routeur est indiquée sur l'étiquette du produit, située sous le routeur.
4. Répétez les étapes 1 à 3 pour ajouter d'autres périphériques sans fil.

Méthode WPS (Wi-Fi Protected Setup)

La norme WPS (Wi-Fi Protected Setup) permet d'ajouter facilement des ordinateurs et autres périphériques à un réseau domestique tout en conservant la sécurité. Pour utiliser la méthode WPS, assurez-vous que tous les périphériques sans fil connectés au réseau sont certifiés Wi-Fi et qu'ils prennent en charge la norme WPS. Lors du processus de connexion, le client obtient les paramètres de sécurité du routeur, de sorte que tous les périphériques du réseau utilisent les mêmes.

➤ **Pour utiliser la méthode WPS afin d'établir une connexion au réseau sans fil :**

Si votre périphérique sans fil prend en charge la norme WPS (fonctionnalité « Appuyez : vous êtes connecté »), suivez les étapes suivantes :

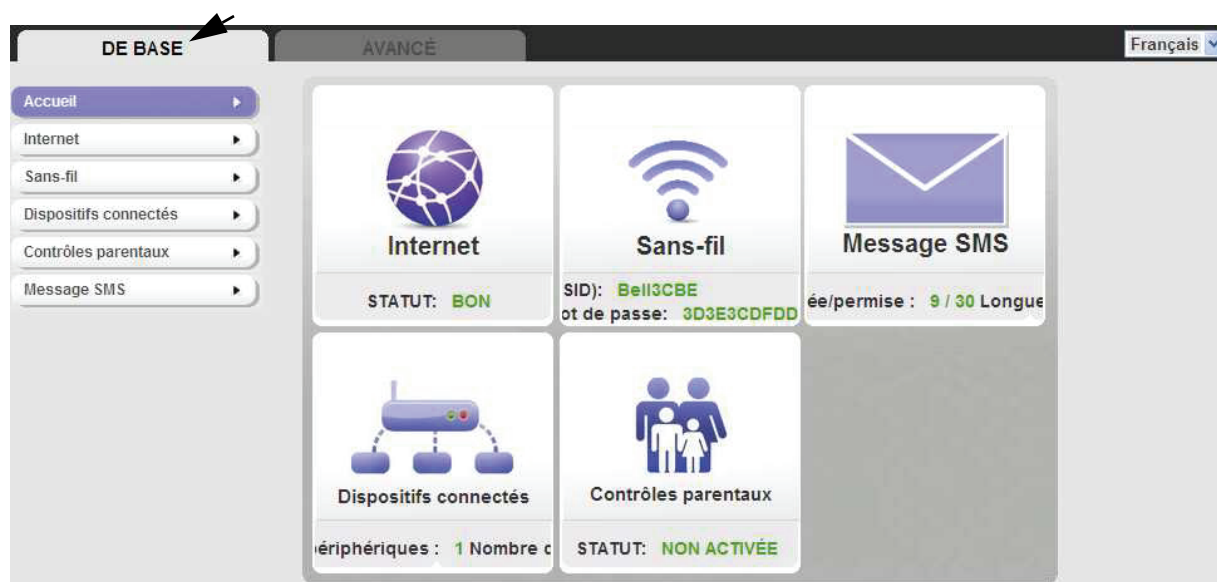
1. Appuyez sur le bouton **WPS** sur le panneau avant du routeur.
2. Dans un délai de deux minutes, appuyez sur le bouton **WPS** sur votre périphérique sans fil ou suivez les instructions de l'utilitaire WPS incluses avec votre appareil. Le périphérique est maintenant connecté à votre routeur.
3. Répétez les étapes 1 et 2 pour ajouter d'autres périphériques sans fil compatibles WPS.

Paramètres DE BASE de NETGEAR Genie

3

Votre connexion Internet et votre réseau

Ce chapitre explique les fonctionnalités disponibles depuis l'écran d'accueil DE BASE de NETGEAR Genie, tel qu'illustré dans la figure suivante :



Ce chapitre comprend les sections suivantes :

- [Configuration Internet](#)
- [Paramètres sans fil](#)
- [Dispositifs connectés](#)
- [Contrôles parentaux](#)
- [Message SMS](#)

Configuration Internet

L'écran de configuration Internet est l'endroit où vous pouvez afficher ou modifier les informations sur le FAI.

1. Depuis l'écran d'accueil, sélectionnez **Internet**. L'écran suivant s'affiche :

Les champs qui s'affichent dans l'écran de configuration Internet sont fonction de votre connexion Internet, laquelle requiert ou non un identifiant.

- **Oui.** Sélectionnez la méthode d'encapsulation et entrez le nom d'utilisateur. Si vous voulez changer le délai de déconnexion, entrez une nouvelle valeur en minutes.
 - **Non.** Entrez le nom de compte et le nom de domaine, seulement si nécessaire.
2. Entrez les paramètres de l'adresse IP et du serveur DNS. Les paramètres par défaut fonctionnent habituellement très bien. Si vous avez de la difficulté à vous connecter, vérifiez les paramètres du FAI.
 3. Cliquez sur **Appliquer** pour enregistrer vos paramètres.
 4. Cliquez sur **Test** pour vérifier votre connexion Internet. Si le site Web de NETGEAR ne s'affiche pas en moins de 1 minute, voir le [Chapitre 8, Dépannage](#).

Champs de l'écran de configuration Internet

Les descriptions suivantes expliquent tous les champs possibles dans l'écran de configuration Internet. Notez que les champs s'affichent dans l'écran selon qu'un identifiant du FAI est requis ou non.

Votre FAI requiert-il un identifiant? Répondez par oui ou par non.

Les champs suivants s'affichent lorsqu'aucun identifiant n'est requis :

- **Nom de compte (si requis).** Entrez le nom de compte fourni par votre FAI. Il peut également être appelé nom d'hôte.

- **Nom de domaine (si requis).** Entrez le nom de domaine fourni par votre FAI.

Ces champs s'affichent lorsque votre FAI requiert un identifiant :

- **Encapsulation du fournisseur d'accès Internet.** Types de FAI. Les choix sont PPPoE, PPTP ou L2TP.
- **Identifiant.** Le nom d'utilisateur fourni par votre FAI. Il s'agit souvent d'une adresse de courriel.
- **Mot de passe.** Le mot de passe que vous utilisez pour vous connecter à votre FAI.
- **Temps d'inactivité (en minutes).** Si vous voulez changer le délai de déconnexion, entrez une nouvelle valeur en minutes. Cela détermine le temps que le routeur maintient la connexion Internet active lorsqu'il n'y a pas d'activité Internet depuis le réseau local. La valeur 0 (zéro) signifie « ne jamais déconnecter ».

Adresse IP Internet.

- **Fournie automatiquement par le FAI.** Votre FAI utilise le protocole DHCP pour attribuer votre adresse IP. Votre FAI attribue automatiquement ces adresses.
- **Utiliser une adresse IP statique.** Entrez l'adresse IP, le masque de sous-réseau IP et l'adresse IP de la passerelle que votre FAI vous a attribuée. La passerelle est le routeur de votre FAI auquel votre routeur se connectera.

Adresse du serveur de nom de domaine (DNS). Le serveur DNS est utilisé pour rechercher des adresses de sites à partir de leur nom.

- **Fournie automatiquement par le FAI.** Votre FAI utilise le protocole DHCP pour attribuer vos serveurs DNS. Votre FAI vous attribue automatiquement cette adresse.
- **Utiliser ces serveurs DNS.** Si vous savez que votre FAI ne transmet pas automatiquement les adresses DNS au routeur durant la connexion, sélectionnez cette option et entrez l'adresse IP du serveur DNS principal de votre FAI. Si une adresse de serveur DNS secondaire est disponible, entrez-la également.

Routeur (adresse MAC). L'adresse MAC Ethernet utilisé par le routeur sur le port Internet. Certains fournisseurs d'accès Internet enregistrent l'adresse MAC de la carte d'interface réseau sur votre ordinateur lorsque votre compte est ouvert pour la première fois. Ils n'acceptent ensuite le trafic qu'à partir de l'adresse MAC de cet ordinateur. Cette fonction permet à votre routeur d'utiliser l'adresse MAC de votre ordinateur (cette procédure est également appelée clonage).

- **Utiliser l'adresse par défaut.** Utiliser l'adresse MAC par défaut.
- **Utiliser une adresse MAC de l'ordinateur.** Le routeur saisira et utilisera l'adresse MAC de l'ordinateur que vous utilisez actuellement. Vous devez utiliser l'ordinateur qui est autorisé par le FAI.
- **Utiliser cette adresse MAC.** Saisissez l'adresse MAC que vous souhaitez utiliser.

Paramètres sans fil

L'écran des paramètres du réseau sans fil vous permet d'afficher ou de configurer le réseau sans fil.

Le Routeur sans fil 11n LTE à haut débit mobile est doté de la sécurité prédéfinie. Cela signifie que le nom du réseau Wi-Fi (SSID), la clé réseau (mot de passe) et l'option de sécurité (protocole de chiffrement) sont prédéfinis en usine. Vous trouverez le SSID et le mot de passe prédéfinis sous l'unité.

Remarque : Le SSID et le mot de passe prédéfinis sont générés de manière unique pour chaque appareil, afin de protéger votre réseau sans fil et d'en optimiser la sécurité.

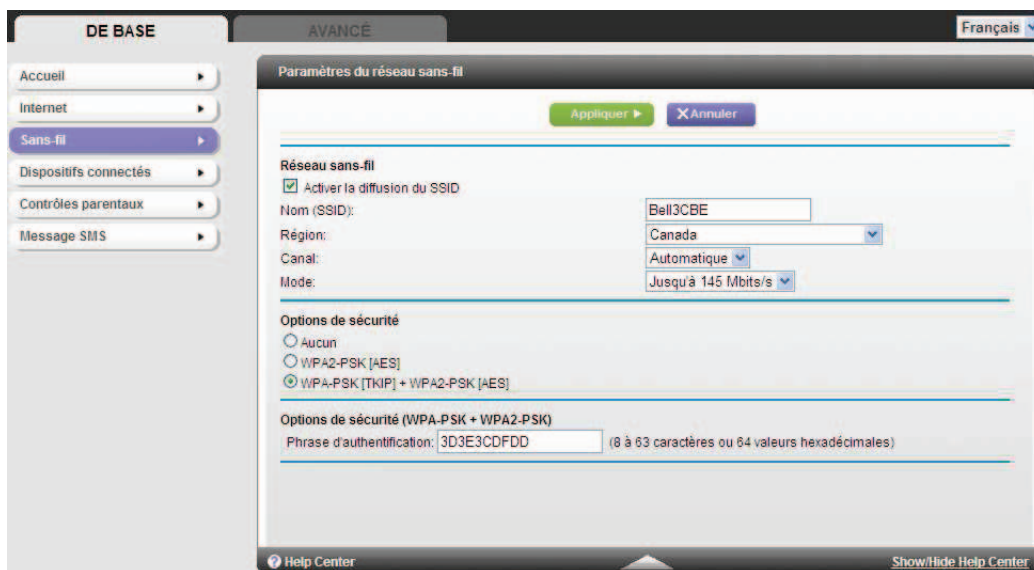
➤ Pour afficher ou modifier les paramètres sans fil de base :

NETGEAR vous recommande de ne pas modifier les paramètres sans fil de base.

Si vous décidez de les modifier, prenez note des nouveaux paramètres et conservez ces renseignements dans un lieu sûr, où vous pourrez les retrouver facilement.

Si vous utilisez un ordinateur connecté par liaison sans fil pour modifier le nom du réseau sans fil (SSID) ou d'autres paramètres de sécurité sans fil, vous serez déconnecté lorsque vous cliquerez sur Appliquer. Pour éviter que cela ne se produise, utilisez un ordinateur doté d'une connexion câblée pour accéder au routeur.

1. Sur l'écran d'accueil DE BASE, sélectionnez **Sans fil** pour afficher l'écran Paramètres sans fil.



Les parties de l'écran, les paramètres et les procédures sont expliquées dans les sections suivantes.

2. Apportez toutes les modifications nécessaires, puis cliquez sur **Appliquer** pour enregistrer vos paramètres.
3. Configurez et vérifiez vos périphériques et ordinateurs sans fil afin de vous assurer qu'ils peuvent se connecter sans fil. S'ils ne le font pas, vérifiez les points suivants :
 - Votre périphérique ou votre ordinateur sans fil est-il connecté à votre réseau ou à un autre réseau sans fil dans votre région? Certains périphériques sans fil se connectent automatiquement au premier réseau ouvert (sans la sécurité sans fil) qu'ils découvrent.
 - Votre périphérique ou votre ordinateur sans fil apparaît-il sur l'écran des dispositifs connectés? S'il apparaît, il est connecté au réseau.
 - Si vous n'êtes pas sûr du nom du réseau (SSID) ou du mot de passe, regardez sur l'étiquette en bas de votre routeur.

Champs de l'écran Paramètres sans fil

Réseau sans fil

La notation b/g/n et a/n fait références aux normes de conformité 802.11. Par exemple, la notation 2,4 b/g/n est conforme aux normes 802.11b, 802.11g et 802.11n à 2,4 GHz de fréquence radio.

Activer la diffusion du SSID. Ce paramètre permet au routeur de diffuser son SSID afin que les stations sans fil puissent voir ce nom sans fil (SSID) dans leurs listes de réseaux numérisées. Cette case est cochée par défaut. Pour désactiver la diffusion du SSID, décochez la case **Activer la diffusion du SSID**, puis cliquez sur **Appliquer**.

Nom (SSID). Le SSID est aussi appelé « nom de réseau sans fil ». Entrez un nom contenant un maximum de 32 caractères dans ce champ. Ce champ fait la distinction entre les majuscules et les minuscules. Le SSID par défaut est généré de manière aléatoire, et **NETGEAR conseille fortement de ne pas modifier ce paramètre**.

Sélection de la région. Emplacement où le routeur est utilisé. Choisissez parmi les pays de la liste. Notez que, aux États-Unis, la région est réglée à États-Unis et n'est pas modifiable.

Canal. Ce paramètre est le canal sans fil utilisé par la passerelle. Entrez une valeur comprise entre 1 et 13. (Pour les produits du marché nord-américain, seuls les canaux 1 à 11 peuvent être utilisés.) Ne changez pas de canal, sauf s'il y a des interférences (que vous pouvez constater par des pertes de connexions ou des transferts de données ralentis). Si cela se produit, essayez avec différents canaux pour voir lequel est le meilleur.

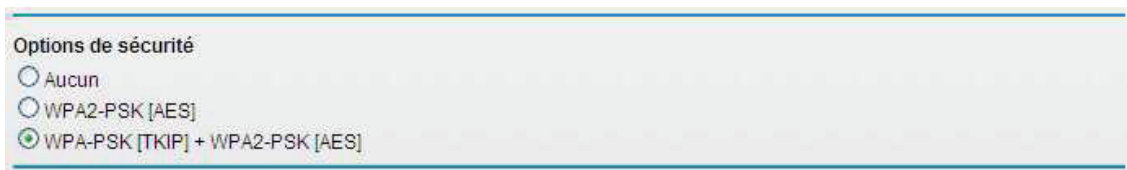
Mode. Jusqu'à 217 Mbits/s est la valeur par défaut et permet aux périphériques sans fil 802.11n et 802.11g de joindre le réseau. Les notations g et b prennent en charge jusqu'à 54 Mbits/s. Le réglage à 450 Mbits/s permet aux périphériques 802.11n de se connecter à cette vitesse.

Options de sécurité

La section Options de sécurité de l'écran Paramètres du réseau sans fil vous permet de modifier les options de sécurité et le mot de passe. Veuillez noter que **NETGEAR vous recommande de ne pas modifier l'option de sécurité ou la phrase d'authentification**, mais si vous souhaitez modifier ces paramètres, la section suivante vous explique comment le faire. **Ne désactivez pas les options de sécurité.**

Changer l'option de sécurité WPA et la phrase d'authentification

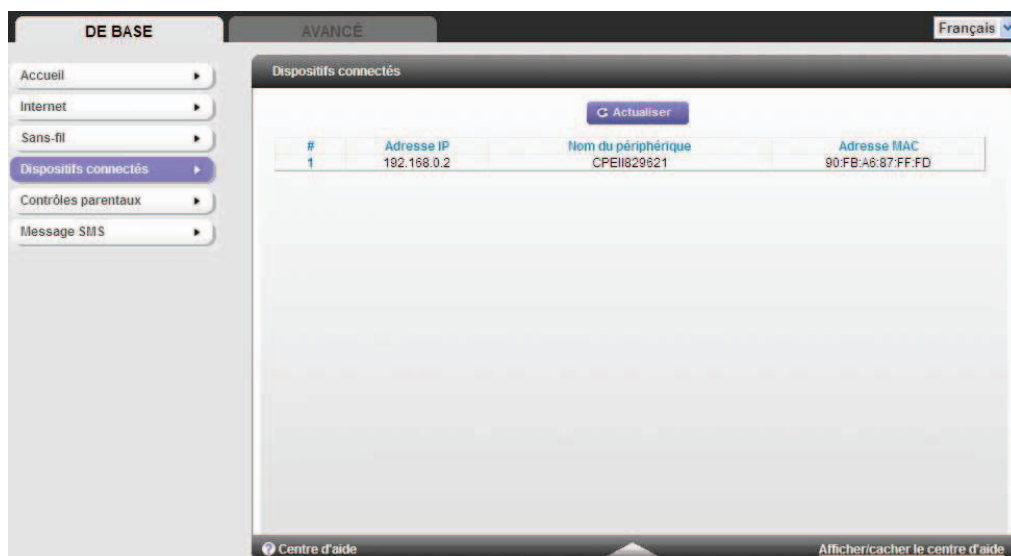
1. Sous Options de sécurité, sélectionnez l'option WPA que vous voulez.



2. Dans le champ Phrase d'authentification qui s'affiche lorsque vous sélectionnez une option de sécurité WPA, entrez la clé réseau (mot de passe) que vous souhaitez utiliser. Il s'agit d'une chaîne de texte de 8 à 63 caractères.

Dispositifs connectés

Vous pouvez afficher ici tous les ordinateurs ou les périphériques qui sont actuellement connectés à votre réseau. Depuis l'écran d'accueil DE BASE, sélectionnez **Dispositifs connectés** pour afficher l'écran suivant :



Les périphériques câblés sont reliés au routeur par des câbles Ethernet. Les périphériques sans fil ont joint le réseau sans fil.

- **# (numéro).** L'ordre dans lequel le périphérique a joint le réseau.
- **Adresse IP.** L'adresse IP que le routeur a attribué à ce périphérique lorsqu'il a joint le réseau. Notez que ce numéro peut changer si un périphérique est désactivé et joint le réseau de nouveau.
- **Nom du périphérique.** Si le nom du périphérique est connu, il est indiqué ici.
- **Adresse MAC.** L'adresse MAC unique pour chaque périphérique ne change pas. L'adresse MAC est généralement indiquée sur l'étiquette du produit.

Vous pouvez cliquer sur **Actualiser** pour mettre à jour cet écran.

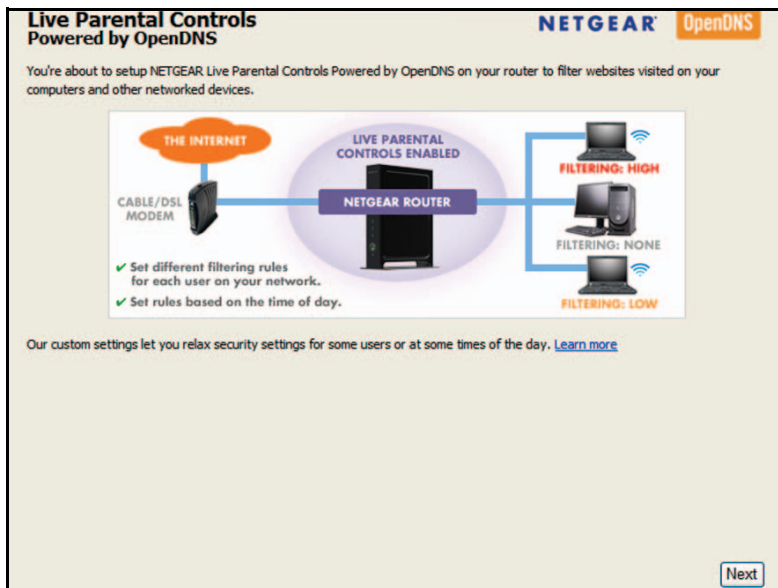
Contrôles parentaux

La première fois que vous sélectionnez Contrôles parentaux à partir de l'écran d'accueil DE BASE, vous êtes automatiquement dirigé vers l'Internet, où vous pouvez en apprendre davantage sur le logiciel Live Parental Controls ou télécharger l'application. L'écran suivant s'affiche :

➤ Pour configurer les contrôles parentaux :

1. Sélectionnez **Contrôle parentaux** sur l'écran du tableau de bord.
2. Cliquez sur le bouton **Utilisateurs Windows** ou **Utilisateurs MAC**.
3. Suivez les instructions à l'écran pour télécharger et installer l'utilitaire de gestion Live Parental Controls de NETGEAR.

Après l'installation, le logiciel Live Parental Controls démarre automatiquement.



4. Cliquez sur **Suivant**, lisez la note, puis cliquez à nouveau sur **Suivant** pour continuer.

Parce que le logiciel Live Parental Controls utilise gratuitement des comptes d'OpenDNS, vous êtes invité à vous connecter ou à créer un compte gratuit.

Setting up Live Parental Controls

Welcome, this setup wizard will quickly configure NETGEAR Live Parental Controls Powered by OpenDNS on your NETGEAR router.

In order to use Live Parental Controls, you need a free OpenDNS account. Do you already have one?

☒ Yes, use my existing OpenDNS account.
 ☐ No, I need to create a free OpenDNS account.

5. Sélectionnez la case d'option qui s'applique à vous et cliquez sur **Suivant**.
 - Si vous avez déjà un compte OpenDNS, sélectionnez la case d'option **Oui**.
 - Si vous n'avez pas de compte OpenDNS, sélectionnez la case d'option **Non**.

Si vous créez un compte, l'écran suivant s'affiche :

Create a free OpenDNS account

Username

Password

Confirm Password

Email

Confirm Email

- Remplissez les champs et cliquez sur **Suivant**.

Une fois que vous êtes connecté ou que vous avez créé un compte, l'écran affiche le niveau de filtrage :

Live Parental Controls: choose a filtering level for your network

All computers connected to your router will be protected from the content you select below. You can customize your Live Parental Controls later on our website.

☐ **High**
Protects against all adult-related sites, illegal activity, social networking sites, video sharing sites, phishing attacks and general time-wasters.

☐ **Moderate**
Protects against all adult-related sites, illegal activity and phishing attacks.

☐ **Low**
Protects against pornography and phishing attacks.

☒ **Minimal**
Protects only against phishing attacks.

☐ **None**
Nothing blocked.

6. Sélectionnez la case d'option correspondant au niveau de filtrage que vous souhaitez et cliquez sur **Suivant**.

Setup is complete!

You have successfully setup NETGEAR Live Parental Controls Powered by OpenDNS. Next time you run the Management Utility it will take you to the status screen where you can:

- check whether Live Parental Controls are enabled
- disable or enable Live Parental Controls
- modify basic settings
- change custom settings such as per-user and time-of-day based Live Parental Controls

Take me to the status screen

7. Cliquez sur le bouton **Emmène-moi à l'écran Statut**.

Les contrôles parentaux sont maintenant configurés pour le routeur. Le tableau de bord indique que les contrôles parentaux sont activés.

Message SMS

Le Short Message Service (SMS) est un service de messagerie texte pour les systèmes de communication. Les écrans SMS vous permettent d'effectuer les tâches expliquées dans les sections suivantes :

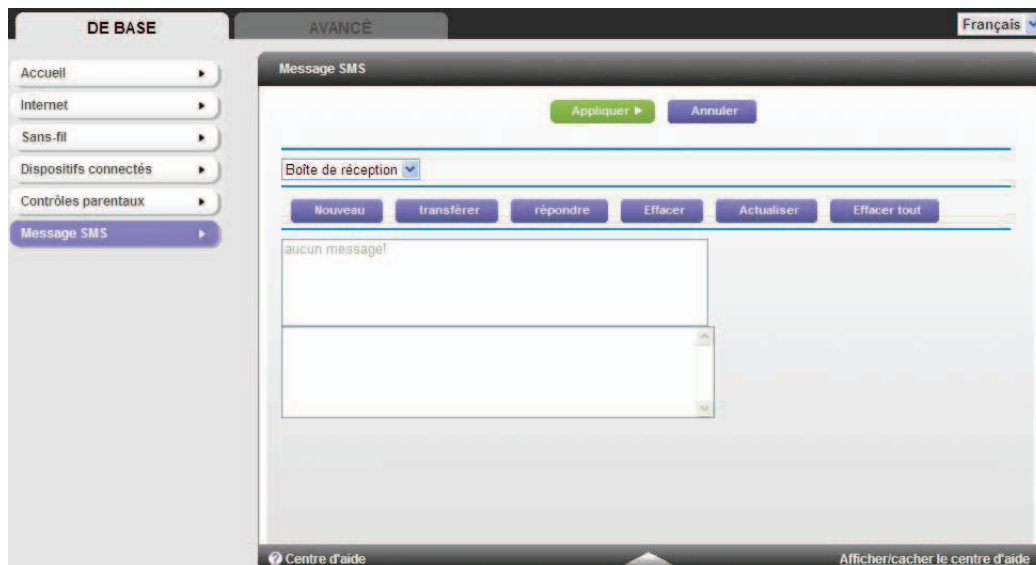
- [Affichage de messages SMS](#)
- [Envoi de messages SMS](#)

Affichage de messages SMS

Des nouveaux messages SMS sont accessibles lorsque le voyant SMS du panneau avant reste allumé en vert.

➤ **Pour afficher les nouveaux messages SMS :**

1. Sélectionnez **DE BASE> Message SMS** pour afficher l'écran suivant :



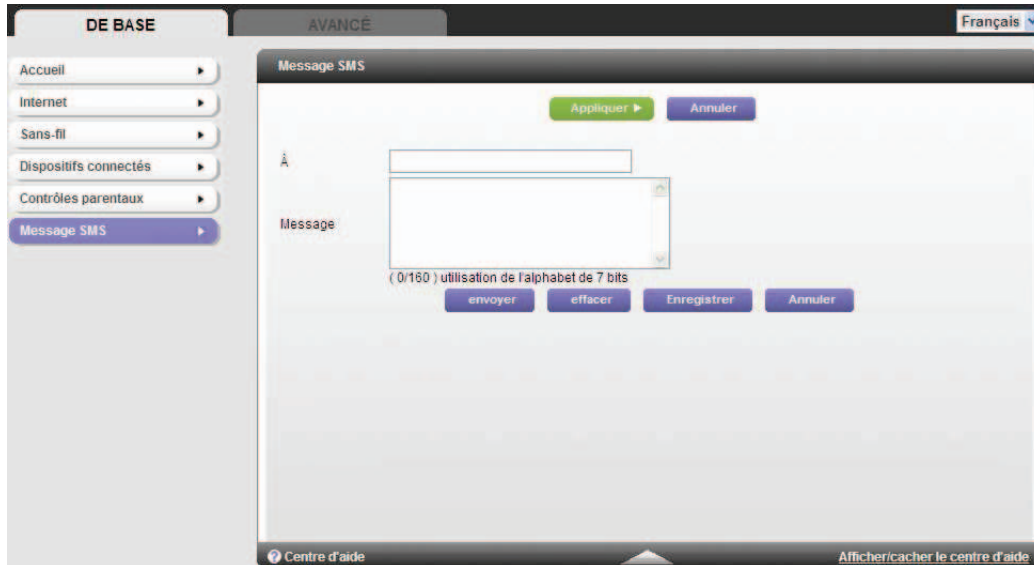
2. Cliquez sur le message que vous souhaitez voir.
 - Cliquez sur **Transférer** ou **Répondre** pour transférer le message spécifié ou y répondre.
 - Cliquez sur **Supprimer** pour supprimer le message SMS spécifié.
3. Sinon, vous pouvez aussi effectuer les opérations suivantes :
 - Cliquez sur **Actualiser** pour réafficher tous les messages SMS se trouvant sur la carte SIM.
 - Cliquez sur **Tout supprimer** pour supprimer tous les messages SMS de la carte SIM.
 - Cliquez sur **Nouveau** pour ouvrir un nouveau message. Consultez la section [Envoi de messages SMS](#) à la page 137 pour obtenir plus d'information.

Envoi de messages SMS

Vous pouvez créer un nouveau message SMS ou envoyer un message SMS par courriel.

➤ **Pour envoyer des messages SMS :**

1. Sélectionnez **DE BASE > Message SMS**, puis cliquez sur **Nouveau** pour afficher l'écran suivant :



2. Dans le champ À, entrez le numéro de téléphone auquel vous souhaitez envoyer le message SMS ou l'adresse de courriel à laquelle vous souhaitez acheminer le message SMS par courriel.

Pour les messages à destinataires multiples, vous pouvez envoyer un message à plusieurs numéros de téléphone. Chaque numéro de téléphone doit être séparé par une virgule (,).

3. Dans le champ Contenu, entre le contenu du message SMS. La longueur du message s'affiche au bas de la boîte.
4. Cliquez sur **Envoyer** pour envoyer le message SMS.

Vous pouvez aussi effectuer l'une des opérations suivantes :

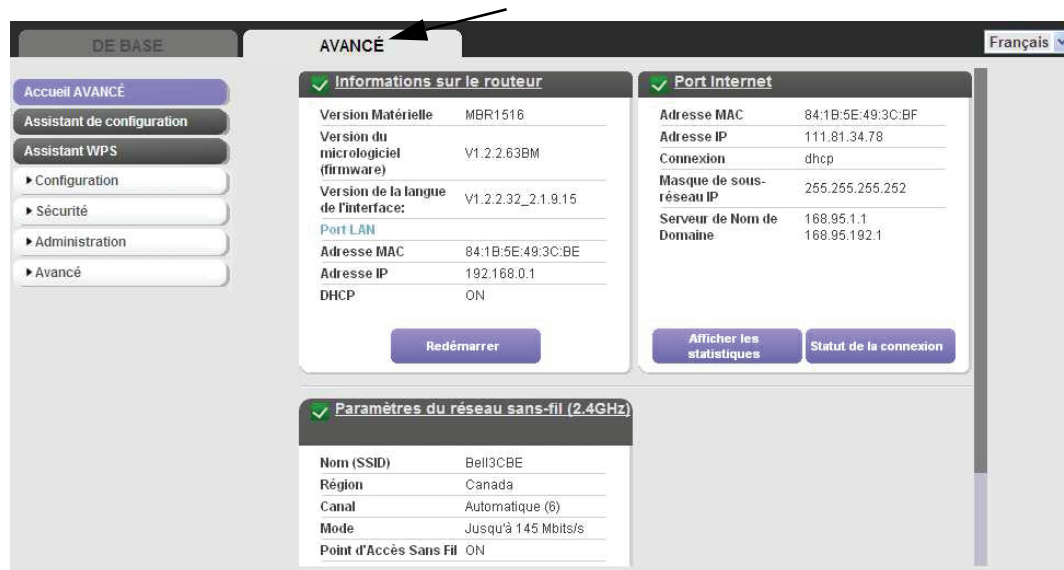
- Cliquez sur **Effacer** pour supprimer l'information contenu dans les champs À et Contenu.
- Cliquez sur **Enregistrer** pour enregistrer un brouillon du message.
- Cliquez sur **Annuler** pour revenir à la boîte de réception sans envoyer le message.

Écran d'accueil AVANCÉ de NETGEAR Genie

4

Spécification des paramètres personnalisés

Ce chapitre explique les fonctionnalités disponibles depuis l'écran d'accueil AVANCÉ de NETGEAR Genie, tel qu'illustré dans la figure suivante :



Ce chapitre comprend les sections suivantes :

- *Assistant de configuration*
- *Assistant WPS*
- *Menu Configuration*
- *Paramètres haut débit*
- *Paramètres haut débit mobile*
- *Paramètres WAN*
- *Paramétrage LAN*
- *Paramétrage QoS (Qualité de service)*

Certaines sélections de l'écran d'accueil AVANCÉ sont décrites dans d'autres chapitres :

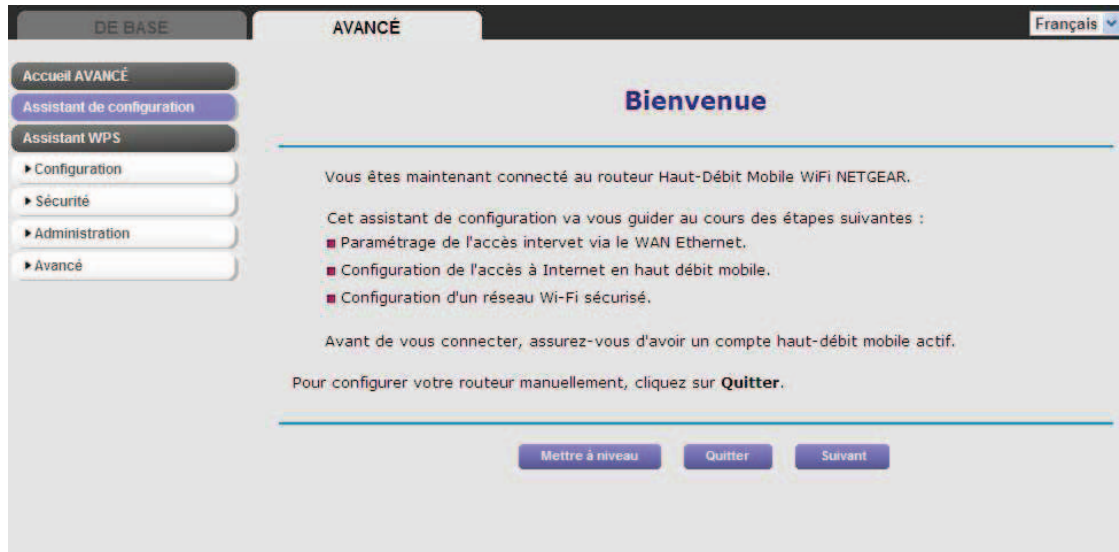
- **Sécurité.** Consultez la section *Chapitre 5, Sécurité*.
- **Administration.** Consultez la section *Chapitre 6, Administration*.
- **Configuration avancée.** Consultez la section *Chapitre 7, Paramètres avancés*.

Assistant de configuration

Le processus d'installation de NETGEAR Genie est lancé la première fois que vous configurez le routeur. Après avoir configuré le routeur pour la première fois, si vous désirez effectuer cette tâche de nouveau, vous pouvez exécuter l'assistant de configuration depuis l'onglet AVANCÉ de NETGEAR Genie.

➤ **Pour exécuter l'assistant de configuration :**

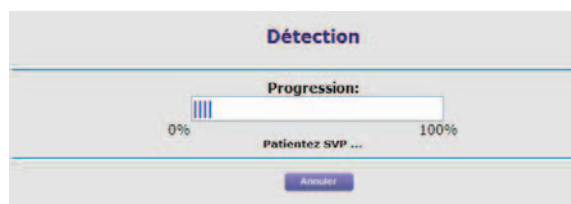
1. Sélectionnez **AVANCÉ** > **Assistant de configuration** pour accéder à l'écran suivant :



2. Cliquez sur **Mettre à niveau** pour mettre à jour le micrologiciel (firmware) (consultez la section [Mise à niveau du routeur](#) à la page 171). Sinon, cliquez sur **Suivant** pour continuer.
3. Sélectionnez les paramètres de connexion haut débit (consultez la section [Paramètres haut débit](#) à la page 142), puis cliquez sur **Suivant**.



Le routeur affiche la barre de progression de la mise à jour.



Remarque : Si vous exécutez l'assistant de configuration à partir d'une connexion Wi-Fi, vous serez déconnecté lorsque le routeur redémarrera.

Assistant WPS

L'assistant WPS vous permet d'ajouter un dispositif client compatible WPS (périphérique sans fil ou ordinateur) à votre réseau. Sur le dispositif client, vous devez appuyer sur le bouton WPS ou rechercher le PIN WPS de l'appareil.

➤ Pour utiliser l'assistant WPS :

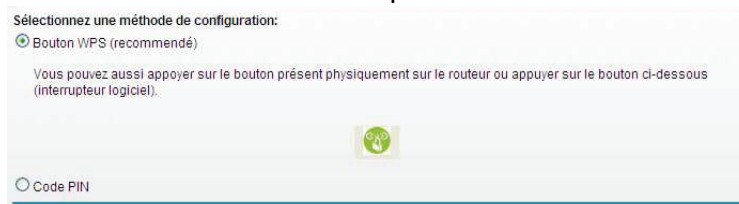
1. Sélectionnez **AVANCÉ > Assistant WPS**.
2. Cliquez sur **Suivant**. L'écran suivant vous permet de sélectionner la méthode qui servira à ajouter le client WPS (périphérique sans fil ou ordinateur).



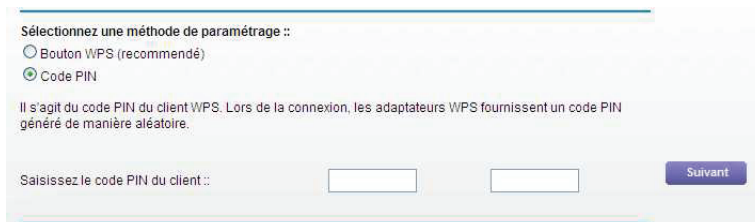
Vous pouvez utiliser soit le bouton-poussoir, soit la méthode PIN.

3. Sélectionnez **Bouton WPS** ou **Code PIN**.

- Pour utiliser la méthode par bouton, cliquez sur le bouton **WPS** de cet écran ou appuyez sur le bouton **WPS** situé sur le côté du routeur. Dans un délai de 2 minutes, allez au client sans fil et appuyez sur son bouton **WPS** pour vous connecter au réseau sans entrer de mot de passe.



- Pour utiliser la méthode PIN, activez le bouton radio **Code PIN**, entrez le PIN de sécurité du client, puis cliquez sur **Suivant**.



Sélectionnez une méthode de paramétrage ::

☐ Bouton WPS (recommandé)

☒ Code PIN

Il s'agit du code PIN du client WPS. Lors de la connexion, les adaptateurs WPS fournissent un code PIN généré de manière aléatoire.

Saisissez le code PIN du client ::

Dans un délai de 2 minutes, allez au dispositif client et utilisez son logiciel WPS pour vous connecter au réseau sans entrer de mot de passe.

Le routeur essaie d'ajouter le périphérique compatible WPS. Le voyant WPS situé à l'avant du routeur clignote en vert. Lorsque le routeur établit une connexion WPS, le voyant est vert continu et l'écran WPS du routeur affiche un message de confirmation.

4. Répétez les étapes 2 et 3 pour ajouter un autre client WPS à votre réseau.

Menu Configuration

Sélectionnez **AVANCÉ > Configuration** pour accéder au menu Configuration. Les options suivantes sont offertes :

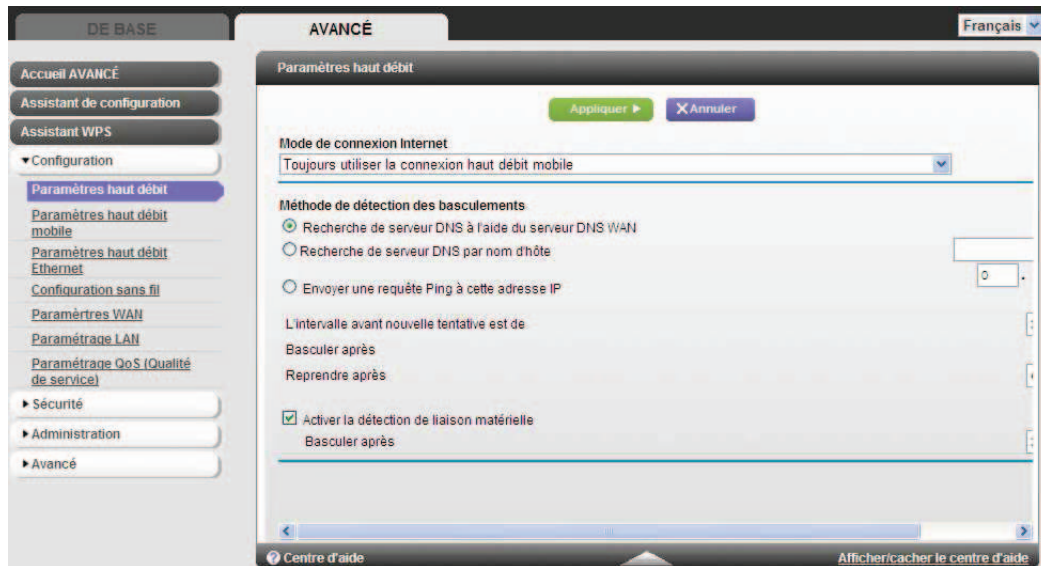
- **Paramètres haut débit.** Permet de configurer le mode de connexion Internet de votre Routeur sans fil 11n LTE à haut débit mobile MBR1516. Consultez la section [Paramètres haut débit](#) à la page 142.
- **Paramètres haut débit mobile.** Permet de configurer l'accès à votre compte haut débit mobile. Consultez la section [Paramètres haut débit mobile](#) à la page 142.
- **Paramètres haut débit Ethernet.** Il s'agit d'un raccourci vers l'écran Configuration Internet, auquel vous pouvez accéder à partir du tableau de bord de l'écran d'accueil DE BASE. Consultez la section [Configuration Internet](#) à la page 128.
- **Configuration sans fil.** Il s'agit d'un raccourci vers l'écran Paramètres sans fil, auquel vous pouvez accéder à partir du tableau de bord de l'écran d'accueil DE BASE. Consultez la section [Paramètres sans fil](#) à la page 130.
- **Paramètres WAN.** Configuration de l'accès Internet (WAN). Consultez la section [Paramètres WAN](#) à la page 144.
- **Paramétrage LAN.** Configuration du réseau local (LAN). Consultez la section [Paramétrage LAN](#) à la page 147.
- **Paramétrage QoS** (Qualité de service). Configuration de la fonction QoS (Qualité de service). Consultez la section [Paramétrage QoS \(Qualité de service\)](#) à la page 151.

Paramètres haut débit

L'écran Paramètres haut débit vous permet de sélectionner le mode de connexion Internet de votre Routeur sans fil 11n LTE à haut débit mobile MBR1516.

➤ **Pour sélectionner votre mode de connexion Internet :**

1. Sélectionnez **AVANCÉ > Configuration > Paramètres haut débit** pour accéder à l'écran suivant :



Voici vos options de connexion Internet :

- Utiliser d'abord la connexion Ethernet puis, en cas d'échec, la connexion haut débit mobile
 - Toujours utiliser la connexion haut débit mobile
 - Toujours utiliser la connexion Ethernet
2. Cliquez sur **Appliquer** pour enregistrer votre sélection.

Paramètres haut débit mobile

L'écran Paramètres haut débit mobile vous permet de configurer l'accès à votre compte haut débit mobile.

Remarque : La connexion au réseau haut débit mobile requiert un compte de services haut débit actif.

➤ Pour configurer l'accès à votre compte haut débit mobile :

1. Sélectionnez **AVANCÉ > Configuration > Paramètres haut débit mobile** pour accéder à l'écran suivant :

Les paramètres suivants sont fournis :

- **Identifiant.** Nom d'utilisateur pour établir une connexion au compte.
 - **Mot de passe.** Mot de passe d'authentification du compte.
 - **Pays.** Pays où est fourni le service haut débit mobile.
 - **Fournisseur d'accès Internet.** Fournisseur d'accès Internet du réseau 4G.
 - **Code PIN.** Code PIN de la carte SIM si le PIN a été activé.
 - **Numéro d'accès.** Numéro de téléphone du site distant.
 - **Nom du point d'accès 3G.** Nom du point d'accès.
 - **Type de PDP.** Type de protocole de transmission de paquets de données.
 - **Utiliser l'antenne interne.** Le Routeur sans fil 11n LTE à haut débit mobile MBR1516 utilise des antennes internes, à moins que vous ne choisissiez d'amplifier la réception du signal au moyen d'antennes externes.
 - **Configuration du bouton sans fil.** Indiquez si vous préférez que le bouton WPS contrôle la connexion Wi-Fi seulement ou les connexions Wi-Fi et haut débit sans fil.
 - **Statut de la connexion.** État actuel du port WAN.
2. Cliquez sur **Appliquer** pour enregistrer vos paramètres.
 3. Cliquez sur **Connecter** pour vous connecter manuellement au réseau.
 4. Cliquez sur **Déconnecter** pour vous déconnecter manuellement du réseau actuel.

Paramètres WAN

L'écran Paramètres WAN vous permet de configurer un serveur DMZ (zone démilitarisée), de modifier la taille maximale des unités de transmission (MTU) et de permettre au routeur de répondre à un ping sur le port WAN (Internet). Sélectionnez **AVANCÉ > Configuration > Paramètres WAN** pour accéder à l'écran suivant :

- **Désactiver la protection DoS et le scan de ports.** La protection DoS protège votre réseau local des attaques par déni de service de types « Syn flood », « Smurf Attack », « Ping of Death », « Teardrop Attack », raz-de-marée UDP, « ARP Attack », usurpation ICMP, balayage nul et bien d'autres encore. Cette fonctionnalité ne devrait être désactivée que dans des circonstances spéciales.
- **Serveur DMZ par défaut.** Cette fonction est parfois utile lorsque vous jouez à certains jeux et que vous utilisez des applications de vidéoconférence en ligne. Soyez prudent lors de l'utilisation de cette fonction, parce qu'elle diminue la sécurité du pare-feu. Consultez la section [Serveur DMZ par défaut](#) à la page 145 pour obtenir plus d'information.
- **Répondre au ping sur le port Internet.** Si vous souhaitez que le routeur réponde à un « ping » provenant d'Internet, cochez cette case. N'utilisez cette fonction que comme outil de diagnostic, puisqu'elle permet de découvrir votre routeur. Ne cochez pas cette case, sauf si vous avez des raisons spécifiques de le faire.
- **Taille de la MTU (en octets).** La valeur habituelle de la MTU (unité de transmission maximale) pour la plupart des réseaux Ethernet est de 1 500 octets ou de 1 492 octets dans le cas des connexions PPPoE. Pour certains FAI, vous devrez peut-être réduire la MTU. Ceci est rarement requis et ne devrait pas être effectué sauf si vous êtes certain qu'il est nécessaire de le faire pour établir une connexion à votre FAI. Consultez la section [Modification de la taille de la MTU](#) à la page 145.
- **Filtrage NAT.** La traduction d'adresses de réseau (NAT) détermine de quelle manière le routeur traite le trafic entrant. L'option NAT sécurisé permet d'obtenir un pare-feu sécurisé afin de protéger les ordinateurs du réseau local contre des attaques provenant d'Internet. Cependant, cette fonctionnalité peut empêcher le bon fonctionnement de certains jeux en ligne, d'applications point à point ou d'applications multimédias. L'option NAT ouvert donne accès à un pare-feu beaucoup moins sécurisé mais permet le fonctionnement de pratiquement toutes les applications Internet.
- **Désactiver le SIP ALG.** Certaines applications VoIP ne fonctionnent pas bien avec le SIP ALG. Si vous cochez cette case afin de désactiver le SIP ALG, vos périphériques VoIP seront davantage en mesure de créer et d'accepter des appels par l'entremise du routeur.

Serveur DMZ par défaut

Le serveur DMZ par défaut est utile lorsque vous jouez à certains jeux et que vous utilisez certaines applications de vidéoconférence en ligne, qui ne sont pas compatibles avec la traduction d'adresses de réseau (NAT). Le routeur est programmé pour reconnaître certaines de ces applications et pour travailler correctement avec celles-ci, mais d'autres applications pourraient ne pas fonctionner correctement. Dans certains cas, un ordinateur local peut exécuter l'application correctement si l'adresse IP de cet ordinateur est entrée comme adresse du serveur DMZ par défaut.



AVERTISSEMENT:

Les serveurs DMZ constituent un risque au niveau de la sécurité. Lorsqu'un ordinateur est désigné comme serveur DMZ par défaut, il perd la protection offerte par le pare-feu et est exposé à des exploits émanant d'Internet. Si sa sécurité est compromise, le serveur DMZ peut attaquer d'autres ordinateurs sur votre réseau.

Le trafic entrant provenant d'Internet est habituellement ignoré par le routeur, sauf si le trafic est une réponse destinée à un ordinateur local ou si vous avez configuré un service dans l'écran Ouverture de port / Déclenchement de port. Plutôt que d'ignorer le trafic, vous pouvez le faire suivre vers un ordinateur du réseau local. Cet ordinateur est appelé le « serveur DMZ par défaut ».

➤ Pour configurer un serveur DMZ par défaut :

1. À l'écran Paramètres WAN, cochez la case **Serveur DMZ par défaut**.
2. Entrez l'adresse IP.
3. Cliquez sur **Appliquer**.

Modification de la taille de la MTU

L'unité de transmission maximale (MTU) correspond au paquet de données le plus volumineux à être transmis par un périphérique réseau. Lorsqu'un périphérique réseau communique avec un autre dispositif réseau par l'entremise d'Internet, les paquets de données voyagent en passant par de nombreux appareils. Si un des dispositifs qui se trouvent sur le chemin de la transmission de données est doté d'une valeur de MTU inférieure à celle des autres appareils, les paquets de données doivent être séparés ou « fragmentés » pour accommoder le dispositif ayant la MTU la plus basse.

Le meilleur paramètre de MTU pour les périphériques associés au NETGEAR correspond dans bien des cas à la valeur par défaut. La modification de cette valeur pourrait régler un problème mais en créer un autre. Laissez la valeur de la MTU inchangée sauf si l'une des situations suivantes se produit :

- Vous avez de la difficulté à vous connecter à votre FAI ou à un autre service Internet et le service de soutien technique du FAI ou de NETGEAR vous recommande de modifier le paramètre de la MTU. Les applications Web suivantes peuvent nécessiter la modification de la valeur de la MTU :

- Un site Web sécurisé qui ne se charge pas ou qui n'affiche qu'une partie d'une page Web
- Yahoo! Mail
- Le portail MSN
- Le service DSL de America Online
- Vous utilisez un RPV et éprouvez de sérieux problèmes de performance.
- Vous avez utilisé un logiciel pour optimiser la MTU à des fins de rendement et vous éprouvez depuis des problèmes de connexion ou de performance.

Remarque : Une valeur de MTU incorrecte occasionne des problèmes de communication Internet, comme l'incapacité à accéder à certains sites Web, aux cadres des sites Web, aux pages à connexion sécurisée et aux serveurs FTP ou POP.

Si vous croyez avoir un problème au niveau de la MTU, la solution générale consiste à modifier la valeur de la MTU à 1 400. Si vous souhaitez expérimenter, vous pouvez réduire graduellement la MTU à partir de la valeur maximale de 1 500, jusqu'à ce que le problème cesse. Le tableau suivant décrit les tailles de MTU communément utilisées et les utilisations connexes.

Tableau 2. Tailles de MTU communément utilisées

MTU	Application
1 500	Paquet Ethernet le plus volumineux et valeur par défaut. Il s'agit du paramètre habituel pour les connexions autres que PPPoE et RPV, ainsi que de la valeur par défaut pour les routeurs, les adaptateurs et les commutateurs de NETGEAR.
1 492	Valeur utilisée dans les environnements PPPoE.
1 472	Taille maximale à utiliser pour l'envoi de requêtes Ping. (Les paquets plus volumineux sont fragmentés.)
1 468	Valeur utilisée dans certains environnements DHCP.
1 460	Peut être utilisée par AOL si vous ne disposez pas de pièces jointes de courriel volumineuses, par exemple.
1 436	Est utilisée dans les environnements PPTP ou dans les RPV.
1 400	Taille maximale pour les connexions DSL d'AOL.
576	Valeur type pour établir une connexion par ligne commutée à des FAI.

➤ **Pour modifier la taille de la MTU :**

1. Sélectionnez **AVANCÉ > Configuration > Paramètres WAN**.
2. Dans le champ Taille de la MTU, entrez une nouvelle valeur entre 64 et 1500.
3. Cliquez sur **Appliquer** pour enregistrer les paramètres.

Paramétrage LAN

L'écran Paramétrage LAN permet de configurer des services IP en réseau, tel que DHCP (Dynamic Host Configuration Protocol) et RIP (Routing Information Protocol).

Le routeur est préconfiguré en usine afin d'utiliser les adresses IP privées du côté du réseau local et d'agir en tant que serveur DHCP. La configuration IP du LAN par défaut du routeur est :

- Adresse IP du LAN : **192.168.0.1**
- Masque de sous-réseau. **255.255.255.0**

Ces adresses font partie de la plage d'adresses désignées définie pour les réseaux privés et devrait convenir à la plupart des applications. Si votre réseau doit utiliser un schéma d'adressage IP différent, vous pouvez effectuer des modifications dans cet écran.

Remarque : Si vous modifiez l'adresse IP réseau du routeur à l'aide d'un navigateur Web, vous perdrez votre connexion. Vous devrez ouvrir une nouvelle session à la nouvelle adresse IP.

➤ Pour modifier les paramètres LAN :

1. Sélectionnez **AVANCÉ > Configuration > Paramétrage LAN** pour accéder à l'écran suivant :

2. Entrez les paramètres que vous désirez personnaliser. Ces paramètres sont décrits dans la section [Paramètres de l'écran Paramétrage LAN](#) à la page 148.
3. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Paramètres de l'écran Paramétrage LAN

Paramétrage TCP/IP du LAN

- **Adresse IP.** L'adresse IP du réseau local du routeur.
- **Masque de sous-réseau IP.** Le masque de sous-réseau du réseau local du routeur. Lorsque combiné à une adresse IP, le masque de sous-réseau IP permet à un périphérique de savoir quelles adresses sont locales et quelles adresses doivent être atteintes à l'aide d'une passerelle ou du routeur.
- **Direction RIP.** Le protocole RIP (Router Information Protocol) permet à un routeur d'échanger des informations sur le routage avec d'autres routeurs. Ce paramètre contrôle la façon dont le routeur envoie et reçoit des paquets de données RIP. Le paramètre par défaut est Les deux. Avec le paramètre Les deux ou Sortie seulement, le routeur diffuse périodiquement sa table de routage. Avec le paramètre Les deux ou Entrée seulement, le routeur incorpore les données RIP qu'il reçoit.
- **Versión RIP.** Ce paramètre contrôle le format et la méthode de diffusion des paquets de données qu'envoie le routeur. Il reconnaît les deux formats lors de la réception. Par défaut, la fonction RIP est désactivée.

RIP-1 est pris en charge universellement. Il convient à la plupart des réseaux, sauf si vous disposez d'une configuration de réseau inusitée.

RIP-2 contient plus d'information. Les versions RIP-2B et RIP-2M envoient tous deux les données de routage au format RIP-2. RIP-2B utilise la diffusion par sous-réseau. RIP-2M utilise la multidiffusion.

Utiliser le routeur comme serveur DHCP

Cette case est habituellement cochée, ce qui permet au routeur de fonctionner comme serveur DHCP.

- **Adresse IP de début.** Définit le début de la plage définie comme réserve d'adresses IP dans le même sous-réseau que le routeur.
- **Adresse IP de fin.** Définit la fin de la plage définie comme réserve d'adresses IP dans le même sous-réseau que le routeur.

Réservation d'adresses

Lorsque vous définissez une adresse IP réservée pour un ordinateur du réseau local, cet ordinateur se fait attribuer la même adresse IP chaque fois qu'il accède au serveur DHCP du routeur. Attribuez des adresses IP réservées à des serveurs nécessitant des paramètres IP permanents.

Utilisation du Routeur comme serveur DHCP

Par défaut, le routeur fonctionne comme un serveur DHCP, ce qui lui permet d'attribuer les adresses IP, l'adresse du serveur DNS et l'adresse de la passerelle par défaut à tous les ordinateurs connectés au réseau local du routeur. L'adresse de passerelle par défaut assignée est l'adresse du LAN du routeur. Les adresses IP sont attribuées par le routeur aux ordinateurs connectés au réseau local à partir de la réserve d'adresses définie dans cet écran. Chaque adresse de la réserve est testée avant l'attribution, pour éviter de dupliquer les adresses dans le réseau local. Pour la plupart des applications, les paramètres par défaut DHCP et TCP/IP définis dans le routeur sont adéquats.

Vous pouvez définir la réserve d'adresses IP à assigner en remplissant les champs Adresse IP de début et Adresse IP de fin. Ces adresses devraient faire partie du même sous-réseau que l'adresse IP du routeur. Avec le schéma d'adressage par défaut, vous devriez définir une plage entre 192.168.1.2 et 192.168.1.254, en réservant peut-être une partie de cette plage pour les périphériques ayant une adresse fixe.

Le routeur fournit les paramètres suivants à tous les périphériques du réseau local transmettant une requête DHCP :

- Une adresse IP provenant de la plage que vous avez définie
- Le masque de sous-réseau
- L'adresse IP de la passerelle (l'adresse IP réseau du routeur)
- Le serveur DNS principal, si vous avez entré une adresse DNS principale dans l'écran Configuration Internet; sinon, l'adresse IP du routeur dans le réseau local
- Le serveur DNS secondaire, si vous avez entré une adresse DNS secondaire dans l'écran Configuration Internet

Pour utiliser un autre dispositif sur votre réseau comme serveur DHCP ou pour configurer manuellement les paramètres réseau de tous vos ordinateurs, décochez la case **Utiliser le routeur comme serveur DHCP**, puis cliquez sur **Appliquer**. Sinon, laissez cette case cochée. Si ce service n'est pas activé et qu'aucun autre serveur DHCP n'est disponible sur votre réseau, vous devez définir manuellement les adresses IP de vos ordinateurs ou ils ne pourront pas accéder au routeur.

Réservation d'adresses

Lorsque vous définissez une adresse IP réservée pour un ordinateur dans votre réseau local, cet ordinateur se voit attribuer la même adresse IP chaque fois qu'il accède au serveur DHCP du routeur. Les adresses IP réservées devraient être attribuées à des ordinateurs ou serveurs ayant besoin de paramètres IP permanents.

➤ **Pour réserver une adresse IP :**

1. Dans la section Réservation d'adresses de l'écran, cliquez sur le bouton **Ajouter** pour accéder à l'écran suivant :

The screenshot shows the 'Réservation d'adresses' interface. At the top, there are buttons for '+ Ajouter', 'X Annuler', and 'G Actualiser'. Below is a table titled 'Tableau d'adresses réservées' with columns: #, Adresse IP, Nom du périphérique, and Adresse MAC. The table contains one row with the following data: #1, 192.168.0.2, CPEI829621, and 90:fb:a6:87:ff:fd. Below the table, there are input fields for adding a new reservation: 'Adresse IP' (with a dotted quad input showing 192.168.0.), 'Adresse MAC', and 'Nom du périphérique'.

2. Dans le champ Adresse IP, entrez l'adresse IP fixe à attribuer à l'ordinateur ou au serveur. Choisissez une adresse IP faisant partie du sous-réseau du réseau local du routeur, par exemple 192.168.1.x.
3. Entrez l'adresse MAC de l'ordinateur ou du serveur.

Conseil : Si l'ordinateur se trouve déjà sur votre réseau, vous pouvez copier son adresse MAC à partir de l'écran Dispositifs connectés et le copier ici.

4. Cliquez sur **Appliquer** pour entrer l'adresse réservée dans le tableau.

L'adresse réservée ne sera pas attribuée jusqu'à ce que cet ordinateur communique avec le serveur DHCP du routeur. Redémarrez l'ordinateur ou ouvrez sa configuration IP et forcez l'abandon et le renouvellement de l'adresse IP avec DHCP.

Pour modifier ou supprimer une entrée d'adresse réservée, activez le bouton radio associé à l'adresse réservée que vous désirez modifier ou supprimer. Ensuite, cliquez sur **Modifier** ou **Supprimer**.

Paramétrage QoS (Qualité de service)

La qualité du service (QoS) est une fonctionnalité avancée qui peut servir à prioriser certains types de trafic par rapport aux autres. Le Routeur sans fil 11n LTE à haut débit mobile peut fournir la priorisation QoS au moyen de la liaison sans fil et de la connexion Internet. Pour configurer la qualité du service, utilisez l'écran Paramétrage QoS (Qualité de service).

Sélectionnez **AVANCÉ > Configuration > Paramétrage QoS** (Qualité de service) pour accéder à l'écran suivant :

The screenshot shows the 'Paramétrage QoS (Qualité de service)' screen in the NETGEAR Genie interface. The left sidebar contains navigation options: 'DE BASE', 'AVANCÉ', and 'Français'. Under 'AVANCÉ', there are buttons for 'Accueil AVANCÉ', 'Assistant de configuration', 'Assistant WPS', and a 'Configuration' dropdown menu. The 'Configuration' menu is expanded, showing options like 'Paramètres haut débit', 'Paramètres haut débit mobile', 'Paramètres haut débit Ethernet', 'Configuration sans fil', 'Paramètres WAN', 'Paramétrage LAN', and 'Paramétrage QoS (Qualité de service)'. The 'Paramétrage QoS (Qualité de service)' option is selected. The main content area has a title bar with 'Paramétrage QoS (Qualité de service)' and buttons for 'Appliquer' and 'Annuler'. Below the title bar, there are three checkboxes: 'Activer les paramètres WMM (Wi-Fi Multimedia)' (checked), 'Activer la QoS de l'accès Internet' (unchecked), and 'Activer le contrôle de bande passante' (unchecked). Under 'Activer le contrôle de bande passante', there are two radio buttons: 'Bande passante montante: maximum' (selected) and 'Vérifier automatiquement la bande passante Internet montante'. The 'Bande passante montante: maximum' option has a text input field with '256' and a dropdown menu with 'Kbit/s'. There is a 'Vérifier' button next to the 'Vérifier automatiquement la bande passante Internet montante' option. At the bottom, there is a section titled 'Liste des règles de priorités QoS' with a button 'Configurer une règle de QoS'. The footer of the screen contains 'Centre d'aide' and 'Afficher/masquer le centre d'aide'.

Activation de WMM QoS pour les applications multimédias sans fil

WMM (Wireless Multimedia) est un sous-ensemble du standard 802.11e. WMM permet de définir une large gamme de priorités, en fonction des données transmises à l'aide de la connexion sans fil. Les données affectées par les délais, comme la vidéo et l'audio, obtiennent une priorité plus élevée que le trafic normal. Pour que WMM fonctionne correctement, les clients sans fil doivent aussi prendre en charge WMM.

WMM QoS est activé par défaut. Vous pouvez le désactiver dans l'écran Paramétrage QoS (Qualité de service) en décochant la case **Activer les paramètres WMM** (Wi-Fi Multimedia), puis en cliquant sur **Appliquer**.

Activer la QoS de l'accès Internet

Activez cette fonctionnalité pour que la fonction QoS priorise le trafic Internet.

Gestion des règles de priorité QoS

Sélectionnez **AVANCÉ > Configuration > Paramétrage QoS** et cliquez sur le bouton **Configurer une règle de QoS** pour accéder à l'écran suivant :

Centre d'aide

AVANCÉ

Afficher/cacher le centre d'aide

Langue: Français

Liste des règles de priorités QoS

Appliquer Annuler

#	Polices de QoS	Priorité	Description
1	MSN Messenger	Haute	MSN_messenger Applications
2	Yahoo Messenger	Haute	Yahoo_messenger Applications
3	IP Phone	La plus haute	IP_Phone Applications
4	Vonage IP Phone	La plus haute	Vonage_IP_Phone Applications
5	NetMeeting	Haute	NetMeeting Applications
6	AIM	Haute	AIM Applications
7	Google Talk	La plus haute	Google_Talk Applications
8	Netgear EVA	La plus haute	Netgear EVA Applications
9	SSH	Haute	SSH Applications
10	Telnet	Haute	Telnet Applications
11	VPN	Haute	VPN Applications
12	FTP	Normale	FTP Applications
13	SMTP	Normale	SMTP Applications
14	WWW	Normale	WWW Applications

#	Polices de QoS	Priorité	Description
17	eMule / eDonkey	Basse	eMule / eDonkey Applications
18	Kazaa	Basse	Kazaa Applications
19	Gnutella	Basse	Gnutella Applications
20	BT / Azureus	Basse	BT / Azureus Applications
21	Counter Strike	Haute	Jeu en ligne Counter Strike
22	Ages of Empires	Haute	Jeu en ligne Age of Empires
23	Everquest	Haute	Jeu en ligne Everquest
24	Quake 2	Haute	Jeu en ligne Quake 2
25	Quake 3	Haute	Jeu en ligne Quake 3
26	Unreal Tournament	Haute	Jeu en ligne Unreal Tournament
27	Warcraft	Haute	Jeu en ligne Warcraft

Modifier Effacer Effacer tout

Ajouter une règle de priorité

Centre d'aide

Afficher/masquer le centre d'aide

Dans le cas d'applications telles que le jeu en ligne, d'un port réseau LAN ou d'une adresse MAC spécifiée qui se trouve déjà dans la liste, modifiez le niveau de priorité en le sélectionnant puis en cliquant sur **Modifier**. Cliquez sur **Supprimer** pour effacer la règle de priorité.

Vous pouvez également définir la politique de priorité pour chaque jeu en ligne, application, port LAN ou adresse MAC de l'ordinateur en cliquant sur **Ajouter une règle de priorité**.

Pour les applications ou les jeux en ligne

- **Pour paramétrer la priorité d'une application ou d'un jeu en ligne :**

1. Sélectionnez **Applications** ou **Jeu en ligne** dans la liste Catégorie de priorité.

2. Sélectionnez l'application Internet ou le jeu à partir de la liste.
3. Sélectionnez le niveau de priorité : La plus élevée, Élevée, Normale ou Basse.

4. Dans le champ Politique QoS pour, entrez le nom de cette règle.
5. Cliquez sur **Appliquer**.

Pour un port LAN Ethernet

➤ **Pour configurer la priorité des ordinateurs connectés à un port LAN :**

1. Sélectionnez **Port Ethernet LAN** dans la liste Catégorie de priorité.

2. Sélectionnez le numéro du port LAN pour lequel vous désirez spécifier le niveau de priorité.
3. Sélectionnez le niveau de priorité : La plus élevée, Élevée, Normale ou Basse.
4. Vous pouvez également entrer le nom de cette règle dans le champ Politique QoS pour.
5. Cliquez sur **Appliquer**.

Pour une adresse MAC

➤ **Pour configurer la priorité d'un ordinateur spécifié par le biais de son adresse MAC :**

1. Sélectionnez **Adresse MAC** à partir de la liste Catégorie de priorité.

2. Cliquez sur le bouton **Actualiser** pour mettre à jour la liste des ordinateurs déjà raccordés au routeur.
3. Activez le bouton radio de l'entrée dans la table.
4. Modifiez l'information dans les champs Adresse MAC et Nom du périphérique.
5. Sélectionnez le niveau de priorité : La plus élevée, Élevée, Normale ou Basse.
6. Vous pouvez également entrer le nom de cette règle dans le champ Politique QoS pour.
7. Cliquez sur **Modifier** ou sur **Ajouter**.
8. Cliquez sur **Appliquer**.

Modification ou suppression d'une politique QoS existante

➤ **Pour modifier ou supprimer une politique QoS :**

1. Sélectionnez **AVANCÉ > Paramétrage QoS** (Qualité de service) pour accéder à l'écran Paramétrage QoS (Qualité de service).
2. Activez le bouton radio associé à la politique QoS à modifier ou supprimer, puis effectuez l'une des étapes suivantes :
 - Cliquez sur **Supprimer** pour retirer la politique QoS.
 - Cliquez sur **Modifier** pour modifier la politique QoS. Suivez les instructions dans les sections précédentes pour modifier les paramètres de la politique.
3. Cliquez sur **Appliquer** dans l'écran Paramétrage QoS (Qualité du service) pour enregistrer vos modifications.

Empêcher le chargement de contenu inapproprié sur votre réseau

Ce chapitre explique comment utiliser les fonctionnalités de pare-feu de base du routeur afin d'empêcher le chargement de contenu inapproprié sur votre ordinateur et autres périphériques connectés à votre réseau.

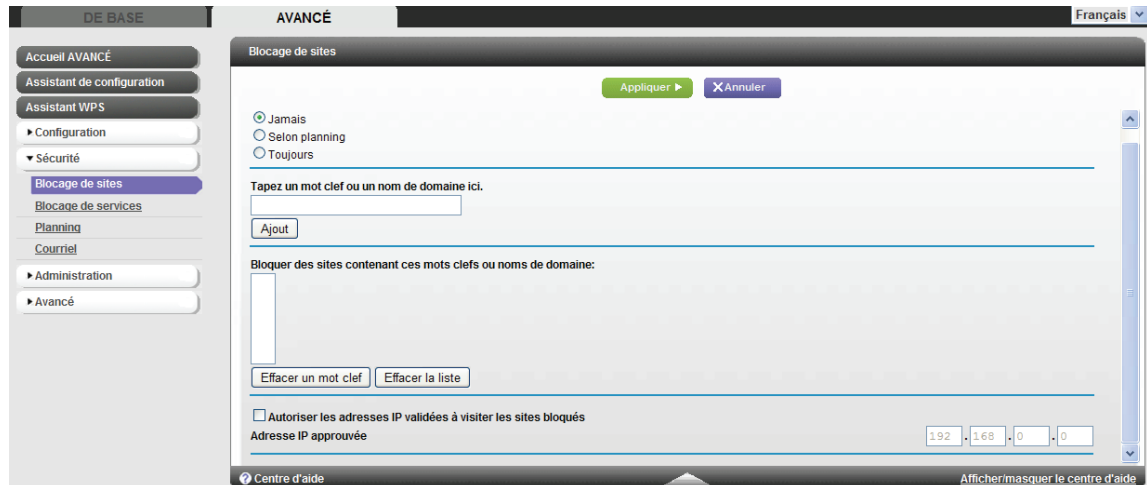
Ce chapitre comprend les sections suivantes :

- *Blocage par mot clef du trafic HTTP*
- *Blocage de services (filtrage de port)*
- *Calendrier de blocage*
- *Notifications d'événements de sécurité par courriel*

Blocage par mot clef du trafic HTTP

Utilisez le blocage par mot clef afin d'empêcher l'accès de certains types de trafic HTTP à votre réseau. Le blocage peut être permanent ou s'effectuer selon un calendrier.

1. Sélectionnez **AVANCÉ > Sécurité > Blocage de sites** pour accéder à l'écran suivant :



2. Sélectionnez une des options de blocage par mot clef :
 - **Selon le planning.** Active le blocage par mot clef selon les paramètres de l'écran Planning.
 - **Toujours.** Active le blocage par mot clef en tout temps, quels que soient les paramètres définis à l'écran Planning.
3. Dans le champ de saisie des mots clefs, entrez un mot clef ou un nom de domaine, cliquez sur **Ajout**, puis sur **Appliquer**.

La liste de mots clefs peut contenir jusqu'à 32 entrées. Voici quelques exemples de saisie :

- Spécifiez XXX pour bloquer <http://www.mauvaiscontenu.com/xxx.html>.
- Spécifiez .com si vous ne voulez autoriser que des sites avec des suffixes de domaine comme .edu ou .gov.
- Entrez un point (.) pour bloquer tout accès à la navigation Web.

➤ **Pour supprimer un mot clef ou un nom de domaine :**

1. Sélectionnez le mot clef à supprimer de la liste.
2. Cliquez sur **Supprimer**, puis sur **Appliquer** pour enregistrer vos modifications.

➤ **Pour spécifier un ordinateur de confiance :**

Vous pouvez exempter un ordinateur de confiance de tout blocage et journalisation. L'ordinateur exempté doit comporter une adresse IP fixe.

1. Entrez l'adresse IP dans le champ Adresse IP approuvée.
2. Cliquez sur **Appliquer** pour enregistrer vos modifications.

Blocage de services (filtrage de port)

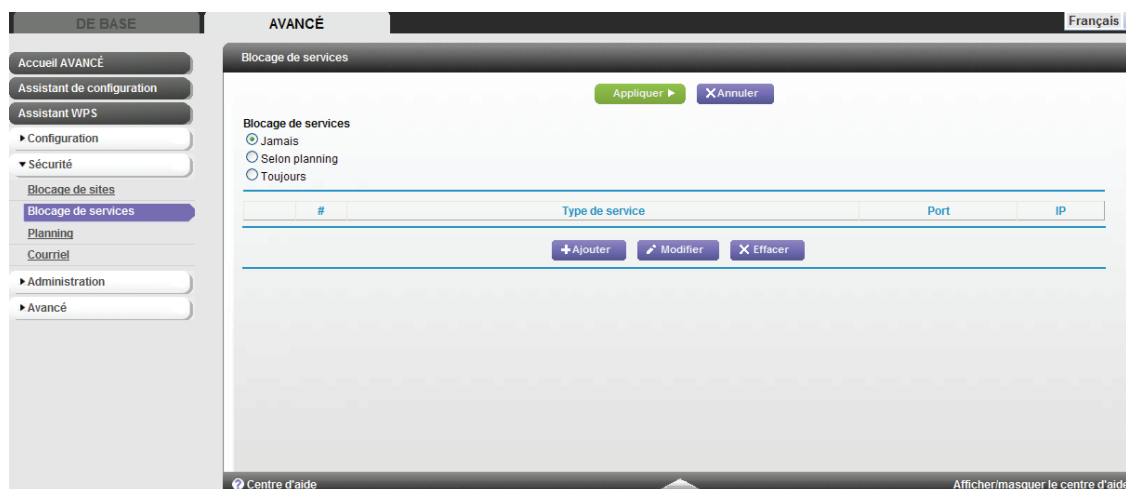
Les services sont des fonctions effectuées par des serveurs à la demande des ordinateurs clients. Par exemple, les serveurs Web fournissent des pages Web, les serveurs temporels fournissent des informations sur l'heure et la date et les serveurs hôtes de jeux fournissent des données sur les actions des autres joueurs. Lorsqu'un ordinateur sur Internet envoie une demande de service à un serveur, le service demandé est identifié selon un numéro de service ou de port. Ce numéro apparaît comme numéro de port de destination dans les paquets de données IP transmis. Par exemple, un paquet envoyé comportant le numéro de port de destination 80 est une demande HTTP (serveur Web).

Les numéros de service de nombreux protocoles fréquemment utilisés ont été définis par l'Internet Engineering Task Force (IETF, au <http://www.ietf.org/>) et publiés dans le document RFC1700, « Assigned Numbers » (Numéros assignés). Les numéros de service des autres applications sont habituellement tirés de la plage 1 024 à 65 535 par les auteurs de l'application. Bien que le routeur contienne déjà la liste de plusieurs numéros de port de service, vous n'êtes pas limité par cette sélection. Dans bien des cas, vous pouvez déterminer le numéro de port en communiquant avec l'éditeur de l'application, en posant la question à des groupes d'utilisateurs ou dans des forums, ou bien en effectuant une recherche.

L'écran Blocage de services vous permet d'ajouter et de bloquer des services Internet spécifiques pour les ordinateurs de votre réseau. C'est ce qu'on appelle le blocage de services ou le filtrage de port. Pour ajouter un service à bloquer, déterminez tout d'abord le numéro de port ou la plage de numéros utilisés par l'application.

➤ Pour bloquer des services :

1. Sélectionnez **AVANCÉ > Sécurité > Blocage de services** pour accéder à l'écran suivant :



2. Sélectionnez **Selon planning** ou **Toujours** pour activer le blocage de services, puis cliquez sur **Appliquer**. Si vous avez sélectionné Selon planning, spécifiez la période dans l'écran Planning, tel que décrit dans la section [Calendrier de blocage](#) à la page 160.

3. Cliquez sur **Ajouter** pour ajouter un service. L'écran Paramétrage du blocage de services s'affiche :

4. À partir de la liste Type de service, sélectionnez l'application ou le service à autoriser ou à bloquer. La liste comprend déjà plusieurs services fréquemment utilisés, mais vous n'êtes pas limité par cette sélection. Pour ajouter des services ou applications supplémentaires, sélectionnez **Défini par l'utilisateur**.
5. Si vous savez si l'application utilise le protocole TCP ou UDP, sélectionnez le protocole approprié. Si vous n'êtes pas certain, sélectionnez **Les deux**.
6. Entrez les numéros de port de début et de fin. Si l'application utilise un seul numéro de port, entrez ce numéro dans les deux champs.
7. Activez le bouton radio associé à la configuration d'adresse IP que vous désirez bloquer, puis entrez les adresses IP. Vous pouvez bloquer le service spécifié pour un seul ordinateur, pour un groupe d'ordinateurs dotés d'adresses IP consécutives ou pour tous les ordinateurs de votre réseau.
8. Cliquez sur **Ajouter** pour activer vos sélections du paramétrage du blocage de services.

Calendrier de blocage

Vous pouvez spécifier les jours et à l'heure auxquels vous désirez bloquer l'accès Internet.

➤ **Pour programmer le blocage :**

1. Sélectionnez **AVANCÉ > Sécurité > Planning** pour accéder à l'écran suivant :

2. Définissez le planning de blocage de mots clefs et de services.
 - **Jours à bloquer.** Sélectionnez les jours auxquels vous désirez appliquer le blocage en cochant les cases appropriées ou bien cochez **Chaque jour** pour cocher les cases associées à tous les jours.
 - **Heures à bloquer.** Sélectionnez une heure de début et de fin en format 24 heures ou cochez **Toute la journée** pour un blocage de 24 heures.
3. Sélectionnez votre fuseau horaire dans la liste. Si vous utilisez l'heure avancée, cochez la case **Ajuster automatiquement l'heure d'été**.
4. Cliquez sur **Appliquer** pour enregistrer vos paramètres.

Notifications d'événements de sécurité par courriel

Pour recevoir des journaux et alertes par courriel, fournissez votre adresse de courriel à l'écran E-mail, puis spécifiez quelles alertes vous désirez recevoir et à quelle fréquence.

➤ **Pour configurer les notifications par courriel :**

1. Sélectionnez **AVANCÉ > Sécurité > E-mail** pour accéder à l'écran suivant :

2. Pour recevoir des envois de journaux et d'alertes par courriel de la part du routeur, cochez la case **Activer la notification par E-mail**.
3. Dans le champ Serveur mail sortant, entrez le nom du serveur de messagerie (SMTP) sortant de votre FAI (ex. courriel.monFAI.com). Vous trouverez peut-être cette information dans l'écran de configuration de votre logiciel de courriel. Si vous laissez ce champ vide, les journaux et alertes ne seront pas envoyés par courriel.
4. Dans le champ Envoyer à cette adresse email, entrez l'adresse de courriel à laquelle les journaux et alertes seront envoyés. Cette adresse de courriel servira également d'adresse d'expéditeur. Si vous laissez ce champ vide, les journaux et alertes ne seront pas envoyés par courriel.
5. Si votre serveur de messagerie sortant requiert une authentification, cochez la case **Mon serveur mail requiert une authentification**. Remplissez les champs Identifiant et Mot de passe pour le serveur de messagerie sortant.
6. Vous pouvez exiger que des alertes soient immédiatement envoyées par courriel lorsqu'une personne tente d'accéder à un site bloqué. Vous pouvez également spécifier que les journaux soient envoyés automatiquement.

Si vous sélectionnez l'option Hebdomadaire, Quotidien ou Chaque heure et que le journal est plein avant la période indiquée, le journal est envoyé automatiquement par courriel à l'adresse entrée. Une fois le journal envoyé, celui-ci est effacé de la mémoire du routeur. Si le routeur ne parvient pas à envoyer par le fichier journal, la mémoire tampon du journal pourrait être pleine. Dans ce cas, le routeur remplace le journal et efface son contenu.

7. Cliquez sur **Appliquer** pour enregistrer vos paramètres.

Gestion de votre réseau

Ce chapitre décrit les paramètres de routeur pour la gestion et la maintenance de votre routeur et de votre réseau domestique. Consultez également la section [Gestion à distance](#) à la page 194 pour obtenir plus d'informations sur la mise à niveau ou pour vérifier le statut de votre routeur sur Internet, ainsi que la section [Mesure de trafic](#) à la page 196 pour des informations sur la surveillance du volume du trafic Internet passant par le port Internet de votre routeur.

Ce chapitre comprend les sections suivantes :

- [Statut du Routeur](#)
- [Journaux](#)
- [Dispositifs connectés](#)
- [Paramètres de sauvegarde](#)
- [Définition du mot de passe](#)
- [Diagnostic](#)
- [Mise à niveau du routeur](#)
- [Mise à niveau du module](#)

Statut du Routeur

Utilisez l'écran Statut du routeur pour vérifier les paramètres et statistiques actuels de votre routeur. Cet écran illustre les paramètres actuels. Si vous devez apporter des changements, faites-le sur l'écran approprié.

➤ **Pour afficher le statut du routeur et les renseignements d'utilisation :**

1. Sélectionnez **Avancé > Administration > Statut du routeur** pour afficher l'écran suivant :



Les informations de statut suivantes s'affichent :

- **Connexion active.** L'interface WAN actuelle utilisée par le routeur.
- **Version du compte.** Le modèle du routeur.
- **Version du micrologiciel (firmware).** La version du micrologiciel (firmware) du routeur. Elle change si vous mettez à niveau le micrologiciel (firmware) du routeur.
- **Port Ethernet.** Les paramètres actuels du port Ethernet haut débit.
 - **Adresse MAC.** L'adresse de commande d'accès au support. Il s'agit de l'unique adresse physique utilisée par le port Internet (WAN) du routeur.
 - **Adresse IP.** L'adresse IP utilisée par le port Internet (WAN) du routeur. Si aucune adresse n'apparaît ou si l'adresse est 0.0.0.0, le routeur ne peut pas se connecter à l'Internet.
 - **Type de réseau.** Indique si le routeur utilise une adresse IP fixe sur le réseau WAN. Si la valeur est Client DHCP, le routeur obtient dynamiquement une adresse IP par le FAI.
 - **Masque de sous-réseau IP.** Le masque de sous-réseau par le port Internet (WAN) du routeur.
 - **Adresse IP de la passerelle.** Adresse IP utilisée par le routeur.
 - **Serveur de nom de domaine.** Les adresses du serveur de nom de domaine utilisées par le routeur. Un serveur de noms de domaine traduit les URL en langage humain comme www.netgear.com en adresses IP.

- **Modem de connexion haut débit.** Indique les propriétés du modem haut débit mobile.
 - **Identité du modem.** Indique le modem utilisé.
 - **Version du logiciel du modem.** Indique la version du logiciel du modem.
 - **Version du pilote du modem.** Indique la version du pilote du modem.
 - **IMEI.** Identité internationale d'équipement mobile. Identité unique du modem.
 - **Fournisseur.** Fournisseur d'accès Internet pour le réseau sans fil haut débit.
 - **Mode réseau.** Mode du réseau actuel auquel le modem est connecté. Le mode dépend de la couverture et de la distance par rapport au site cellulaire.
- **Port à haut débit mobile.** Les paramètres actuels du port à haut débit mobile.
 - **Statut de la connexion.** Indique le statut de la connexion haut débit sans fil.
 - **Adresse IP.** L'adresse IP utilisée par le port Internet (WAN) du routeur. Si aucune adresse n'apparaît ou si l'adresse est 0.0.0, le routeur ne peut pas se connecter à l'Internet.
 - **Protocole.** Indique si le routeur utilise une adresse IP fixe sur le réseau WAN. Si la valeur est Client DHCP, le routeur obtient dynamiquement une adresse IP par le FAI.
 - **Masque de sous-réseau IP.** Le masque de sous-réseau par le port Internet (WAN) du routeur.
 - **Serveur de nom de domaine.** Les adresses du serveur de nom de domaine utilisées par le routeur. Un serveur de noms de domaine traduit les URL en langage humain comme www.netgear.com en adresses IP.
- **LAN Port (Port LAN).** Ce sont les paramètres courants, tels que définis dans l'écran Paramétrage LAN.
 - **Adresse MAC.** L'adresse de commande d'accès au support. Il s'agit de l'unique adresse physique utilisée par le port Ethernet (LAN) du routeur.
 - **Adresse IP.** L'adresse IP utilisée par le port Ethernet (LAN) du routeur. La valeur par défaut est 192.168.0.1.
 - **DHCP.** Indique si le serveur DHCP intégré dans le routeur est actif pour les périphériques LAN connectés.
 - **Masque de sous-réseau IP.** Le masque de sous-réseau associé à l'adresse LAN IP.
- **Port réseau sans fil.** Ce sont les paramètres courants, tels que définis dans l'écran des Paramètres du réseau sans fil.
 - **Nom (SSID).** Nom de réseau sans fil du routeur.
 - **Région.** Le lieu (pays).
 - **Canal.** Le canal actuellement utilisé.
 - **Point d'accès sans fil.** Indique si la fonction de point d'accès est activée ou non sur le routeur. Si elle est désactivée, le voyant Wi-Fi situé sur le panneau avant est éteint.
 - **Nom diffusé.** Indique si le routeur diffuse son SSID.

2. Cliquez sur **Afficher les statistiques** pour afficher les statistiques de performance du routeur, par exemple le nombre de paquets envoyés et le nombre de paquets reçus pour chaque port.

Show Statistics

System Up Time 01:22:14

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	100MFull	922	8930	0	0	123	01:21:43,01:21:45
LAN1	Link Down						--
LAN2	Link Down						--
LAN3	Link Down						--
LAN4	Link Down						--
WLAN	145M	4004	2987	0	677	62	01:21:57

Poll Interval: 5 (secs)

- **Temps de disponibilité du système.** Le temps écoulé depuis le dernier redémarrage du routeur.
- **Port.** Les statistiques pour les ports WAN (Internet) et LAN (Ethernet). Pour chaque port, l'écran affiche :
 - **Statut.** Le statut de la liaison du port.
 - **TxPkts.** Nombre de paquets transmis sur ce port depuis la dernière réinitialisation ou suppression manuelle.
 - **RxPkts.** Nombre de paquets reçus sur ce port depuis la dernière réinitialisation ou suppression manuelle.
 - **Collisions.** Nombre de collisions sur ce port depuis la dernière réinitialisation ou suppression manuelle.
 - **Tx B/s.** La bande passante de transmission (sortant) actuelle utilisée sur les ports WAN et LAN.
 - **Rx B/s.** La bande passante de réception (entrant) actuelle utilisée sur les ports WAN et LAN.
 - **Temps de disponibilité.** Le temps écoulé depuis que ce port a acquis le lien.
 - **Intervalle d'interrogations.** La fréquence à laquelle les statistiques sont mises à jour dans cet écran.

Pour modifier la fréquence d'interrogation, entrez une durée en secondes dans le champ Intervalle d'interrogation, puis cliquez sur **Définir intervalle**.

Pour arrêter entièrement l'interrogation, cliquez sur **Arrêter**.

3. Cliquez sur **Statut de la connexion** pour voir des informations sur votre connexion courante.

The screenshot shows two sections of a web interface. The top section, titled 'Statut de la connexion haut-débit mobile', contains a table with the following data:

Statut de la connexion	Négociation
Received Signal Quality(in dbm)	0
Octets transmis	---
Octets reçus	---
Tx B/s	---
Rx B/s	---
Durée de fonctionnement du système	00:00:56
Durée de la connexion	00:00:00

The bottom section, titled 'Statut de la connexion', contains a table with the following data:

Adresse IP	0.0.0.0
Masque de sous-réseau	0.0.0.0
Passerelle par défaut	0.0.0.0
Serveur DNS	0.0.0.0

At the bottom of the interface, there is a 'Recharger' button with a dropdown menu set to '5 (secs)', a 'Définir intervalle' button, an 'Arrêter' button, and a 'Fermer la' button.

- Statut de la connexion haut débit mobile.
 - **Statut de la connexion.** Statut de la connexion Internet.
 - **Qualité du signal reçu, en dBm.** Réception radio du modem. Une valeur faible ou négative indique que la qualité du signal est bonne.
 - **Octets transmis.** Nombre d'octets transmis au cours de la dernière session de connexion.
 - **Octets reçus.** Nombre d'octets reçus au cours de la dernière session de connexion.
 - **Tx B/s.** Débit de transmission.
 - **Rx B/s.** Débit de réception.
 - **Durée de fonctionnement du système.** Temps écoulé depuis le dernier redémarrage.
 - **Durée de la connexion.** Durée de la connexion en cours.
- Statut de la connexion.
 - **Adresse IP.** L'adresse IP qui est attribuée au routeur.
 - **Masque de sous-réseau.** Le masque de sous-réseau qui est attribué au routeur.
 - **Passerelle par défaut.** L'adresse IP de la passerelle par défaut avec laquelle le routeur communique.
 - **Serveur DHCP.** L'adresse IP du serveur DHCP qui fournit la configuration TCP/IP à tous les ordinateurs qui sont connectés au routeur.
 - **Serveur DNS.** L'adresse IP du serveur de nom de domaine qui fournit la traduction des noms de réseau aux adresses IP.
 - **Bail obtenu.** La date et l'heure de l'obtention du bail.
 - **Expiration du bail.** La date et l'heure de l'expiration du bail.

Pour modifier la fréquence d'interrogation, entrez une durée en secondes dans le champ Intervalle d'interrogation, puis cliquez sur **Définir intervalle**.

Pour arrêter entièrement l'interrogation, cliquez sur **Arrêter**.

Le bouton Fermer la fenêtre ferme l'écran Statut de la connexion.

Journaux

Le journal est un compte rendu détaillé des sites Web que vous avez visités ou tenté de visiter. Si vous avez configuré le filtrage de contenu sur l'écran de blocage de sites, l'écran Journaux vous montre à quel moment quelqu'un de votre réseau a tenté d'accéder à un site bloqué. Si vous avez activé la notification par courriel, vous recevez ces journaux dans un message électronique. Si vous n'avez pas activé la notification par courriel, consultez les journaux ici.

Sélectionnez **AVANCÉ** > **Administration** > **Journaux**. L'écran Journaux s'affiche.



Pour actualiser l'écran des journaux, cliquez sur le bouton **Actualiser**.

Pour effacer les entrées de journal, cliquez sur le bouton **Effacer les journaux**.

Pour envoyer le journal immédiatement, cliquez sur le bouton **Envoyer les journaux**. Cette fonctionnalité peut être très utile pour vérifier vos paramètres de messagerie.

Dispositifs connectés

Consultez la section [Dispositifs connectés](#) à la page 132.

Paramètres de sauvegarde

Les paramètres de configuration du Routeur sans fil 11n LTE à haut débit mobile sont conservés dans un fichier de configuration dans le routeur. Vous pouvez sauvegarder (enregistrer) le fichier sur votre ordinateur, le restaurer ou réinitialiser les paramètres par défaut d'usine.

Paramètres de sauvegarde

➤ Pour sauvegarder les paramètres de configuration du routeur :

1. Sélectionnez **Avancé > Administration > Paramètres de sauvegarde** pour afficher l'écran suivant :



2. Cliquez sur **Sauvegarder** pour enregistrer une copie des paramètres actuels.
3. Choisissez un emplacement pour stocker le fichier .cfg qui se trouve sur un ordinateur de votre réseau.

Restaurer les paramètres de configuration

➤ Pour restaurer les paramètres de configuration que vous avez sauvegardés :

1. Entrez le chemin d'accès complet du fichier sur votre réseau ou cliquez sur **Parcourir** pour rechercher le fichier.
2. Une fois le fichier .cfg trouvé, cliquez sur **Restaurer** pour charger le fichier sur le routeur.

Lorsque la restauration est terminée, le routeur redémarre.



AVERTISSEMENT:

Ne pas interrompre le processus de redémarrage.

Effacer

Dans certaines circonstances (par exemple si vous déplacez le routeur vers un autre réseau ou si vous avez oublié le mot de passe), vous pouvez effacer la configuration et restaurer les paramètres par défaut d'usine.

Vous pouvez utiliser le bouton de réinitialisation des paramètres d'usine à l'arrière du routeur (consultez la section [Paramètres par défaut d'usine](#) à la page 208), ou vous pouvez cliquer sur le bouton **Effacer** dans cet écran.

La fonction Effacer règle le nom d'utilisateur à admin, le mot de passe à password et l'adresse IP du LAN à 192.168.1.1, et active le DHCP du routeur.

Définition du mot de passe

Cette fonction vous permet de changer le mot de passe par défaut qui est utilisé pour vous connecter au routeur avec le nom d'utilisateur.

Ce n'est pas la même chose que de changer le mot de passe pour l'accès sans fil. L'étiquette sur le fond de votre routeur montre votre nom de réseau sans fil (SSID) et mot de passe uniques prédéfinis pour l'accès sans fil (consulter la section [Étiquette](#) à la page 117).

➤ Pour définir le mot de passe associé au nom d'utilisateur du :

1. Sélectionnez **Avancé > Administration > Définir le mot de passe** pour accéder à l'écran de définition du mot de passe :

2. Entrez l'ancien mot de passe, puis entrez le nouveau mot de passe deux fois dans les champs de cet écran.
3. Si vous voulez être en mesure de récupérer le mot de passe, cochez la case **Activer la récupération du mot de passe**.
4. Cliquez sur **Appliquer** pour instaurer vos modifications.

Récupération du mot de passe

NETGEAR vous recommande d'activer la récupération du mot de passe si vous modifiez le mot de passe pour le nom d'utilisateur du routeur. Vous aurez alors un moyen facile de récupérer le mot de passe en cas d'oubli. Ce processus de récupération est pris en charge dans les navigateurs Internet Explorer, Firefox et Chrome, mais pas dans le navigateur Safari.

➤ **Pour configurer la récupération mot de passe :**

1. Cochez la case **Activer la récupération du mot de passe**.
2. Sélectionnez deux questions de sécurité et fournissez les réponses.
3. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Lorsque vous utilisez votre navigateur pour accéder au routeur, l'écran de connexion s'affiche. Si la récupération de mot de passe est activée, lorsque vous cliquez sur Annuler, le processus de récupération de mot commence. Vous pouvez alors entrer les réponses enregistrées aux questions de sécurité pour récupérer le mot de passe.

Diagnostic

Utilisez l'écran Diagnostics pour effectuer divers diagnostics. Pour un fonctionnement normal, ces tests ne sont pas nécessaires.

➤ **Pour exécuter les diagnostics :**

Sélectionnez **Avancé > Administration > Diagnostic** pour accéder à l'écran suivant :

Envoyer une requête Ping à une adresse IP. Utilisez ce test pour envoyer une demande de paquet ping à l'adresse IP spécifiée. Cette procédure est souvent utilisée pour vérifier une connexion. Si la requête expire parce qu'aucune réponse n'est reçue, ce résultat signifie habituellement que la destination est inaccessible. Cependant, certains périphériques réseau peuvent être configurés pour ne pas répondre à un ping.

Effectuer une recherche de serveur DNS. Un serveur de nom de domaine (DNS) convertit un nom Internet (par exemple www.netgear.com) en une adresse IP. Si vous avez besoin de l'adresse IP d'un serveur Web, FTP, de messagerie et autre sur l'Internet, vous pouvez effectuer une recherche de serveur DNS pour trouver son adresse IP.

Afficher la table de routage. Cette opération affiche la table de routage interne. Cette information est utilisée par le service de soutien technique et d'autres employés qui comprennent les tables de routage.

Redémarrer le routeur. Utilisez ce bouton pour effectuer un redémarrage à distance. Vous pouvez utiliser cette option si le routeur semble être devenu instable ou ne fonctionne pas normalement.

Remarque : Le redémarrage interrompra toutes les connexions existantes vers le routeur (comme celle-ci) ou par l'intermédiaire du routeur (par exemple, les utilisateurs du LAN qui accèdent à Internet). Cependant, les connexions à Internet sont automatiquement rétablies lorsque cela est possible.

Enregistrer les données de diagnostic. Utilisez ce bouton pour afficher les données de diagnostic.

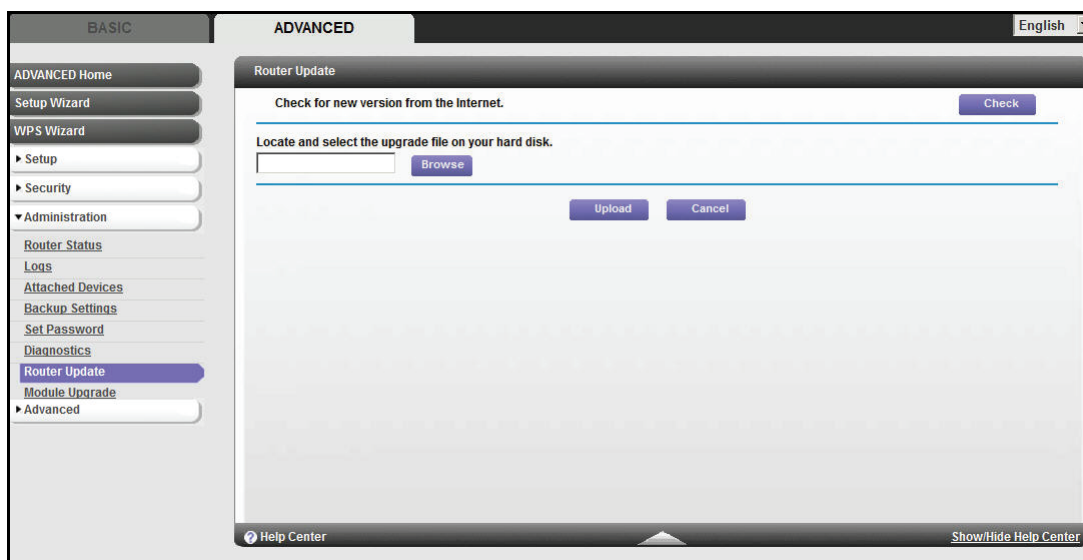
Mise à niveau du routeur

Le micrologiciel (firmware) routeur (logiciel de routage) est stocké dans la mémoire flash. Vous pouvez mettre à jour le micrologiciel (firmware) dans le menu Administration sur l'onglet AVANCÉ. Vous pouvez voir un message en haut des écrans de NETGEAR Genie lorsque le nouveau micrologiciel (firmware) est disponible pour votre produit.

Vous pouvez utiliser le bouton Vérifier sur l'écran Mise à jour du routeur pour vérifier et mettre à jour la toute dernière version du micrologiciel (firmware) pour votre produit si un nouveau micrologiciel (firmware) est disponible.

➤ **Pour vérifier l'existence d'un nouveau micrologiciel (firmware) et mettre à jour votre routeur :**

1. Sélectionnez **Avancé > Administration > Mise à jour du routeur** pour afficher l'écran suivant :



2. Cliquez sur **Vérifier**.

Le routeur trouve les informations du nouveau micrologiciel (firmware), le cas échéant.

3. Cliquez sur **Oui** pour mettre à jour et localisez le micrologiciel (firmware) que vous avez téléchargé (le fichier se termine par .img).



AVERTISSEMENT:

Lors du chargement du micrologiciel (firmware) sur le routeur, *n'interrompez pas* le navigateur en fermant la fenêtre, en cliquant sur un lien ou en chargeant une nouvelle page. Si le navigateur est interrompu, il peut corrompre le micrologiciel (firmware).

Lorsque le téléchargement est terminé, votre routeur redémarrera. Le processus de mise à niveau prend environ une minute. Lisez les notes de la nouvelle version du micrologiciel (firmware) afin de déterminer si oui ou non vous devez reconfigurer le routeur après la mise à jour.

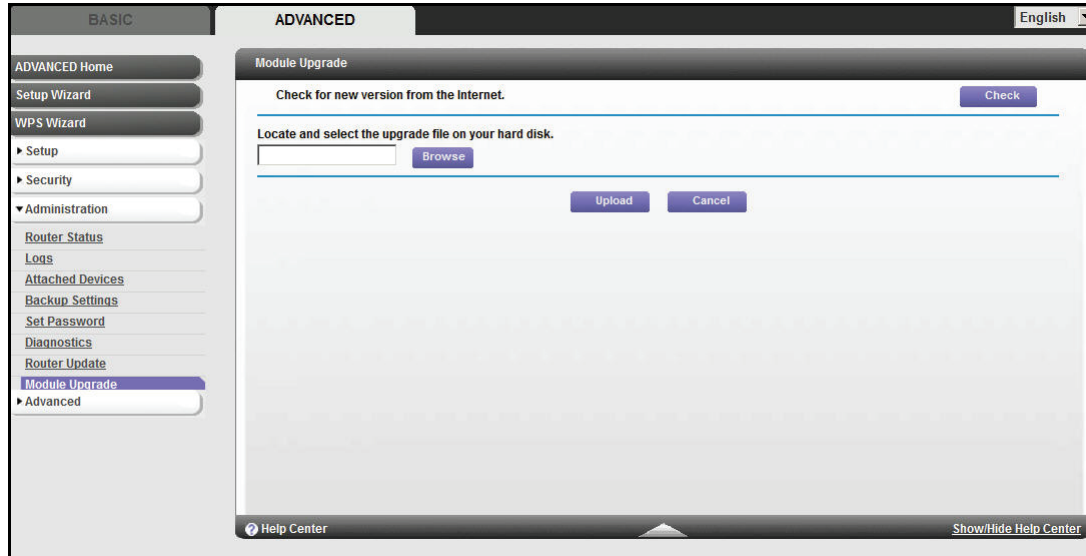
Mise à niveau du module

Le micrologiciel (firmware) du module (logiciel haut débit mobile) est stocké dans la mémoire flash. Vous pouvez mettre à niveau le micrologiciel (firmware) dans le menu Administration sur l'onglet AVANCÉ. Vous pouvez voir un message en haut des écrans de NETGEAR Genie lorsque le nouveau micrologiciel (firmware) est disponible pour votre produit.

Vous pouvez utiliser le bouton Vérifier sur l'écran Mise à jour du module pour vérifier et mettre à jour la toute dernière version du micrologiciel (firmware) pour votre produit si un nouveau micrologiciel (firmware) est disponible.

- Pour vérifier l'existence d'un nouveau micrologiciel (firmware) et mettre à jour votre routeur :

1. Sélectionnez **Avancé > Administration > Mise à jour du module** pour afficher l'écran suivant :



2. Cliquez sur **Vérifier**.

Le routeur trouve les informations du nouveau micrologiciel (firmware), le cas échéant.

3. Cliquez sur **Oui** pour mettre à jour et localisez le micrologiciel (firmware) que vous avez téléchargé (le fichier se termine par .img).



AVERTISSEMENT:

Lors du chargement du micrologiciel (firmware) sur le routeur, ***n'interrompez pas*** le navigateur en fermant la fenêtre, en cliquant sur un lien ou en chargeant une nouvelle page. Si le navigateur est interrompu, il peut corrompre le micrologiciel (firmware).

Lorsque le téléchargement est terminé, votre routeur redémarrera. Le processus de mise à niveau prend environ une minute. Lisez les notes de la nouvelle version du micrologiciel (firmware) afin de déterminer si oui ou non vous devez reconfigurer le routeur après la mise à jour.

Paramètres avancés

7

Ce chapitre décrit les fonctionnalités avancées de votre routeur. L'information est destinée aux utilisateurs ayant une bonne compréhension des concepts de réseautage qui veulent configurer le routeur pour des situations particulières, par exemple lorsqu'un accès distant par adresse IP ou nom de domaine Internet est requis.

Ce chapitre comprend les sections suivantes :

- *Paramètres de carte SIM*
- *Messages SMS*
- *Paramètres sans fil*
- *Répéteur sans fil*
- *Ouverture de port et déclenchement de port*
- *DNS dynamique*
- *Routes statiques*
- *Gestion à distance*
- *Service UPnP*
- *Mesure de trafic*

Paramètres de carte SIM

Votre FAI vous fournit une carte SIM qui vous permet d'accéder à la connexion haut débit mobile. Utilisez cet écran pour modifier les paramètres de votre carte SIM.

➤ **Pour modifier les paramètres de votre carte SIM :**

1. Sélectionnez **AVANCÉ > Avancé > Paramètres SIM** pour afficher l'écran suivant :

2. Modifiez les paramètres de la carte SIM, tel que requis :
 - **Activer ou Désactiver le code PIN.** Activez ou désactivez l'utilisation du code PIN de la carte SIM. Entrez votre code PIN pour autoriser cette modification.
 - **Modifier le code PIN.** Le code PIN empêche l'utilisation de la carte SIM dans un périphérique non autorisé. Modifiez aussi le code PIN régulièrement pour des raisons de sécurité. Entrez votre code PIN pour autoriser cette modification, suivi par le nouveau code PIN que vous avez choisi.
3. Cliquez sur **Appliquer** pour instaurer vos modifications.

Messages SMS

Consultez la section [Message SMS](#) à la page 136.

Paramètres sans fil

Remarque : Le routeur sans fil est déjà configuré avec les paramètres optimaux. Ne modifiez pas ces paramètres, sauf si le soutien technique de NETGEAR vous y invite. Des paramètres incorrects désactivent le routeur sans fil.

Sélectionnez **AVANCÉ > Avancé > Paramètres du réseau sans fil** pour afficher l'écran suivant :

Les paramètres suivants sont accessibles sur cet écran :

Paramètres sans fil avancés. Ne modifiez pas ces paramètres à moins d'y être invité par le soutien technique de NETGEAR.

- **Activer la liaison radio au réseau sans fil.** Vous pouvez désactiver complètement la portion sans fil du routeur sans fil en décochant cette case. Cochez cette case de nouveau pour activer la partie sans fil du routeur. Lorsque la case Activer le réseau sans fil est désactivé, les autres membres de la maison peuvent utiliser le routeur en reliant leurs ordinateurs au routeur à l'aide d'un câble Ethernet.
- **Activer la diffusion SSID.** Ce réglage permet la diffusion du SSID.

Remarque : Les options de longueur de fragmentation, de seuil CTS/RTS et de mode de préambule sont réservées uniquement pour les tests sans fil et la configuration avancée. Ne modifiez pas ces paramètres.

- **Puissance du signal sans fil.** Ce paramètre permet de régler la puissance de la connexion Wi-Fi de 1 % (minimum) à 100 % (maximum). Entrez un nombre entier de 1 à 100 (par défaut) dans ce champ. Le fait d'abaisser la puissance Wi-Fi limite la portée du Wi-Fi et réduit le rayonnement du Wi-Fi.

Paramètres WPS. Vous pouvez ajouter des dispositifs WPS à votre réseau.

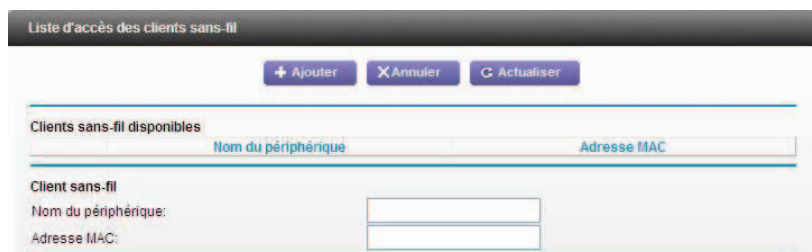
- **PIN du routeur.** Il s'agit du numéro d'identification que vous utilisez sur un registre (par exemple, à partir de l'Explorateur de réseaux sur un PC Windows Vista) pour configurer les paramètres sans fil du routeur par l'intermédiaire de WPS. Vous pouvez également trouver le code PIN sur l'étiquette du routeur.
- **Désactiver le code PIN du routeur.** Vous pouvez configurer les paramètres sans fil du routeur ou ajouter un client sans fil par l'intermédiaire de WPS en utilisant le code PIN du routeur seulement lorsque le code PIN est activé. Le code PIN du routeur peut être désactivé temporairement lorsque le routeur détecte des tentatives suspectes de percer les paramètres sans fil du routeur à l'aide du code PIN du routeur par l'intermédiaire de WPS. Vous pouvez activer manuellement cette fonction en décochant la case et en cliquant sur le bouton Appliquer.
- **Garder les paramètres existants du réseau sans fil.** Ce paramètre indique si le routeur est dans le statut WPS configuré. Si cette option n'est pas sélectionnée, l'ajout d'un nouveau client sans fil change les paramètres sans fil du routeur pour un SSID généré automatiquement de manière aléatoire et une clé de sécurité. En outre, lorsque cette option est sélectionnée, certains registres externes (par exemple, le Réseau Explorer sur Windows Vista) pourraient ne pas voir le routeur.

La configuration des paramètres sans fil de base de l'interface de gestion Web du routeur sélectionne automatiquement cette option.

Liste d'accès de cartes sans fil. Par défaut, tout ordinateur sans fil configuré avec le SSID approprié peut accéder à votre réseau sans fil. Pour augmenter la sécurité, restreignez l'accès au réseau sans fil pour n'autoriser que certains ordinateurs, en fonction de leur adresse MAC. Cliquez sur **Paramétrage de la liste d'accès** pour afficher l'écran Liste d'accès de cartes sans fil. Sur cet écran, vous pouvez restreindre l'accès à votre réseau à des périphériques précis en fonction de leur adresse MAC.



Cliquez sur **Ajouter** pour ajouter des périphériques sans fil à votre réseau en fonction de leur adresse MAC.



Cliquez sur **Appliquer** pour instaurer vos modifications.

Répéteur sans fil

Vous pouvez configurer le Routeur sans fil 11n LTE à haut débit mobile pour être utilisé comme un point d'accès sans fil. Cela permet au routeur d'agir comme un répéteur sans fil. Un répéteur sans fil se connecte à un autre routeur sans fil en tant que client, là où le réseau auquel il se connecte devient le service du FAI.

La répétition sans fil est un type de système de distribution sans fil (WDS). Un système de distribution sans fil permet à un réseau sans fil de s'étendre dans de multiples points d'accès au lieu d'utiliser un réseau fédérateur câblé pour relier ces points. La figure suivante montre un scénario de répétition sans fil.

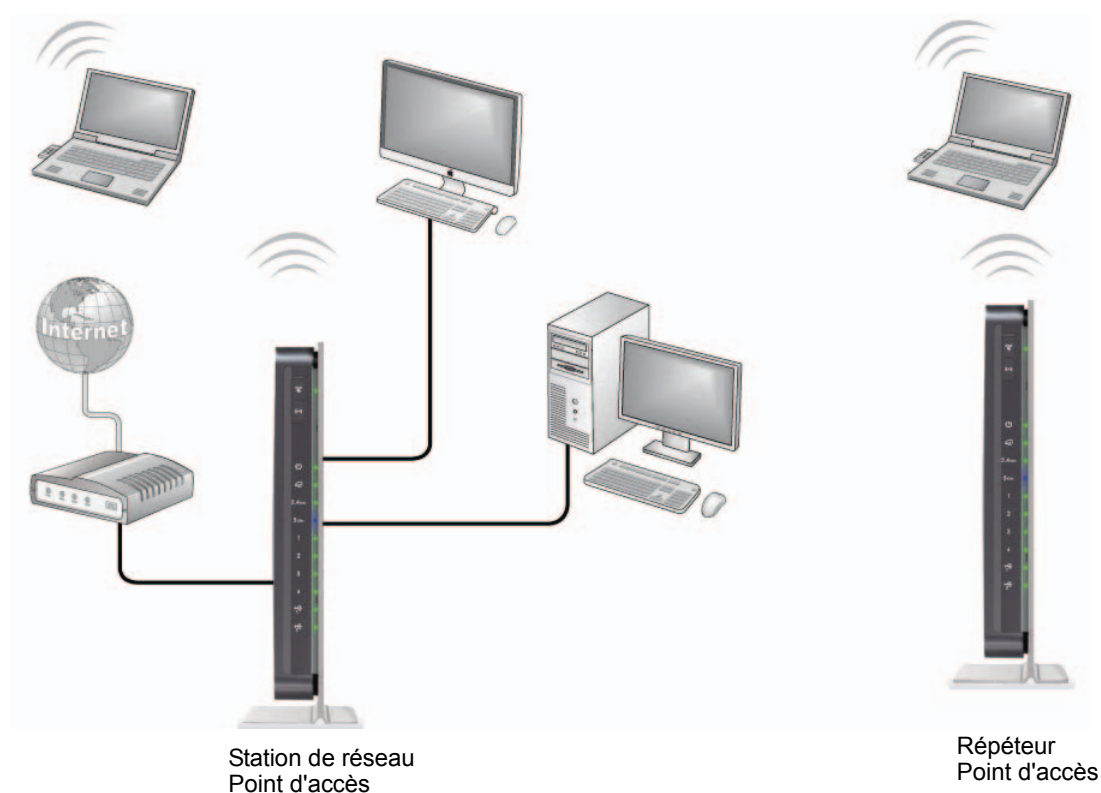


Figure 6. Scénario de répétition sans fil

Remarque : Si vous utilisez la fonction répéteur sans fil, vous devez sélectionner **WEP** ou **Aucun** comme option de sécurité dans l'écran Paramètres du réseau sans fil. L'option WEP ne s'affiche que si vous sélectionnez le mode sans fil **jusqu'à 54 Mbits/s** dans l'écran Paramètres du réseau sans fil.

Station de réseau sans fil. Le routeur agit comme le point d'accès parent, en faisant le pont entre le point d'accès répéteur enfant et en prenant en charge des ordinateurs sans fil et câblés locaux. Pour configurer ce mode, vous devez connaître les adresses MAC du point d'accès répéteur enfant.

Répéteur de réseau sans fil. Le routeur envoie tout le trafic de ses ordinateurs sans fil ou câblés à un point d'accès distant. Pour configurer ce mode, vous devez connaître l'adresse MAC du point d'accès parent éloigné.

Le routeur MBR1516 est toujours en mode bibande simultané, sauf si vous éteignez une bande radio. Soyez conscient que si vous activez le répéteur sans fil dans l'autre bande radio, la station de base sans fil ou le répéteur sans fil ne peuvent pas être activés dans la bande radio. Toutefois, si vous activez la station de base sans fil dans l'une des bandes radio et utilisez l'autre bande radio en tant que routeur sans fil ou station de base sans fil, le mode bibande simultané n'est pas modifié.

Pour qu'un réseau sans fil avec système de distribution sans fil soit configuré, les conditions suivantes doivent être respectées pour les deux points d'accès :

- Les deux points d'accès doivent utiliser les mêmes SSID, canal sans fil et mode de cryptage.
- Les deux points d'accès doivent être sur le même sous-réseau que l'adresse IP du réseau local. Autrement dit, toutes les adresses IP de réseau local des points d'accès sont sur le même réseau.
- Tous les périphériques du réseau local (ordinateurs câblés et sans fil) doivent être configurés pour fonctionner sur la même plage d'adresses de réseau local que les points d'accès.

Fonction Répéteur de réseau sans fil

Sélectionnez **AVANCÉ > Avancé > Répéteur sans fil** pour afficher ou modifier les paramètres de répéteur sans fil pour le routeur.

The screenshot shows the 'Fonction répéteur de réseau sans fil' configuration page. On the left is a sidebar with navigation links: Accueil AVANCÉ, Assistant de configuration, Assistant WPS, Configuration, Sécurité, Administration, Avancé, Paramètres SIM, Message SMS, Paramètres du réseau sans fil, Répéteur sans fil (selected), Ouverture de port / Déclenchement de port, DNS Dynamique, Routes statiques, Gestion à distance, UPnP, and Mesure de trafic. The main content area has a title bar with 'Fonction répéteur de réseau sans fil' and buttons for 'Appliquer' and 'Annuler'. Below the title bar, there is a checkbox 'Activer la fonction répéteur sans fil'. Underneath, the router's MAC address is displayed as 'Adresse MAC du réseau sans fil de ce routeur : 84:1B:5E:49:3C:BE'. There are two radio button options: 'Répéteur de réseau sans fil' and 'Station de réseau sans fil'. The 'Répéteur' option has fields for 'Adresse IP du répéteur' (192.168.0) and 'Adresse MAC de la station'. The 'Station' option has a checkbox 'Désactiver l'association de clients sans fil' and four fields for 'Adresse MAC du répéteur 1' through '4'. At the bottom, there are links for 'Centre d'aide' and 'Afficher/cacher le centre d'aide'.

- **Activer la fonction Répéteur de réseau sans fil.** Cochez la case pour le réseau de 2,4 GHz ou 5 GHz pour utiliser la fonction Répéteur de réseau sans fil.
- **Adresse MAC du réseau sans fil de ce routeur.** Ce champ affiche l'adresse MAC de votre routeur à titre de référence. Vous devez entrer cette adresse MAC dans l'écran Fonction répéteur de réseau sans fil correspondant de l'autre point d'accès que vous utilisez.
- **Répéteur de réseau sans fil.** Si votre routeur est le répéteur, sélectionnez cette case d'option.

Adresse IP du répéteur. Si votre routeur est le répéteur, entrez l'adresse IP du point d'accès.

Désactiver l'association de clients sans fil. Si votre routeur est le répéteur, cocher cette case signifie que les clients sans fil ne peuvent pas s'y associer. Seules les associations de clients du réseau local sont autorisées.

- Si vous configurez un pont point à point, cochez cette case.
- Si vous voulez que tout le trafic client passe par l'autre point d'accès (répéteur avec association clients sans fil), laissez cette case non cochée.

Adresse MAC de la station. Si votre routeur est le répéteur, entrez l'adresse MAC du point d'accès qui est la station du réseau.

- **Station de réseau sans fil.** Si votre routeur est la station du réseau, sélectionnez cette case d'option.

Désactiver l'association de clients sans fil. Si votre routeur est la station du réseau, cocher cette case signifie que les clients sans fil ne peuvent pas s'y associer. Seules les associations de clients du réseau local sont autorisées.

Adresse MAC du répéteur (1 à 4). Si votre routeur est la station du réseau, il peut agir comme le «parent» d'un maximum de 4 points d'accès. Entrez les adresses MAC des points d'accès dans ces champs.

Configurer la station du réseau

La fonction répéteur de réseau sans fil ne fonctionne que dans le mode en étoile. Les unités ne peuvent pas être connectées en série. Vous devez connaître les paramètres sans fil pour les deux unités. Vous devez connaître l'adresse MAC de l'unité distante. Tout d'abord, configurez la station du réseau, puis configurez le répéteur.

➤ Pour configurer la station du réseau :

1. Configurez les deux unités avec exactement les mêmes paramètres sans fil (SSID, mode, canal et sécurité). Notez que l'option de sécurité sans fil doit être réglée sur Aucun ou WEP.
2. Sélectionnez **AVANCÉ > Avancé > Fonction Répéteur de réseau sans fil** pour afficher l'écran Fonction répéteur de réseau sans fil.
3. Dans l'écran Fonction répéteur de réseau sans fil (selon la fréquence d'utilisation souhaitée), sélectionnez **Activer la fonction Répéteur de réseau sans fil** et sélectionnez la case d'option **Station de réseau sans fil**.

4. Entrez l'adresse MAC pour une ou plusieurs répéteurs.
5. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Configuration d'un répéteur

Utilisez une connexion Ethernet câblée pour configurer le répéteur afin d'éviter les conflits avec la connexion sans fil de la station du réseau.

Remarque : Si vous utilisez la station du réseau MBR1516 avec un Routeur qui n'est pas de NETGEAR comme répéteur, vous devrez peut-être modifier d'autres paramètres de configuration. En particulier, vous devez désactiver la fonction de serveur DHCP sur le répéteur AP sans fil.

➤ Pour configurer le routeur en tant que répéteur:

1. Connectez-vous au routeur qui sera le répéteur. Sélectionnez **DE BASE> Paramètres sans fil** et vérifiez que les paramètres sans fil correspondent exactement à l'unité de base. L'option de sécurité sans fil doit être réglée sur **WEP** ou **aucun**.
2. Sélectionnez **AVANCÉ > Avancé > Fonction Répéteur de réseau sans fil**. Sélectionnez la case **Activer la fonction répéteur sans fil** et le bouton **Répéteur de réseau sans fil**.
3. Remplissez le champ Adresse IP du répéteur. Cette adresse IP doit être dans le même sous-réseau que la station du réseau, mais doit être différente de l'adresse IP du réseau local de la station du réseau.
4. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.
5. Vérifiez la connectivité sur l'ensemble des réseaux locaux.

Un ordinateur sur n'importe quel segment de réseau local sans fil ou câblé du routeur devrait être en mesure de se connecter à Internet ou de partager des fichiers et des imprimantes avec tout autre ordinateur ou serveur sans fil ou câblé connecté au point d'accès.

Ouverture de port et déclenchement de port

Par défaut, le routeur bloque le trafic entrant depuis Internet vers vos ordinateurs à l'exception des réponses à votre trafic sortant. Vous pourriez avoir besoin de créer des exceptions à cette règle pour les fins suivantes :

- Pour permettre aux ordinateurs distants sur Internet d'accéder à un serveur sur votre réseau local.
- Pour permettre à certaines applications et jeux de fonctionner correctement lorsque leurs réponses ne sont pas reconnues par votre routeur.

Votre routeur offre deux fonctionnalités pour créer ces exceptions: l'ouverture de port et le déclenchement de port. Les sections suivantes fournissent des informations de base pour vous aider à comprendre le fonctionnement de l'ouverture de port et du déclenchement de port et les différences entre les deux fonctionnalités.

Les bases de l'accès à un ordinateur distant

Quand un ordinateur sur votre réseau doit accéder à un ordinateur sur Internet, votre ordinateur envoie à votre routeur un message contenant l'adresse source et l'adresse de destination et traiter l'information. Avant de transmettre votre message à l'ordinateur distant, votre routeur doit modifier la source d'information et créer et suivre la session de communication pour que les réponses puissent être acheminées vers votre ordinateur.

Voici un exemple de trafic sortant normal et des réponses entrantes qui en résultent :

1. Vous ouvrez un navigateur et votre système d'exploitation affecte le numéro de port 5 678 à cette session de navigation.
2. Vous entrez `http://www.exemple.com` dans le champ URL et votre ordinateur crée un message de demande de page Web avec l'adresse et les informations de port suivantes. Le message de demande est envoyé à votre routeur.

Adresse source. Adresse IP de votre ordinateur.

Numéro de port source. 5 678, qui est la session de navigation.

Adresse de destination. L'adresse IP de `www.exemple.com`, que votre ordinateur trouve en demandant à un serveur DNS.

Numéro de port de destination. 80, qui est le numéro de port standard pour un processus de services Web.

3. Votre routeur crée une entrée dans son tableau de session interne décrivant cette session de communication entre votre ordinateur et le serveur Web à l'adresse `www.exemple.com`. Avant d'envoyer le message de demande de page Web vers `www.exemple.com`, votre routeur stocke les informations d'origine, puis modifie la source d'information dans le message de demande, effectuant la traduction d'adresses réseau (NAT) :
 - L'adresse source est remplacée par l'adresse IP publique de votre routeur. Cela est nécessaire parce que votre ordinateur utilise une adresse IP privée qui n'est pas unique au monde et ne peut pas être utilisée sur l'Internet.
 - Le numéro de port source est changé pour le numéro choisi par le routeur, comme 33 333. Cela est nécessaire parce que deux ordinateurs pourraient utiliser le même numéro de session de manière indépendante.

Votre routeur envoie ensuite ce message de demande par Internet au serveur Web à l'adresse `www.exemple.com`.

4. Le serveur Web à l'adresse `www.exemple.com` compose un message de retour contenant les données des pages Web demandées. Le message de retour contient les informations d'adresse et de port suivantes. Le serveur Web envoie ensuite ce message de réponse à votre routeur.

Adresse source. L'adresse IP de `www.exemple.com`.

Numéro de port source. 80, qui est le numéro de port standard pour un processus de services Web.

Adresse de destination. L'adresse IP publique de votre routeur.

Numéro de port de destination. 33 333.

5. Dès réception du message entrant, votre routeur vérifie son tableau de session pour déterminer s'il y a une session active pour le numéro de port 33 333. Lorsqu'il trouve une session active, le routeur modifie alors le message pour restaurer les informations d'adresse d'origine remplacées par la traduction d'adresses de réseau. Votre routeur envoie ce message de réponse à votre ordinateur, qui affiche la page Web à partir de www.exemple.com. Le message contient maintenant les informations d'adresse et de port suivantes.

Adresse source. L'adresse IP de www.exemple.com.

Numéro de port source. 80, qui est le numéro de port standard pour un processus de services Web.

Adresse de destination. Adresse IP de votre ordinateur.

Numéro de port de destination. 5 678, qui est la session du navigation qui a fait la demande initiale.

6. Lorsque vous avez terminé votre session de navigation, votre routeur détecte finalement une période d'inactivité dans les communications. Votre routeur retire alors les informations de session de son tableau de session et le trafic entrant n'est plus accepté sur le numéro de port 33 333.

Du port de déclenchement aux ports entrants ouverts

Dans l'exemple précédent, les demandes sont envoyées à un ordinateur distant par votre routeur à partir d'un numéro de port de service particulier, et les réponses envoyées depuis l'ordinateur distant vers votre routeur sont dirigées vers ce numéro de port. Si le serveur distant renvoie une réponse vers un numéro de port différent, votre routeur ne le reconnaît pas et le rejette. Cependant, certains serveurs d'applications (tels que les serveurs FTP et IRC) renvoient des réponses vers plusieurs numéros de port. À l'aide de la fonction de déclenchement de port de votre routeur, vous pouvez dire à votre routeur d'ouvrir d'autres ports entrants lorsqu'un port sortant particulier est à l'origine d'une session.

Un exemple est le programme IRC (logiciel de conversation en ligne). Votre ordinateur se connecte à un serveur IRC au port de destination 6 667. Le serveur IRC ne fait pas que répondre à votre port source d'origine, il envoie également un message d'identification à votre ordinateur sur le port 113. En utilisant la fonction de déclenchement de port, vous pouvez dire au routeur : « Quand tu lances une session avec le port de destination 6 667, tu dois également autoriser le trafic entrant sur le port 113 à atteindre l'ordinateur d'origine. » En utilisant des étapes similaires à ceux de l'exemple précédent, vous pouvez voir dans la séquence suivante les effets de la règle de déclenchement de port que vous avez définie :

1. Vous ouvrez un programme client IRC pour démarrer une session de clavardage sur votre ordinateur.
2. Votre client IRC compose un message de demande à un serveur IRC en utilisant le numéro de port de destination 6 667, le numéro de port standard pour un processus de serveur IRC. Votre ordinateur envoie ensuite ce message de demande à votre routeur.

3. Votre routeur crée une entrée dans son tableau de session interne décrivant cette session de communication entre votre ordinateur et le serveur IRC. Votre routeur stocke les informations d'origine, effectue la traduction d'adresses réseau (NAT) sur le port et l'adresse sources, puis envoie ce message de demande par Internet par l'intermédiaire du serveur IRC.
4. Après avoir noté votre règle de déclenchement de port et constaté que le numéro de port de destination est 6 667, votre routeur crée une entrée de session supplémentaire pour envoyer tout trafic entrant du port 113 vers votre ordinateur.
5. Le serveur IRC envoie un message de retour à votre routeur en utilisant le port source attribué par la traduction d'adresses de réseau (comme dans l'exemple précédent, disons le port 33 333) comme port de destination. Le serveur IRC envoie également un message d'identification à votre routeur avec le port de destination 113.
6. Dès réception du message entrant au port de destination 33 333, votre routeur vérifie son tableau de session pour déterminer s'il y a une session active pour le numéro de port 33 333. Lorsqu'il trouve une session active, le routeur restaure les informations initiales sur l'adresse qui avaient été remplacées par la traduction d'adresses de réseau, puis il envoie ce message de réponse à votre ordinateur.
7. Dès réception du message entrant au port de destination 113, votre routeur vérifie son tableau de session et constate qu'il y a une session active pour le port 113 associée à votre ordinateur. Le routeur remplace l'adresse IP de destination du message par l'adresse IP de votre ordinateur et fait suivre le message vers votre ordinateur.
8. Lorsque vous avez terminé votre session de clavardage, votre routeur détecte finalement une période d'inactivité dans les communications. Votre routeur retire alors les informations de session de son tableau de session et le trafic entrant n'est plus accepté sur les numéros de port 33 333 ou 113.

Pour configurer le déclenchement de port, vous devez connaître les ports entrants requis par l'application. De plus, vous devez connaître le numéro du port sortant qui déclenchera l'ouverture des ports entrants. Vous pouvez généralement obtenir ce renseignement en communiquant avec l'éditeur de l'application ou avec des groupes d'utilisateurs ou des forums.

Remarque : Un seul ordinateur à la fois peut utiliser l'application déclenchée.

Ouverture de port pour permettre des communications d'accueil externes

Dans les deux exemples précédents, votre ordinateur démarre une session d'application avec un ordinateur serveur sur Internet. Toutefois, il vous faudra peut-être permettre à un ordinateur client sur Internet d'établir une connexion vers un ordinateur serveur sur votre réseau. Normalement, votre routeur ignore tout trafic entrant qui n'est pas une réponse à votre propre trafic sortant. Vous pouvez configurer des exceptions à cette règle par défaut en utilisant la fonction d'ouverture de port.

Une application typique de l'ouverture de port peut être démontrée en inversant la relation client-serveur à partir de l'exemple du serveur Web précédent. Dans ce cas, le navigateur

d'un ordinateur distant doit accéder à un serveur Web fonctionnant sur un ordinateur de votre réseau local. En utilisant l'ouverture de port, vous pouvez dire au routeur : « Quand tu reçois du trafic entrant sur le port 80 (le numéro de port standard pour un processus de service Web), fais-le suivre vers l'ordinateur local à l'adresse 192.168.1.123. » La séquence suivante montre les effets de la règle d'ouverture de port que vous avez définie :

1. L'utilisateur d'un ordinateur distant ouvre un navigateur et demande une page Web sur le serveur `www.exemple.com`, qui décide de l'adresse IP publique de votre routeur. L'ordinateur distant compose un message de demande de page Web avec les informations de destination suivantes :

Adresse de destination. L'adresse IP de `www.exemple.com`, qui est l'adresse de votre routeur.

Numéro de port de destination. 80, qui est le numéro de port standard pour un processus de services Web.

L'ordinateur distant envoie ensuite ce message de demande par Internet à votre routeur.

2. Votre routeur reçoit le message de demande et recherche dans sa table de règles toute règle régissant la disposition du trafic entrant de port 80. Votre règle d'ouverture de port précise que le trafic entrant du port 80 doit être transféré à l'adresse IP locale 192.168.1.123. Par conséquent, votre routeur modifie les informations de destination dans le message de demande :

L'adresse de destination est remplacée par 192.168.1.123.

Votre routeur envoie ensuite ce message de demande à votre réseau local.

3. Votre serveur Web à l'adresse 192.168.1.123 reçoit la demande et compose un message de retour contenant les données des pages Web demandées. Votre serveur Web envoie ensuite ce message de réponse à votre routeur.
4. Votre routeur effectue la traduction d'adresses réseau (NAT) sur l'adresse IP source et envoie ce message de demande par Internet à l'ordinateur distant, qui affiche la page Web depuis l'adresse `www.exemple.com`.

Pour configurer l'ouverture de port, vous devez connaître les ports entrants requis par l'application. Vous pouvez généralement obtenir ce renseignement en communiquant avec l'éditeur de l'application ou avec des groupes d'utilisateurs ou forums concernés.

En quoi l'ouverture de port diffère-t-elle du déclenchement de port ?

Les points suivants résument les différences entre l'ouverture de port et le déclenchement de port :

- Le déclenchement de port peut être utilisé par n'importe quel ordinateur sur votre réseau, même si un seul ordinateur peut l'utiliser à la fois.
- L'ouverture de port est configurée pour un seul ordinateur sur votre réseau.
- Le déclenchement de port requiert que vous connaissiez à l'avance l'adresse IP de l'ordinateur. L'adresse IP est automatiquement captée.

- L'ouverture de port requiert que vous précisiez l'adresse IP de l'ordinateur lors de la configuration, et l'adresse IP ne peut jamais changer.
- Le déclenchement de port requiert qu'un trafic sortant particulier ouvre les ports entrants, et les ports déclenchés sont fermés après une période d'inactivité.
- L'ouverture de port est toujours active et n'a pas besoin d'être déclenchée.

Configurer l'ouverture de port pour les serveurs locaux

En utilisant la fonction d'ouverture de port, vous pouvez autoriser certains types de trafic entrant à atteindre les serveurs de votre réseau local. Par exemple, vous voulez peut-être faire en sorte qu'un serveur Web local, un serveur FTP local ou un serveur de jeu local soit visible et accessible sur Internet.

Utilisez l'écran Ouverture de port pour configurer le routeur afin qu'il transmette des protocoles entrants particuliers vers les ordinateurs de votre réseau local. En plus de configurer des serveurs pour des applications particulières, vous pouvez également choisir un serveur DMZ par défaut auquel tous les autres protocoles entrants seront renvoyés.

Avant de commencer, vous devez déterminer le type de service, d'application ou de jeu que vous souhaitez offrir, ainsi que l'adresse IP locale de l'ordinateur qui fournira le service. L'ordinateur serveur doit toujours avoir la même adresse IP.

➤ Pour configurer une ouverture de port :

Conseil : Pour vous assurer que votre ordinateur serveur a toujours la même adresse IP, utilisez la fonction de réservation d'adresse IP de votre Routeur sans fil 11n LTE à haut débit mobile.

1. Sélectionnez **AVANCÉ > Avancé > Ouverture de port, déclenchement de port** pour afficher l'écran suivant :

Le bouton Ouverture de port est sélectionné comme type de service.

2. Dans la liste Nom du service, sélectionnez le service ou le jeu que vous hébergerez sur votre réseau. Si le service ne figure pas dans la liste, consultez la section [Ajouter un service personnalisé](#) à la page 187.
3. Dans le champ Adresse IP du serveur correspondant, entrez le dernier chiffre de l'adresse IP de votre ordinateur local qui fournira ce service.
4. Cliquez sur **Ajouter**. Le service apparaît dans la liste à l'écran.

Ajouter un service personnalisé

Pour définir un service, un jeu ou une application qui n'apparaît pas dans la liste Nom du service, vous devez d'abord déterminer le numéro de port ou la plage de numéros utilisés par l'application. Vous pouvez généralement obtenir ce renseignement en communiquant avec l'éditeur de l'application ou avec des groupes d'utilisateurs ou des forums.

➤ **Pour ajouter un service personnalisé :**

1. Sélectionnez **AVANCÉ > Avancé > Ouverture de port/déclenchement de port**.
2. Sélectionnez **Ouverture de port** comme type de service.
3. Cliquez sur le bouton **Ajouter un service personnalisé** pour afficher l'écran suivant :

The screenshot shows a configuration window titled 'Ports - Services personnalisés'. At the top, there are two buttons: 'Appliquer' (green) and 'Annuler' (purple). Below these are several input fields: 'Nom de service' (a text box), 'Type de service' (a dropdown menu showing 'TCP/UDP'), 'Port de début' (a text box with '1-65535' below it), 'Port de fin' (a text box with '1-65535' below it), and 'Adresse IP du serveur' (a text box with '192.168.0' below it).

4. Dans le champ Nom du service, entrez un nom descriptif.
5. Dans la liste Type de service, sélectionnez le protocole. En cas d'incertitude, sélectionnez **TCP/UDP**.
6. Dans le champ Port de début, entrez le numéro de port de début.
 - Si l'application utilise un seul port, entrez le même numéro de port dans le champ Port de fin.
 - Si l'application utilise une plage de numéros de ports, entrez le numéro de port de fin de la plage dans le champ Port de fin.
7. Dans le champ Adresse IP du serveur, entrez l'adresse IP de votre ordinateur local qui fournira ce service.
8. Cliquez sur **Appliquer**. Le service apparaît dans la liste dans l'écran Ouverture de port/déclenchement de port écran.

Modifier ou supprimer une entrée d'ouverture de port

➤ **Pour modifier ou supprimer une entrée d'ouverture de port :**

1. Dans le tableau, sélectionnez la case d'option à côté du nom du service.
2. Cliquez sur **Éditer le service** ou **Suppression de service**.

Exemple d'application : Rendre public un serveur Web local

Si vous hébergez un serveur Web sur votre réseau local, vous pouvez utiliser l'ouverture de port pour autoriser les requêtes Web de n'importe qui sur l'Internet à atteindre votre serveur Web.

➤ Pour rendre public un serveur Web local

1. Attribuez à votre serveur Web soit une adresse IP fixe, soit une adresse IP dynamique, à l'aide de la fonction de réservation d'adresse DHCP. Dans cet exemple, votre routeur donne toujours à votre serveur Web une adresse IP 192.168.1.33.
2. Dans l'écran Ouverture de port, configurez le routeur pour faire suivre le service HTTP à l'adresse locale de votre serveur Web à l'adresse **192.168.1.33**. HTTP (port 80) est le protocole standard pour les serveurs Web.
3. (Facultatif) Enregistrez un nom d'hôte avec un service de DNS dynamique et configurez votre routeur pour utiliser le nom, tel que décrit dans la section [DNS dynamique](#) à la page 191. Pour accéder à votre serveur Web à partir d'Internet, un utilisateur distant doit connaître l'adresse IP qui a été attribuée par votre FAI. Toutefois, si vous utilisez un service DNS dynamique, l'utilisateur distant peut accéder à votre serveur en utilisant un nom Internet convivial, comme mynetgear.dyndns.org.

Configurer un déclenchement de port

Le déclenchement de port est une extension dynamique de l'ouverture de port qui est utile dans les cas suivants :

- Plus d'un ordinateur local a besoin d'ouverture de port pour la même application (mais pas simultanément).
- Une application doit ouvrir des ports entrants qui sont différents du port sortant.

Lorsque le déclenchement de port est activé, le routeur surveille le trafic sortant à la recherche d'un port « déclencheur » sortant particulier. Lorsque le routeur détecte le trafic sortant sur ce port, il se souvient de l'adresse IP de l'ordinateur local qui a envoyé les données. Le routeur ouvre alors temporairement le (les) port(s) entrant(s) précisé(s) et transfère le trafic entrant sur les ports déclenchés vers l'ordinateur déclencheur.

Alors que l'ouverture de port crée un mappage statique d'un numéro de port ou d'une plage de numéros vers un seul ordinateur local, le déclenchement de port peut ouvrir des ports de manière dynamique vers n'importe quel ordinateur qui en a besoin et peut fermer les ports lorsque ceux-ci ne sont plus nécessaires.

Remarque : Si vous utilisez des applications telles que des jeux multi-joueurs, des communications poste à poste, des communications en temps réel comme la messagerie instantanée ou l'assistance à distance (une fonctionnalité de Windows XP), vous devez également activer Universal Plug and Play (UPnP) selon les instructions indiquées à la section [Service UPnP](#) à la page 195.

Pour configurer le déclenchement de port, vous devez connaître les ports entrants requis par l'application. De plus, vous devez connaître le numéro du port sortant qui déclenchera l'ouverture des ports entrants. Vous pouvez généralement obtenir ce renseignement en communiquant avec l'éditeur de l'application ou avec des groupes d'utilisateurs ou des forums.

➤ **Pour configurer un déclenchement de port :**

1. Sélectionnez **AVANCÉ > Avancé > Ouverture de port/déclenchement de port**.
2. Sélectionnez le bouton d'option **Déclenchement de port** pour afficher les informations sur le déclenchement de port.

3. Décochez la case **Désactiver le déclenchement de port** si elle est sélectionnée.

Remarque : Si la case *Désactiver le déclenchement de port* est sélectionnée après que vous ayez configuré le déclenchement de port, celui-ci est désactivé. Cependant, toute information de configuration de déclenchement de port que vous avez ajoutée au routeur est conservée même si elle n'est pas utilisée.

4. Dans le champ **Durée d'inactivité du déclenchement de port**, entrez une valeur jusqu'à 9 999 minutes.

Cette valeur commande l'horloge d'inactivité sur les ports entrants désignés. Les ports entrants se ferment lorsque le délai d'inactivité expire. Cette action est nécessaire parce que le routeur ne peut pas être sûr du moment où l'application est terminée.

5. Cliquez sur **Ajout de service** pour afficher l'écran suivant :

6. Dans le champ Nom du service, entrez un nom descriptif de service.
7. Dans la liste des utilisateurs de services, sélectionnez **Tous** (valeur par défaut) pour permettre à ce service d'être utilisé par n'importe quel ordinateur connecté à Internet. Sinon, sélectionnez **Adresse unique** et entrez l'adresse IP d'un ordinateur pour restreindre le service à un ordinateur particulier.
8. Sélectionnez le type de service, **TCP**, **UDP** ou les deux (**TCP/UDP**). En cas d'incertitude, sélectionnez TCP/UDP.
9. Dans le champ Déclenchement de port, entrez le numéro du port du trafic sortant qui provoquera l'ouverture des ports entrants.
10. Entrez les informations du port de connexion entrant dans les champs Type de connexion, Port de début et Port de fin.
11. Cliquez sur **Appliquer**. Le service apparaît sous la ligne Déclenchement de ports – Tableau des ports.

DNS dynamique

Si votre fournisseur d'accès à Internet (FAI) vous a donné une adresse IP attribuée de manière permanente, vous pouvez enregistrer un nom de domaine et le lier à votre adresse IP à l'aide d'un serveur DNS public. Toutefois, si votre compte Internet utilise une adresse IP attribuée de manière dynamique, vous ne connaissez pas à l'avance votre adresse IP et cette adresse changera régulièrement. Dans ce cas, vous pouvez utiliser un service commercial DNS dynamique. Ce type de service vous permet d'enregistrer votre nom de domaine à l'adresse IP du FAI et fait suivre le trafic dirigé vers votre domaine vers votre adresse IP qui change fréquemment.

Si votre FAI attribue une adresse WAN privée (comme 192.168.x.x ou 10.x.x.x), le service de DNS dynamique ne fonctionnera pas parce que les adresses privées ne sont pas acheminées sur Internet.

Votre routeur contient un client qui peut se connecter au service DNS dynamique fourni par DynDNS.org. Visitez d'abord le site Web à l'adresse <http://www.dyndns.org> et obtenez un compte et un nom d'hôte que vous configurez dans le routeur. Ensuite, chaque fois que votre adresse IP attribuée par le FAI change, votre routeur communique automatiquement avec le fournisseur de service DNS dynamique, se connecte à votre compte et enregistre votre nouvelle adresse IP. Si votre nom d'hôte est nomdhote, par exemple, vous pouvez atteindre votre routeur à l'adresse <http://nomdhote.dyndns.org>.

Dans l'onglet **AVANCÉ**, sélectionnez **Avancé > DNS Dynamique** pour afficher l'écran suivant :



Figure 7. Trafic envoyé à une adresse IP qui change

➤ **Pour configurer le service DNS dynamique :**

1. Inscrivez-vous pour obtenir un compte avec l'un des fournisseurs de service DNS dynamique dont les noms figurent dans la liste Fournisseur du service.
2. Cochez la case **Utiliser un service de DNS dynamique**.
3. Sélectionnez le nom de votre fournisseur du service de DNS dynamique. Par exemple, pour dyndns.org, sélectionnez **www.dyndns.org**.
4. Entrez le nom d'hôte (ou nom de domaine) que votre fournisseur de service DNS dynamique vous avez donné.
5. Entrez l'identifiant pour votre compte DNS dynamique. C'est le nom que vous utilisez pour vous connecter à votre compte, et non votre nom d'hôte.
6. Entrez le mot de passe (ou clé) de votre compte DNS dynamique.
7. Cliquez sur **Appliquer** pour enregistrer votre configuration.

Routes statiques

Les routes statiques fournissent des informations d'acheminement supplémentaires à votre routeur. Dans des circonstances habituelles, le routeur contient des informations de routage adéquates après avoir été configuré pour l'accès Internet et vous n'avez pas besoin de configurer des routes statiques supplémentaires. Vous devez configurer des routes statiques pour les cas inhabituels, par exemple lorsqu'il y a plusieurs routeurs ou plusieurs sous-réseaux IP dans votre réseau.

Le cas suivant illustre une situation où une route statique est nécessaire :

- Votre accès Internet principal se fait à l'aide d'un modem câble, vers un FAI.
- Votre réseau domestique utilise un routeur ISDN pour se connecter à l'entreprise pour laquelle vous travaillez. L'adresse de ce routeur sur votre réseau local est 192.168.0.100.
- L'adresse du réseau de votre entreprise est 134.177.0.0.

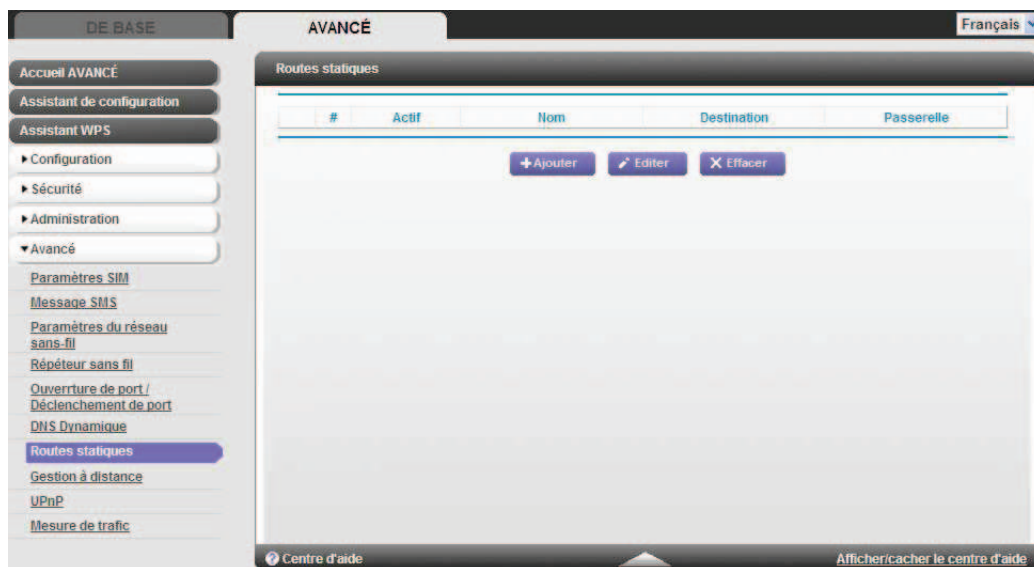
Lorsque vous avez configuré votre routeur, deux routes statiques implicites ont été créées. Une route par défaut a été créée vers votre FAI pour la passerelle et une seconde route statique a été créée pour votre réseau local, pour toutes les adresses 192.168.1.x. Avec cette configuration, si vous tentez d'accéder à un service sur le réseau 134.177.0.0, votre routeur achemine votre requête à votre FAI. Le FAI achemine votre requête vers votre employeur et la requête sera fort probablement bloquée par le pare-feu de l'entreprise.

Dans ce cas, vous devez définir une route statique, en indiquant à votre routeur que 134.177.0.0 doit être accédé par le routeur ISDN à l'adresse 192.168.1.100. Dans cet exemple :

- Les champs Adresse IP de destination et Masque de sous-réseau IP spécifient que cette route statique s'applique à toutes les adresses 134.177.x.x.
- Le champ Adresse IP de la passerelle précise que tout le trafic pour ces adresses doit être transféré vers le routeur ISDN à l'adresse 192.168.1.100.
- Une valeur métrique de 1 fonctionnera, car le routeur ISDN est sur le réseau local.
- Privée est sélectionné uniquement par mesure de précaution, en cas d'activation de RIP.

➤ **Pour configurer une route statique :**

1. Sélectionnez **AVANCÉ > Avancé > Routes statiques** pour afficher l'écran suivant :



2. Cliquez sur **Ajouter** pour afficher l'écran suivant :

3. Dans le champ Nom de la route, entrez un nom pour cette route statique (à des fins d'identification uniquement.)
4. Cochez la case **Privée** si vous désirez limiter l'accès au réseau local seulement. Si la case Privé est sélectionnée, la route statique n'est pas rapportée dans RIP.
5. Cochez la case **Actif** pour rendre cette route active.
6. Entrez l'adresse IP de la destination finale.
7. Entrez le masque de sous-réseau IP pour cette destination. Si la destination est un hôte unique, entrez **255.255.255.255**.
8. Entrez l'adresse IP de la passerelle, qui doit être un routeur sur le même segment de réseau local que le Routeur sans fil 11n LTE à haut débit mobile.
9. Entrez un nombre compris entre 1 et 15 comme valeur métrique.
Cette valeur représente le nombre de routeurs entre votre réseau et la destination.
En général, un paramètre de 2 ou 3 fonctionne, mais s'il s'agit d'une connexion directe, configurez-le à 1.
10. Cliquez sur **Appliquer** pour ajouter la route statique.

Gestion à distance

La fonction de gestion à distance vous permet de mettre à jour ou de vérifier le statut de votre Routeur sans fil 11n LTE à haut débit mobile sur Internet.

➤ Pour configurer la gestion à distance:

1. Sélectionnez **AVANCÉ** > **Avancé** > **Gestion à distance**.

The screenshot shows the 'Gestion à distance' (Remote Management) configuration page. The left sidebar contains a menu with options like 'Accueil AVANCÉ', 'Assistant de configuration', 'Assistant WPS', 'Configuration', 'Sécurité', 'Administration', 'Avancé', 'Paramètres SIM', 'Message SMS', 'Paramètres du réseau sans-fil', 'Répéteur sans fil', 'Ouverture de port / Déclenchement de port', 'DNS Dynamique', 'Routes statiques', 'Gestion à distance' (highlighted), 'UPnP', and 'Mesure de trafic'. The main content area has a title 'Gestion à distance' and buttons for 'Appliquer' and 'Annuler'. It includes a checkbox for 'Activer la gestion à distance', a text field for 'Adresse de gestion à distance' (http://0.0.0.0:8080), and radio buttons for 'Autoriser l'accès distant pour:'. The selected option is 'Tout le monde'. There are also input fields for 'De' and 'A' IP addresses, and a 'Numéro de port' field set to 8080.

Remarque : Assurez-vous de modifier le mot de passe par défaut du routeur pour un mot de passe très sécuritaire. Le mot de passe idéal ne devrait pas figurer dans un dictionnaire, quelle que soit la langue, et il devrait comporter à la fois des lettres en majuscules et en minuscules, des chiffres et des symboles. Il peut comporter jusqu'à 30 caractères.

2. Cochez la case **Activer la gestion à distance**.
3. Sous Autoriser l'accès à distance pour, sélectionnez l'étendue des adresses IP externes qui doivent être autorisées à accéder à la gestion à distance du routeur.

Remarque : Par une sécurité accrue, restreignez l'accès au plus petit nombre d'adresses IP externes que possible :

- Pour permettre l'accès à une seule adresse IP sur Internet, sélectionnez **Seulement cet ordinateur**. Entrez l'adresse IP qui permettra l'accès au réseau.
 - Pour permettre l'accès à une plage d'adresses IP sur Internet, sélectionnez **Plage d'adresses IP**. Entrez une adresse IP de début et de fin pour définir la plage permise.
 - Pour permettre l'accès à partir de n'importe quelle adresse IP sur Internet, sélectionnez **Tout le monde**.
4. Précisez le numéro de port permettant d'accéder à l'interface de gestion Web.

L'accès normal du navigateur Web utilise le port 80 du service HTTP standard. Pour plus de sécurité, entrez un numéro de port personnalisé pour l'interface de gestion Web à distance. Choisissez un nombre entre 1 024 et 65 535, mais n'utilisez pas le numéro d'un

port de service commun. La valeur par défaut est 8 080. Il s'agit d'un substitut courant pour HTTP.

5. Cliquez sur **Appliquer** pour instaurer vos modifications.
6. Lorsque vous accédez à votre routeur depuis Internet, entrez l'adresse IP WAN de votre routeur dans le champ d'adresse ou d'emplacement de votre navigateur, suivie de deux points (:) et du numéro de port personnalisé. Par exemple, si votre adresse externe est 134.177.0.123 et que vous utilisez le numéro de port 8 080, entrez **http://134.177.0.123:8080** dans votre navigateur.

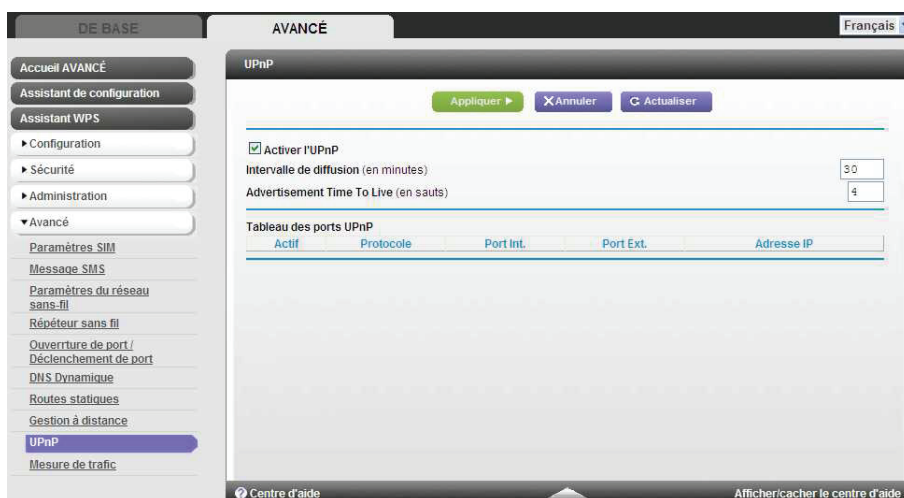
Service UPnP

L'Universal Plug and Play (UPnP) aide les périphériques tels que les ordinateurs et les appareils Internet à accéder au réseau et à se connecter à d'autres périphériques selon les besoins. Les périphériques UPnP peuvent détecter automatiquement sur le réseau les services d'autres périphériques UPnP enregistrés.

Remarque : Si vous utilisez des applications telles que des jeux multi-joueurs, des communications poste à poste ou des communications en temps réel comme la messagerie instantanée ou l'assistance à distance (une fonctionnalité de Windows XP), vous devez activer UPnP.

➤ Pour activer Universal Plug and Play :

1. Sélectionnez **AVANCÉ > Avancé > UPnP**. L'écran affiche UPnP.



2. Les paramètres et informations disponibles dans cet écran sont :

Activer l'UPnP. L'UPnP peut être activé ou désactivé pour la configuration de périphérique automatique. Par défaut, l'UPnP est désactivé. Si cette case n'est pas

cochée, le routeur ne permettra à aucun périphérique de commander automatiquement les ressources, comme l'ouverture de port (mappage), du routeur.

Intervalle de diffusion. L'intervalle de diffusion représente la fréquence à laquelle le routeur diffuse ses informations UPnP. Cette valeur peut être spécifiée entre 1 et 1 440 minutes. L'intervalle par défaut est de 30 minutes. Des intervalles inférieurs permettront aux points de contrôle d'obtenir l'état courant des périphériques, mais au prix d'un surcroît de trafic réseau. Des intervalles plus longs peuvent compromettre l'actualisation de l'état des périphériques, mais peuvent réduire de manière considérable le trafic réseau.

Durée de vie de diffusion. La durée de vie de diffusion se mesure en sauts pour chaque paquet UPnP envoyé. Le compte de sauts de durée de vie est le nombre d'étapes qu'un paquet de diffusion est autorisé à propager pour chaque diffusion UPnP avant qu'elle ne disparaisse. Le nombre de sauts peut être spécifié entre 1 et 255. La valeur par défaut de la durée de vie de diffusion est de 4 sauts, ce qui convient parfaitement à la plupart des réseaux domestiques. Si vous remarquez que certains périphériques ne sont pas correctement mis à jour ou sont difficilement accessibles, il peut être nécessaire d'augmenter cette valeur.

Tableau des ports UPnP. Le tableau des ports UPnP affiche l'adresse IP de chaque périphérique UPnP qui accède présentement au routeur et les ports (internes et externes) que le périphérique a ouverts. Le tableau des ports UPnP indique également le type de port qui est ouvert et si ce port est toujours actif pour chaque adresse IP.

3. Cliquez sur **Appliquer** pour enregistrer vos paramètres.

Mesure de trafic

Le compteur de trafic vous permet de surveiller le volume de trafic Internet qui passe par le port Internet de votre routeur. Grâce à l'utilitaire de compteur de trafic, vous pouvez configurer des limites pour le volume de trafic, configurer une limite mensuelle et obtenir une mise à jour en temps réel du trafic.

➤ Pour surveiller le trafic Internet :

1. Cliquez sur **AVANCÉ > Avancé > Mesure de trafic** pour afficher l'écran suivant :

2. Pour activer le compteur de trafic, cochez la case **Activer la mesure du trafic pour la connexion Ethernet**.
3. Si vous désirez enregistrer et restreindre le volume de trafic Internet, sélectionnez la case d'option **Volume du trafic contrôlé par...** Vous pouvez sélectionner l'une des options suivantes pour contrôler le volume de trafic :

Aucune limite. Aucune restriction n'est appliquée quand la limite de trafic est atteinte.

Téléchargement seulement. La restriction spécifiée s'applique uniquement aux données entrantes.

Dans les deux sens. La restriction spécifiée s'applique aux données entrantes et sortantes.
4. Vous pouvez limiter la quantité de trafic de données permise par mois en précisant le nombre de mégaoctets permis par mois ou en précisant le nombre d'heures de trafic permis.
5. Paramétrez le compteur de trafic pour qu'il commence à une heure et une date précise.
6. Paramétrez le contrôle de trafic pour qu'il émette un message d'avertissement avant d'atteindre la limite mensuelle de mégaoctets ou d'heures. Vous pouvez sélectionner l'une des options suivantes quand la limite est atteinte :
 - Faire clignoter la LED Internet en vert/ambré.
 - Déconnecter et désactiver la connexion Internet.
7. Paramétrez les statistiques du trafic Internet afin de surveiller le trafic de données.
8. Cliquez sur le bouton **Statut du trafic** si vous désirez une mise à jour en direct de l'état du trafic Internet sur votre routeur.
9. Cliquez sur **Appliquer** pour enregistrer vos paramètres.

Ce chapitre contient des renseignements sur le dépannage de votre Routeur sans fil 11n LTE à haut débit mobile. Après la description de chaque problème, des instructions sont fournies pour vous aider à établir un diagnostic et à corriger la situation. Pour les problèmes courants présentés, accédez à la section indiquée.

- Le routeur est-il sous tension?
Consultez la section [Fonctionnement de base](#) à la page 199.
- Le routeur est-il correctement connecté?
Consultez la section [Fonctionnement de base](#) à la page 199.
- Impossible d'accéder à la configuration du routeur à partir de mon navigateur.
Consultez la section [Dépannage de l'accès au menu principal du routeur](#) à la page 201.
- J'ai configuré le routeur mais je ne parviens pas à accéder à Internet.
Consultez la section [Dépannage de la connexion au FAI](#) à la page 202.
- J'ai configuré le routeur mais ne peux accéder à mon réseau local.
Consultez la section [Dépannage d'un réseau TCP/IP à l'aide de l'utilitaire Ping](#) à la page 204.
- Comment configurer l'heure avancée d'été?
Consultez la section [Problèmes de date et d'heure](#) à la page 206.
- J'aimerais effacer les données de configuration et recommencer entièrement la procédure.
Consultez la section [Rétablissement du mot de passe et de la configuration par défaut](#) à la page 206.

Fonctionnement de base

Une fois que le routeur est sous tension, la séquence d'événements suivante devrait se produire :

1. Après la mise sous tension initiale, vérifiez que le voyant d'alimentation est allumé.
2. Après environ une minute, assurez-vous que :
 - a. Le voyant d'alimentation reste allumé en vert. Un voyant orange vous indique que le test d'autodiagnostic de l'appareil a échoué.
 - b. Le voyant du port Internet est allumé.
 - c. Le voyant de liaison Wi-Fi est allumé. La liaison radio Wi-Fi est activée par défaut.
 - d. Le voyant des ports de réseau local est allumé lorsqu'un des ports locaux est connecté.

Si le voyant de port de réseau local est allumé sur le panneau arrière de l'unité, une liaison a été établie au périphérique connecté. Si un port de réseau local est connecté à un périphérique de 100 Mbit/s, vérifiez que son voyant est allumé en vert. S'il s'agit d'un port de 10 Mbit/s, le voyant doit être orange.

- e. Le voyant de port de réseau étendu (WAN) est allumé lorsque le routeur est connecté à un modem filaire.
- f. Le voyant de qualité du signal est allumé lorsque le routeur a détecté un signal haut débit mobile.

Si l'une ou l'autre de ces conditions n'est pas respectée, veuillez consulter le tableau suivant.

Voyant		Action
Alimentation 	Le voyant d'alimentation est éteint.	- Assurez-vous que le cordon d'alimentation est bien raccordé à votre routeur et que l'adaptateur secteur est correctement branché à une prise de courant fonctionnant normalement. - Assurez-vous d'utiliser l'adaptateur secteur fourni par NETGEAR avec ce produit. Si l'erreur persiste, cela signifie que le problème peut provenir de votre matériel. Communiquez alors avec le soutien technique.
	Le voyant d'alimentation est orange.	La défaillance se situe du côté du routeur. Essayez de corriger le problème comme suit : - Éteignez le routeur, puis rallumez-le et vérifiez qu'il s'active. - Rétablissez la configuration par défaut du routeur. L'adresse IP du routeur devient www.routerlogin.net. Cette procédure est décrite dans la section Rétablissement du mot de passe et de la configuration par défaut à la page 206. Si l'erreur persiste, cela signifie que le problème peut provenir de votre matériel. Communiquez alors avec le soutien technique.

Voyant		Action
Port Internet 	Le voyant de port Internet est éteint.	Assurez-vous que la carte SIM reçue est insérée dans le routeur. Les cartes SIM provenant d'autres appareils ne fonctionneront pas avec le routeur et cette carte SIM ne fonctionnera pas avec d'autres périphériques.
	Le voyant de port Internet est orange.	Le routeur ne peut pas se connecter à Internet. Vérifiez l'option de connexion Internet sélectionnée. • Pour l'option de connexion haut débit mobile, vérifiez les voyants de qualité du signal. • Pour l'option de connexion Ethernet, vérifiez le voyant du port de réseau étendu (WAN).
	Le voyant de port Internet clignote en orange et en vert.	La fonction de mesure du trafic est activée et la limite établie a été atteinte.
Wi-Fi 	Le voyant de liaison Wi-Fi est éteint.	La liaison radio Wi-Fi est désactivée. Si vous voulez établir une connexion Wi-Fi avec le routeur, appuyez sur le bouton Wi-Fi pour réactiver la liaison radio Wi-Fi.
	Le voyant de liaison Wi-Fi ne clignote pas.	Si ce voyant ne clignote pas lorsque vous tentez de transmettre des données par liaison Wi-Fi, accédez au menu du routeur en utilisant la connexion Ethernet de réseau local et vérifiez la configuration de connexion sans fil (Wi-Fi) de votre routeur.
Ports de réseau local 	Le voyant des ports de réseau local est éteint.	Si ce voyant ne s'allume pas lorsqu'une connexion Ethernet est établie, vérifiez les points suivants : • Assurez-vous que le câble Ethernet est correctement branché au routeur et au concentrateur ou au poste de travail. • Assurez-vous que le concentrateur ou le poste de travail connecté est sous tension.
Port WAN 	Le voyant de réseau étendu (WAN) est éteint.	Si ce voyant ne s'allume pas lorsqu'une connexion Ethernet est établie au moyen de l'option de connexion Ethernet, vérifiez les points suivants : • Assurez-vous que le câble Ethernet est correctement branché au routeur et au modem. • Assurez-vous que le modem est sous tension.
Qualité du signal 	Le voyant de qualité du signal est éteint.	Si ce voyant ne s'allume pas lorsque la connexion haut débit mobile est utilisée, vérifiez les points suivants : • Vérifiez auprès de votre FAI si la couverture est bonne dans votre zone. • Assurez-vous que votre compte haut débit mobile est actif. • Assurez-vous que la carte SIM est correctement insérée dans le routeur. • Placez le routeur près d'une fenêtre ou à un endroit différent. Assurez-vous qu'un des voyants de qualité du signal est allumé, ce qui vous indique qu'une couverture haut débit mobile est disponible pour le routeur. • Accédez au menu du routeur et vérifiez la configuration Internet. Vérifiez auprès du FAI si le nom d'utilisateur (identifiant), le mot de passe et le nom du point d'accès sont correctement définis. Si vous utilisez un code PIN pour établir la connexion à Internet, assurez-vous que ce code est correctement entré.

Dépannage de l'accès au menu principal du routeur

Si vous ne parvenez pas à accéder au menu principal du routeur à partir d'un ordinateur de votre réseau local, vérifiez les points suivants :

- Si vous utilisez un ordinateur connecté à un réseau Ethernet, vérifiez la connexion Ethernet entre l'ordinateur et le routeur en suivant la procédure décrite à la section précédente.
- Assurez-vous que l'adresse IP de votre ordinateur comporte le même sous-réseau que celui du routeur. Si vous utilisez le schéma d'adressage recommandé, l'adresse de votre ordinateur doit être comprise entre 192.168.0.2 et 192.168.0.254.

Remarque : Si l'adresse IP de votre ordinateur correspond à 169.254.x.x :
Les versions récentes de Windows et de Mac OS génèrent et attribuent une adresse IP lorsque l'ordinateur ne parvient pas à se connecter à un serveur DHCP. Les adresses générées automatiquement sont comprises dans la plage d'adresses 169.254.x.x. Si votre adresse IP est dans cette plage, vérifiez que le routeur est bien connecté à l'ordinateur et redémarrez ce dernier.

- Si l'adresse IP du routeur a été modifiée et que vous ne connaissez pas l'adresse IP actuelle, rétablissez les paramètres par défaut du routeur. L'adresse IP du routeur devient www.routerlogin.net. Cette procédure est décrite dans la section [Rétablissement du mot de passe et de la configuration par défaut](#) à la page 206.
- Assurez-vous que Java, JavaScript ou ActiveX sont activés dans votre navigateur. Si vous utilisez Internet Explorer, cliquez sur **Actualiser** pour vous assurer que l'applet Java est chargé.
- Essayez de fermer le navigateur puis de le rouvrir.
- Assurez-vous d'utiliser les renseignements de connexion adéquats. Le nom de connexion par défaut est **admin** et le mot de passe par défaut est **password**. Assurez-vous que le verrouillage des majuscules n'est pas activé.

Si le routeur n'enregistre pas les modifications que vous avez apportées depuis l'interface de gestion Web, vérifiez les points suivants :

- Lorsque vous modifiez les paramètres de configuration, n'oubliez pas de cliquer ensuite sur le bouton **Appliquer** avant de passer à un autre écran ou à un autre onglet, sans quoi vos modifications seront perdues.
- Cliquez sur le bouton **Actualiser** ou **Recharger** du navigateur Web. Il est possible que les modifications aient été appliquées mais que le navigateur Web affiche l'ancienne configuration stockée dans la mémoire cache.

Dépannage de la connexion au FAI

Si vous éprouvez des difficultés à vous connecter à Internet ou à naviguer sur Internet, vérifiez les causes possibles ci-dessous.

Connexion à Internet

Si vous ne parvenez pas à vous connecter à Internet, vérifiez les points suivants :

1. Le compte Internet doit être actif.

Si votre FAI vous a remis une carte SIM et que vous ne l'avez pas encore insérée dans la fente de carte SIM à l'arrière du routeur, faites-le maintenant.

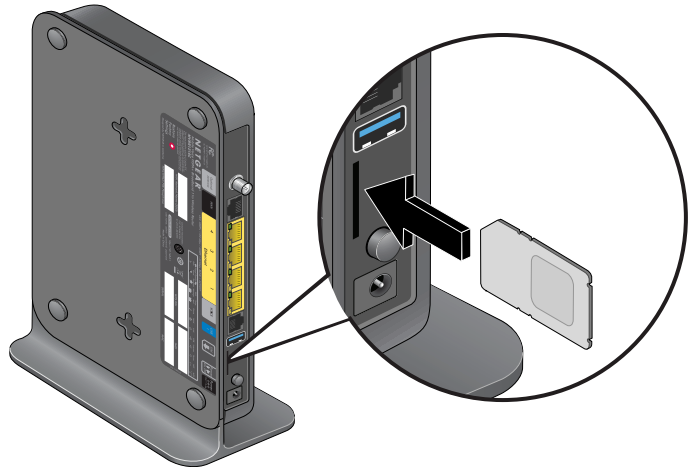
2. Une couverture haut débit sans fil doit être disponible à l'endroit où se trouve l'appareil.

3. Accédez au menu principal du routeur pour vérifier si les paramètres de connexion haut débit sont exacts. Si vous n'en êtes pas certain, informez-vous auprès de votre FAI.

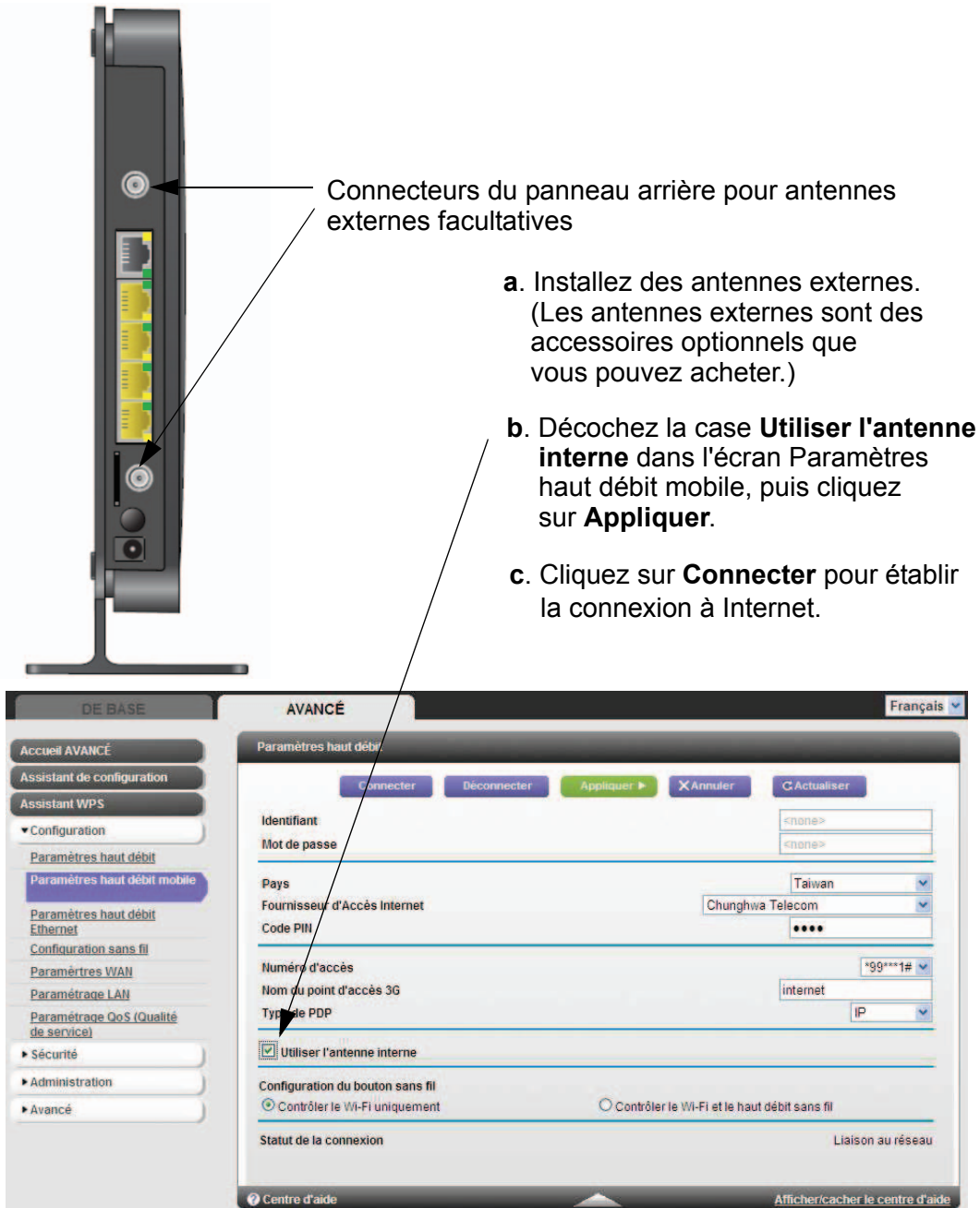
4. Vérifiez l'emplacement du routeur.

a. Rapprochez le routeur d'une fenêtre afin d'améliorer la réception du signal Internet. Un voyant de qualité du signal éteint indique qu'il n'y a aucune couverture.

b. Maintenez les distances minimum recommandées entre l'équipement NETGEAR et les appareils électroménagers afin de réduire les interférences.



5. Utilisez des antennes externes pour augmenter la puissance du signal.



Connecteurs du panneau arrière pour antennes externes facultatives

- a. Installez des antennes externes.
(Les antennes externes sont des accessoires optionnels que vous pouvez acheter.)
- b. Décochez la case **Utiliser l'antenne interne** dans l'écran Paramètres haut débit mobile, puis cliquez sur **Appliquer**.
- c. Cliquez sur **Connecter** pour établir la connexion à Internet.

DE BASE AVANCÉ Français

Accueil AVANCÉ
Assistant de configuration
Assistant WPS
▼ Configuration
Paramètres haut débit
Paramètres haut débit mobile
Paramètres haut débit Ethernet
Configuration sans fil
Paramètres WAN
Paramétrage LAN
Paramétrage QoS (Qualité de service)
► Sécurité
► Administration
► Avancé

Paramètres haut débit mobile

Connecter Déconnecter Appliquer Annuler Actualiser

Identifiant <none>
Mot de passe <none>

Pays Taiwan
Fournisseur d'accès Internet Chunghwa Telecom
Code PIN ****

Numéro d'accès *99***1#
Nom du point d'accès 3G internet
Type de PDP IP

☒ Utiliser l'antenne interne

Configuration du bouton sans fil
☒ Contrôler le Wi-Fi uniquement
☐ Contrôler le Wi-Fi et le haut débit sans fil

Statut de la connexion Liaison au réseau

Centre d'aide Afficher/cacher le centre d'aide

Dépannage de la navigation Internet

Si votre routeur obtient une adresse IP mais que votre ordinateur ne parvient pas à charger de pages Web depuis Internet :

- La mesure de trafic est activée et la limite établie a été atteinte.

Vous pouvez rétablir l'accès Internet si vous configurez la mesure de trafic de manière à ne pas désactiver (bloquer) la connexion. Cependant, si votre compte est assorti d'une limite d'utilisation, il est possible que votre FAI vous facture des frais de dépassement de limite.

- Il se peut que votre ordinateur ne reconnaisse pas les adresses du serveur DNS.

Un serveur DNS est un hôte Internet qui remplace les noms Internet (comme une adresse www) par des adresses IP numériques. En règle générale, votre fournisseur d'accès indique les adresses d'un ou de deux serveurs DNS que vous pouvez utiliser. Si vous avez entré une adresse DNS durant la configuration du routeur, redémarrez l'ordinateur et vérifiez cette adresse. Vous pouvez également configurer manuellement votre ordinateur avec ces adresses DNS, comme expliqué dans la documentation de votre système d'exploitation.

- Il se peut que le routeur ne soit pas configuré dans votre ordinateur en tant que routeur TCP/IP.

Si votre ordinateur obtient les données du routeur par l'intermédiaire du serveur DHCP, redémarrez-le et vérifiez l'adresse du routeur.

Dépannage d'un réseau TCP/IP à l'aide de l'utilitaire Ping

La plupart des routeurs et périphériques terminaux TCP/IP contiennent un utilitaire Ping qui envoie un paquet d'appel écho au périphérique désigné. Le périphérique peut alors répondre en envoyant une réponse par écho. Vous pouvez facilement résoudre les problèmes de réseau TCP/IP en vous servant de l'utilitaire Ping de votre ordinateur.

Vérification de la connexion entre le réseau local et votre routeur

Vous pouvez lancer un test Ping vers le routeur depuis votre ordinateur afin de vérifier que la connexion au réseau local est correctement configurée sur le routeur.

- **Pour effectuer un Ping sur le routeur à partir d'un ordinateur sous Windows 95 ou une version plus récente :**
 1. Dans la barre d'outils Windows, cliquez sur le bouton **Démarrer** et choisissez **Exécuter**.
 2. Dans le champ qui apparaît, entrez **ping** suivi de l'adresse IP du routeur, comme dans l'exemple suivant :

```
ping 192.168.0.1
```


3. Cliquez sur OK.

Un message comme celui-ci devrait apparaître :

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

Si la connexion est établie, le message suivant apparaît :

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

Si la connexion échoue, le message suivant apparaît :

```
Request timed out
```

Si la connexion n'est pas établie, cela peut être dû à l'un des problèmes suivants :

- Mauvaises connexions physiques
 - Assurez-vous que le voyant des ports de réseau local est allumé. Si le voyant est éteint, suivez les instructions de la section [Connexion à Internet](#) à la page 202.
 - Assurez-vous que les voyants de liaison correspondants sont allumés pour votre carte d'interface réseau et pour les ports du concentrateur qui sont connectés à votre poste de travail et au routeur (le cas échéant).
- Mauvaise configuration réseau
 - Vérifiez que le logiciel pilote de la carte Ethernet et le logiciel TCP/IP sont bien installés et configurés sur votre ordinateur ou poste de travail.
 - Vérifiez que l'adresse IP de votre routeur et de votre poste de travail sont exactes et que celles-ci sont font partie du même sous-réseau.

Vérification de la connexion entre l'ordinateur et un périphérique distant

Après vous être assuré que la connexion entre le réseau local et le routeur est active, vérifiez la connexion entre l'ordinateur et un périphérique distant.

➤ **Pour vérifier la connexion :**

1. Dans la barre d'outils Windows, cliquez sur le bouton **Démarrer** et choisissez **Exécuter**.
2. Dans la fenêtre Exécuter, tapez :

```
ping -n 10 adresse IP
```

où *adresse IP* correspond à l'adresse IP d'un périphérique distant, tel que le serveur DNS de votre fournisseur d'accès.

Si la connexion est établie, les messages mentionnés à la section précédente apparaissent. Si vous n'obtenez aucun message :

- Vérifiez que votre ordinateur et le routeur configuré comme routeur par défaut ont la même adresse IP. Si les paramètres IP de votre ordinateur sont configurés par DHCP, ces renseignements n'apparaîtront pas dans le panneau de configuration réseau de l'ordinateur. Vérifiez que l'adresse IP du routeur apparaît en tant que routeur par défaut.

- Assurez-vous que l'adresse réseau de votre ordinateur (la partie de l'adresse IP spécifiée par le masque de sous-réseau) est différente de l'adresse réseau du périphérique distant.
- Assurez-vous que le modem câble ou DSL est connecté et en état de marche.
- Si votre fournisseur d'accès a attribué un nom d'hôte à votre ordinateur, entrez ce nom d'hôte en tant que nom de compte dans l'écran Paramètres de base.
- Votre FAI pourrait rejeter les adresses MAC Ethernet de tous vos ordinateurs sauf un. De nombreux FAI haut débit limitent l'accès en autorisant uniquement le trafic provenant de l'adresse MAC de votre modem haut débit, mais certains FAI limitent encore davantage l'accès en autorisant l'adresse MAC d'un seul ordinateur connecté au modem. Dans ce cas, vous devez configurer votre routeur de manière à cloner ou à usurper l'adresse MAC de l'ordinateur autorisé.

Problèmes de date et d'heure

L'écran E-mail affiche la date et l'heure actuelles. Le Routeur sans fil 11n LTE à haut débit mobile utilise le protocole de synchronisation réseau NTP pour obtenir l'heure actuelle d'un des nombreux serveurs temporels réseau sur Internet. Chaque entrée de journal est estampillée avec la date et l'heure en cours. Voici quelques problèmes éventuels concernant la fonction de date et heure :

- La date affichée est le 1er janvier 2000.
Cause : Le routeur n'a pas réussi à communiquer avec un serveur temporel réseau. Assurez-vous que les paramètres d'accès Internet sont correctement configurés. Si vous venez de terminer la configuration du routeur, attendez au moins cinq minutes et revérifiez la date et l'heure.
- Il existe un décalage d'une heure.
Cause : Le routeur ne détecte pas automatiquement l'heure avancée d'été. Dans l'écran E-mail, cochez ou décochez la case **Ajuster automatiquement l'heure d'été**.

Rétablissement du mot de passe et de la configuration par défaut

Cette section explique comment restaurer les paramètres de configuration par défaut du routeur, afin de rétablir le mot de passe d'administrateur **password** et l'adresse IP **www.routerlogin.net**. Vous pouvez effacer les paramètres de configuration actuels et rétablir les paramètres par défaut de deux manières :

- Utilisez la fonction Effacer (consultez la section [Effacer](#) à la page 168).
- Appuyez pendant six secondes sur le bouton de **réinitialisation des paramètres d'usine** situé au bas du routeur. Utilisez cette méthode lorsque vous ne connaissez pas l'adresse IP ou le mot de passe de l'administrateur.

Les paramètres par défaut sont indiqués à la section [Paramètres par défaut d'usine](#) à la page 208.

Informations complémentaires



La présente annexe fournit les renseignements suivants :

- *Paramètres par défaut d'usine*
- *Caractéristiques techniques*

Paramètres par défaut d'usine

Appuyez sur le bouton de réinitialisation au bas du routeur pour rétablir tous les paramètres à leurs valeurs par défaut d'usine. Cette procédure est appelée réinitialisation à froid. Pour effectuer une réinitialisation à froid, maintenez enfoncé le **bouton de réinitialisation** pendant six secondes. Les paramètres du routeur sont rétablis à leurs valeurs par défaut d'usine (présentées dans le tableau suivant).

Fonction		Valeur par défaut
Connexion au routeur	Adresse de connexion de l'utilisateur	http://192.168.0.1
	Nom d'utilisateur (sensible à la casse)	admin
	Mot de passe de connexion (sensible à la casse)	password
Connexion Internet	Adresse MAC (réseau étendu)	Utilise l'adresse par défaut
	Unité de transfert maximale (MTU) de réseau étendu (WAN)	1 500
	Vitesse de port	Compatible automatique
Réseau local (LAN)	IP de réseau local	www.routerlogin.net
	Masque de sous-réseau	255.255.255.0
	Direction RIP	Aucune
	Version RIP	Désactivée
	Authentification RIP	Aucune
	Serveur DHCP	Activée
	Adresse IP de début DHCP	192.168.0.2
	Adresse IP de fin DHCP	192.168.0.254
	Zone démilitarisée (DMZ)	Désactivée
	Fuseau horaire	PST (Heure du Pacifique) pour l'Amérique du Nord
	Ajustement à l'heure avancée	Activé
Pare-feu	Communications entrantes provenant d'Internet	Désactivées (sauf sur le port 80, le port HTTP)
	Communications sortantes en direction d'Internet	Activées (toutes)
	Filtrage MAC source	Désactivé

Routeur sans fil 11n LTE à haut débit mobile MBR1516

Fonction (suite)		Valeur par défaut (suite)
Modem haut débit mobile	Fournisseur d'accès Internet	Bell Mobilité
	Nom du point d'accès 3G	inet.bell.ca
	Numéro d'accès	*99#
	Type de PDP	IP
	Nom d'utilisateur	Aucun requis
WiFi	Communications sans fil	Activées
	SSID name (Nom de réseau sans fil (SSID))	Voir l'étiquette au bas du routeur
	Sécurité	Mode mixte WPA-PSK/WPA2-PSK
	Diffusion du nom de réseau sans fil	Activée
	Vitesse de transmission	Auto (Vitesse maximale du signal sans fil conformément à la norme IEEE 802.11. Le débit réel peut varier. L'état du réseau et les conditions d'utilisation, notamment le volume du trafic, les matériaux et la structure du bâtiment ainsi que le surdébit du réseau, diminuent la vitesse de transmission des données.)
	Pays/région	Canada
	Canal radio	Automatique
	Mode de fonctionnement	Jusqu'à 145 Mbit/s
	Débit de transfert de données	Optimal
	Puissance de sortie	Maximale
	Point d'accès	Activé
	Type d'authentification	Système ouvert
	Liste d'accès de cartes sans fil	Toutes les stations sans fil permises

Caractéristiques techniques

Caractéristiques techniques	
Protocole réseau et normes	TCP/IP, DHCP
Adaptateur secteur	- Amérique du Nord : 120 V CA, 60 Hz, entrée 12 V CC / 2,5 A
Caractéristiques physiques	- Dimensions : 6,8 po x 5,03 po x 1,28 po (173 mm x 128 mm x 33 mm) - Poids : 0,65 lb (0,29 kg) sans support
Spécifications environnementales	- Températures de fonctionnement : de 0 °C à 40 °C (de 32 °F à 104 °F) - Humidité de fonctionnement : humidité relative de 90 % maximum, hors condensation
Émissions électromagnétiques	Article 15 de la FCC, classe B; IC, EN 55 022 (CISPR 22), classe B
Caractéristiques d'interface	- Réseau local (LAN) : 10BASE-T ou 100BASE-Tx, RJ-45 - WAN : 10BASE-T ou 100BASE-Tx, RJ-45
Connexion de l'antenne (facultative)	Connecteur SMA

Avis de conformité



Routeurs sans fil, passerelles et points d'accès NETGEAR

Déclaration de conformité

Remarque : Cette section décrit les exigences que doit respecter l'utilisateur concernant l'utilisation de ce produit conformément aux lois et règlements nationaux en matière d'utilisation du spectre des radiofréquences et des appareils radio. Le non-respect par l'utilisateur final des exigences applicables peut entraîner un fonctionnement illégal et une action en justice contre l'utilisateur final par les autorités réglementaires nationales.

Remarque : Le fonctionnement du micrologiciel (firmware) de ce produit est limité aux canaux permis dans une région ou un pays donné. Par conséquent, certaines options décrites dans le présent guide pourraient ne pas être disponibles dans votre version du produit.

Exigences de la FCC concernant l'utilisation du produit aux États-Unis

Information de la FCC destinée à l'utilisateur

Ce produit ne contient aucune pièce pouvant être réparée par l'utilisateur et il doit être utilisé uniquement avec les antennes approuvées. Tout changement ou modification du produit annulera l'ensemble des certifications et approbations réglementaires applicables.

Directives de la FCC concernant l'exposition des personnes

Cet appareil est conforme aux limites d'exposition aux rayonnements de la FCC pour un environnement non contrôlé. Il doit être installé de façon à garder une distance minimale de 20 centimètres entre la source de rayonnements et votre corps.

L'émetteur ne doit pas être colocalisé ni fonctionner conjointement avec une autre antenne ou un autre émetteur.

Déclaration de conformité à la FCC

Nous, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, déclarons sous notre responsabilité exclusive que le Routeur sans fil 11n LTE à haut débit mobile MBR1516 est conforme à la Section 15, Sous-section B, des règlements FCC CFR47. Son fonctionnement est sujet aux deux conditions suivantes :

- Cet appareil ne doit pas provoquer d'interférences nuisibles; et
- Cet appareil doit accepter toutes les interférences reçues, y compris celles pouvant causer un fonctionnement indésirable.

Avertissements et directives en matière de brouillage radioélectrique de la FCC

Cet appareil a été testé et certifié conforme aux restrictions pour les appareils numériques de Classe B, conformément à l'article 15 de la réglementation de la FCC. Ces restrictions visent à garantir une protection suffisante contre les interférences nuisibles dans une installation à domicile. Cet appareil utilise et peut diffuser des fréquences radio. S'il n'est pas installé et utilisé conformément aux instructions, il peut provoquer des interférences nuisibles aux communications radio. Cependant, il se peut que des interférences se produisent dans une installation particulière. Pour déterminer si cet appareil produit des interférences nuisibles à la réception de la radio ou de la télévision, éteignez puis rallumez l'appareil. Si c'est le cas, nous vous recommandons de suivre les instructions ci-dessous pour éliminer les interférences :

- Réorientez l'antenne de réception.
- Éloignez davantage l'appareil du récepteur.
- Branchez l'appareil sur un circuit électrique différent de celui où le récepteur radio est branché.
- Consultez le vendeur ou un technicien expérimenté pour obtenir de l'aide.

Mise en garde de la FCC

- Les changements ou modifications non expressément approuvées par les autorités compétentes en matière de conformité peuvent priver l'utilisateur du droit d'utiliser l'équipement en question.
- Cet appareil est conforme aux limites imposées par la Section 15 de la réglementation FCC. Son fonctionnement est sujet aux deux conditions suivantes : (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.
- Pour les produits commercialisés aux États-Unis, seuls les canaux 1 à 11 peuvent être utilisés. La sélection d'autres canaux n'est pas possible.
- Cet appareil et son antenne (ou ses antennes) ne doivent pas être colocalisés ni fonctionner conjointement avec une autre antenne ou un autre émetteur.

Règlement sur le brouillage radioélectrique du ministère des Communications du Canada

Cet appareil numérique (Routeur sans fil 11n LTE à haut débit mobile MBR1516) ne dépasse pas les limitations de la classe B en matière de transmission de bruit radioélectrique des appareils numériques, qui sont établies dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

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

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

Industrie Canada

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE: Radiation Exposure Statement:

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

Attention :

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. 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.

REMARQUE IMPORTANTE : Déclaration d'exposition aux radiations :

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

Tableau de réduction du brouillage

Le tableau ci-dessous montre la distance minimale recommandée entre l'appareil NETGEAR et les appareils électroménagers afin de réduire les interférences (indiquée en mètres et en pieds).

Appareil électroménager	Distance minimale recommandée (en mètres et en pieds)
Fours à micro-ondes	9 mètres / 30 pieds
Interphones de surveillance – analogiques	6 mètres / 20 pieds
Interphones de surveillance – numériques	12 mètres / 40 pieds
Téléphone sans fil – analogiques	6 mètres / 20 pieds
Téléphone sans fil – numériques	9 mètres / 30 pieds
Appareils Bluetooth	6 mètres / 20 pieds
Appareils ZigBee	6 mètres / 20 pieds

Index

A

- accès
 - consultation des journaux **167**
 - distant **194**
- accès à un ordinateur distant **182**
- adresse IP de la passerelle **129**
- adresse MAC **206**
- adresses de serveur de nom de domaine (DNS) **129**, **163**, **164**
- adresses DNS principales **129**
- adresses IP
 - actuelles **163**, **164**
 - DHCP **122**
 - dynamiques **191**
 - réservées **150**
- adresses IP réservées **150**
- adresses IP
 - générées automatiquement **201**
- alertes, envoi de courriel **161**
- antenne **118**
- Appuyez
 - vous êtes connecté **126**
- assistant de configuration **139**
- authentification, requise par le serveur de messagerie **161**

B

- bail, DHCP **166**
- blocage
 - mots clefs **157**
 - services **158**
 - sites **157**
 - trafic entrant **181**
- bouton Wi-Fi **115**, **200**
- bouton WPS **115**, **126**
- boutons de commande **114**

C

- calendrier de blocage de mots clefs et de services **160**
- canal sans fil **131**

- carte SIM **118**
- code PIN de sécurité **141**
- configuration
 - déclenchement de port **188**
 - DNS dynamique **191**
 - NAT **144**
 - ouverture de port **186**
 - répéteurs **181**
 - serveur DMZ **145**
 - services définis par l'utilisateur **158**
- conformité **211**
- connexion **122**, **124**
- connexion Internet, configuration **128**
- connexion sans fil **120**
- connexions sans fil **120**
- consultation
 - état du routeur **163**
 - journaux **167**
- contenu de l'emballage **113**
- contrôles parentaux **133**

D

- date et heure **206**
- déclenchement de port **181**, **183**, **186**, **188**
- délai de déconnexion, déclenchement de port **190**
- dépannage **198**
- description des voyants **115**
- dispositifs connectés **132**
- DNS dynamique **191**
- DNS secondaires **129**
- durée de vie, intervalle de diffusion **196**
- DynDNS.org **191**

E

- envoi de journaux par courriel **161**
- état du port **165**
- état du routeur, consultation **163**
- état, routeur, consultation **163**
- étiquette, produit **117**

F

fichier de configuration **167**, **168**
 filtrage de port **158**
 fournisseur d'accès Internet (FAI)
 écran Internet Setup (Configuration Internet) **128**

G

Genie, NETGEAR **122**
 gestion à distance **194**
 gestion à distance du routeur **194**

H

heure **206**
 heure avancée d'été **206**
 hôte approuvé **157**
 hôte, approuvé **157**

I

installation avec l'assistant de configuration **139**
 installation de NETGEAR Genie **122**
 interface du routeur, description **125**
 intervalle d'interrogations **165**
 intervalle de diffusion **196**
 intervalle, interrogations **165**
 IRC (Internet Relay Chat) **183**

J

journaux
 consultation **167**
 envoi de courriel **161**

L

longueur de la fragmentation **176**

M

marques de commerce **108**
 masque de sous-réseau **163**, **164**
 masque de sous-réseau IP **163**, **164**
 menus, description **125**
 mesure de trafic **196**
 micrologiciel (firmware), mise à niveau **124**, **171**, **172**
 mise à niveau du micrologiciel (firmware) **124**, **171**, **172**
 mode de préambule **176**
 mode sans fil **131**
 mot de passe, rétablissement **206**

mots clefs **157**
 multidiffusion **148**

N

NAT (traduction d'adresses de réseau) **144**
 NAT (traductions d'adresses de réseau) **145**, **182**
 NETGEAR Genie **122**
 nom de l'hôte **128**
 nom du réseau sans fil (SSID)
 description **131**
 diffusion **131**
 notifications par courriel **161**
 numéros de port **158**

O

ouverture de port **181**, **185**, **186**

P

panneau arrière **116**
 panneau avant **114**, **199**
 paquets de données fragmentés **145**
 paquets de données, fragmentés **145**
 paquets, fragmentés **145**
 paramètre de langue **139**
 paramètre de pays **139**
 paramètres d'usine par défaut, rétablissement **168**
 paramètres de connexion haut débit **142**
 paramètres de maintenance **162**
 paramètres de pare-feu **156**
 paramètres de réseau sans fil **131**
 paramètres DHCP **164**
 paramètres haut débit mobile **142**
 paramètres LAN **147**
 paramètres par défaut **117**, **208**
 paramètres par défaut d'usine, rétablissement **168**
 paramètres sans fil **130**
 diffusion SSID **131**
 paramètres WAN **144**
 passerelle par défaut **166**
 passerelle, par défaut **166**
 périphériques sans fil, ajout au réseau **126**
 phrases d'authentification, modification **132**
 points d'accès **178**
 portée des connexions sans fil **120**
 ports, LAN et WAN **115**, **200**
 positionnement du routeur **120**
 priorité du trafic **151**

protection des attaques de déni de service **156**
protocole de synchronisation réseau (NTP) **206**

Q

QoS (qualité de service) **151**
qualité du signal **116, 200**

R

radio sans fil **176**
radio, sans fil **176**
récupération du mot de passe d'administrateur **169**
récupération du mot de passe, administrateur **169**
répéteurs **181**
répétition de réseau sans fil **178, 179**
 répéteur **181**
 station **180**
réseau TCP/IP, dépannage **204**
réservation d'adresses **150**
rétablissement
 fichier de configuration **168**
 paramètres par défaut d'usine **117, 168**
routes statiques **192**

S

sauvegarde de la configuration **168**
sécurité **130, 156**
sécurité prédéfinie
 à propos de **130**
 phrase d'authentification **132**
serveur de messagerie sortant **161**
serveur de messagerie, sortant **161**
serveur DMZ **145**
serveur DMZ par défaut **145**
serveur SMTP **161**
serveur DHCP **149, 166**
serveur DMZ **145**
serveurs DNS **182**
serveurs locaux, ouverture de port vers **186**
service personnalisé (ouverture de port) **187**
services définis par l'utilisateur **158**
services Internet, blocage d'accès **158**
services, blocage **158**
seuil CTS/RTS **176**
sites, blocage **157**
SMS (Short Message Service), configuration **137**
soutien technique **108**
SSID, description **131**
station, configuration **180**

suppression de la configuration **168**
système de distribution sans fil **178, 179**

T

tableau de bord **125**
taille de l'unité de transfert maximale (MTU) **145**
temps de disponibilité du système **165**
temps de disponibilité, système **165**
trafic entrant, autorisation ou blocage **181**
trafic, priorité **151**

U

Universal Plug and Play (service UPnP) **195**

V

valeur des mesures **193**
vérification automatique du micrologiciel
 (firmware) **171, 172**
version du micrologiciel (firmware) **163**
voyant d'alimentation **115, 199**
voyant de port Internet **115, 200**
voyant de port WAN **115, 200**
voyant SMS **116**
voyant Wi-Fi **115**
voyants d'état **114, 199**

W

WMM (Wi-Fi Multimedia) **151**
WPS (Wi-Fi Protected Setup) **126, 140**