



4G LTE ROUTER  
MBR1515L

Guía del  
Usuario



4G LTE Router MBR1515L User Guide

OM1515WRev.00



User Guide

4G LTE ROUTER  
MBR1515L

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.

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. NETGEAR, Inc. All rights reserved.

## **Technical Support**

To register your product, get the latest product updates, get support online, or for more information about the topics covered in this manual, visit the Verizon Support website at:

[http://support.verizonwireless.com/contact\\_us/](http://support.verizonwireless.com/contact_us/)

## **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.

# Table of Contents

## Chapter 1 Basic Setup and Traffic Meter

Assemble the Router	7
Place the Router	9
Optional: Horizontal Mount	10
Hardware Features	12
Router Front Panel	12
Router Back Panel	14
Router Label	15
Power Your Router On	15
How Do I Connect My Device to the Router?	16
Log In to Your Router	17
Basic Setup: Configure Your Internet Settings	18
Broadband Settings	19
4G LTE Broadband Settings	20
Wide Area Network (WAN) Ethernet Broadband Settings	22
Traffic Meter	27

## Chapter 2 Wi-Fi Settings

Plan Your Wireless Network	30
Wireless Placement and Range Guidelines	31
Wireless Security Options	31
Manually Configure Your Wireless Settings	32
Configure WPA, WPA2, or WPA + WPA2	34
Configure WEP	35
Use Push 'N' Connect (WPS) to Configure Your Wireless Network	36
WPS Button	37
WPS PIN Entry	38
Add Wireless Computers That Do Not Support WPS	39

## Chapter 3 Content Filtering

Block Sites	42
Block Services	43
Schedule	44
Schedule Content Filtering	44
Localize Your Time Zone	45
Email	46

## Chapter 4 Maintenance

Router Status . . . . .	49
Attached Devices . . . . .	52
Back Up Settings . . . . .	53
Back Up the Configuration to a File . . . . .	53
Restore the Configuration from a File. . . . .	54
Erase the Configuration . . . . .	54
Set Password . . . . .	55
Change the Built-In Password . . . . .	55
Change the Administrator Login Time-Out. . . . .	56
Diagnostics. . . . .	57
Logs . . . . .	58

## Chapter 5 Advanced

Access Control . . . . .	60
Advanced Wi-Fi Settings . . . . .	61
Wireless Station Access Control . . . . .	62
Restrict Access by MAC Address. . . . .	63
Wi-Fi Repeating Function. . . . .	65
Port Forwarding/Port Triggering . . . . .	66
Remote Computer Access Basics . . . . .	66
Port Triggering to Open Incoming Ports. . . . .	67
Port Forwarding to Permit External Host Communications . . . . .	68
How Port Forwarding Differs from Port Triggering . . . . .	69
Set Up Port Forwarding . . . . .	70
Set Up Port Triggering . . . . .	70
Miscellaneous. . . . .	72
Set Up a Default DMZ Server. . . . .	73
LAN Setup . . . . .	74
DHCP Settings . . . . .	76
Reserved IP Addresses . . . . .	76
QoS Setup . . . . .	78
QoS Priority Rule List. . . . .	79
QoS Priority Rules . . . . .	79
Dynamic DNS. . . . .	82
Static Routes . . . . .	84
Static Route Example. . . . .	84
Remote Management. . . . .	86
UPnP . . . . .	88
IPv6 . . . . .	89

## Chapter 6 Troubleshooting

Basic Functioning . . . . .	97
Troubleshoot Access to the Router Main Menu . . . . .	99
Troubleshoot Your Connection. . . . .	100
Connecting to the Internet . . . . .	100

Troubleshoot Internet Browsing . . . . .	101
Troubleshoot a TCP/IP Network Using the Ping Utility . . . . .	102
Test the LAN Path to Your Router . . . . .	102
Test the Path from Your Computer to a Remote Device . . . . .	102
Problems with Date and Time . . . . .	103
Restore the Default Configuration and Password . . . . .	103

**Appendix A List of Acronyms**

**Appendix B Factory Default Settings**

**Appendix C Compliance Notification**

**Index**

# Basic Setup and Traffic Meter

---

# 1

This chapter describes how to configure your Verizon 4G LTE Router MBR1515LVW Internet connection.

- *Assemble the Router*
- *Hardware Features*
- *Power Your Router On*
- *How Do I Connect My Device to the Router?*
- *Log In to Your Router*
- *Basic Setup: Configure Your Internet Settings*
- *Traffic Meter*

---

**Note:** For help with installation, see the *Verizon 4G LTE Router MBR1515L Installation Guide*.

---

---

**Note:** For more information about the topics that are covered in this manual, visit the support website at [support.verizonwireless.com/contact\\_us/](http://support.verizonwireless.com/contact_us/).

---

---

**Note:** To access online help, click the online help button ().

---

## Assemble the Router

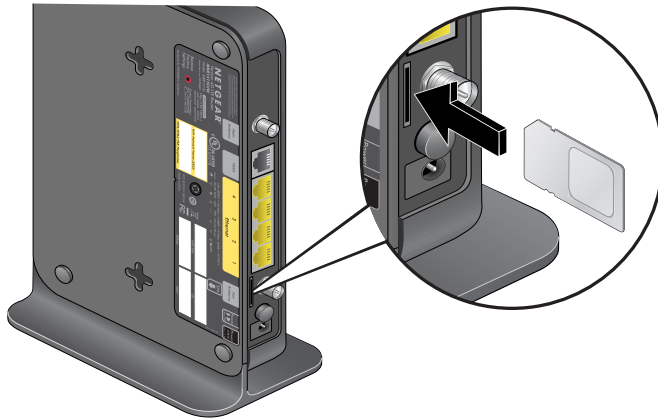
The router requires assembly. The SIM card and antennas must be installed and positioned.

➤ **To assemble the router:**

1. Install the 4G LTE SIM card.

**Note:** *The SIM (subscriber identity module) card is a small rectangular plastic card that stores your phone number and important information about your wireless service. Insert the SIM card into the slot until you hear a click.*

Insert the SIM card into the labeled SIM card slot with its gold contacts facing back and its cut-off corner facing inward.



If you need to remove your SIM card from your router, gently press the SIM card inward to release it, and remove it from the slot.

2. Install the antennas.

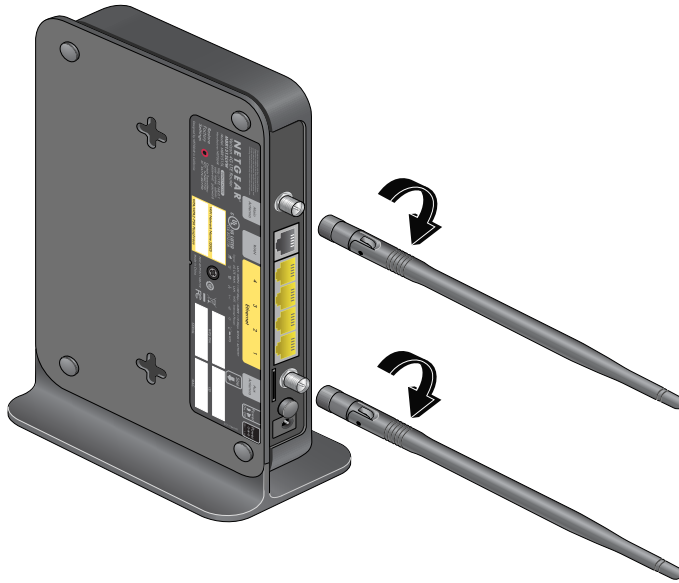
The Verizon 4G LTE router comes with two detachable antennas. These two external antennas are required for proper 4G LTE service and are in addition to the internal antennas that are used for Wi-Fi.

---

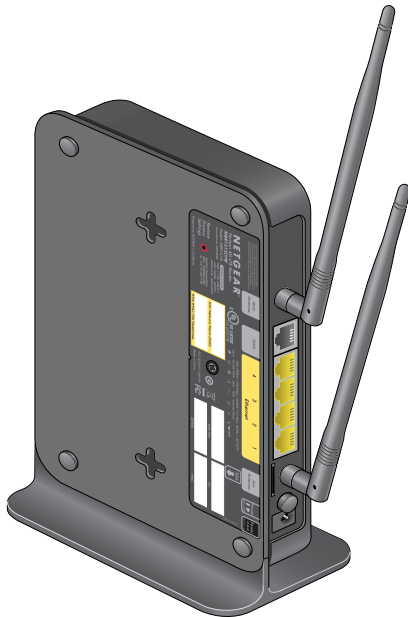
**Note:** For best 4G LTE reception, position these external antennas so that they are at right angles to each other.

---

- a. Align the antennas with the antenna posts on the router as shown in the following illustrations.

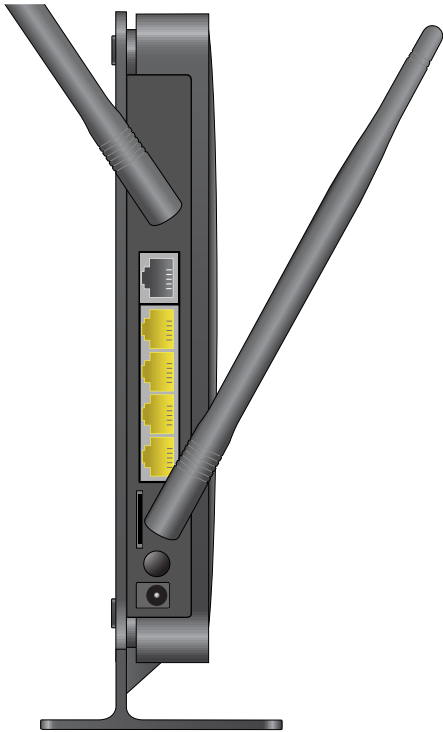


- b. Mount the antennas on the threaded antenna posts, ensuring that the connection is secure.
- c. You can swivel the antennas in any direction, to better fit the space where your router is placed.





3. For best 4G LTE reception, position these external antennas so that they are at right angles to each other.



## Place the Router

Position your router upright. Place your router near an AC power outlet in a location where you can connect the cables you need for your home network. The router must also be located where you can receive a strong mobile broadband signal while indoors (preferably near a window) if you are planning to connect to the Internet using mobile broadband.

## Optional: Horizontal Mount

---

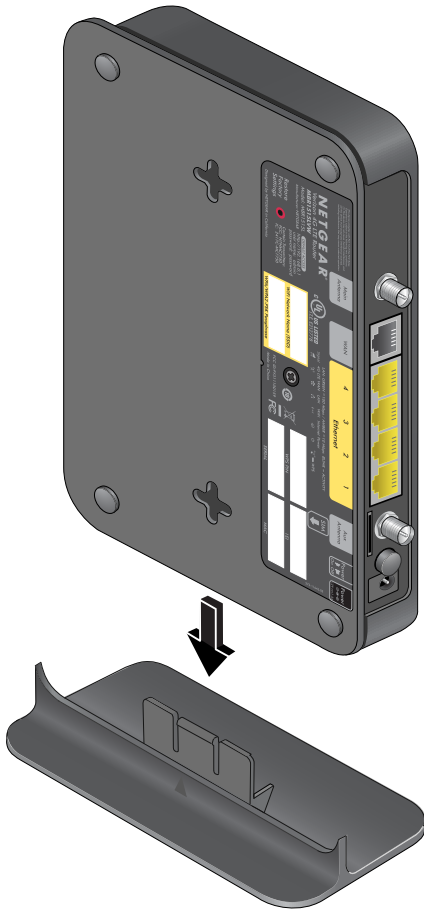
**Note:** The Verizon 4G LTE router comes attached to a vertical stand. The upright position saves space, optimizes antenna position, and improves Wi-Fi signal strength for best performance when you are browsing the Internet, streaming videos, downloading or uploading files.

---

You can remove the detachable plastic base for the vertical stand when you prefer to place the router horizontally on a flat surface.



To remove the plastic base, hold the router firmly with one hand. With your other hand, pull down the plastic base to detach it from the vertical stand.



## Hardware Features

This section outlines the physical aspects of your Verizon 4G LTE Router.

### Router Front Panel

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

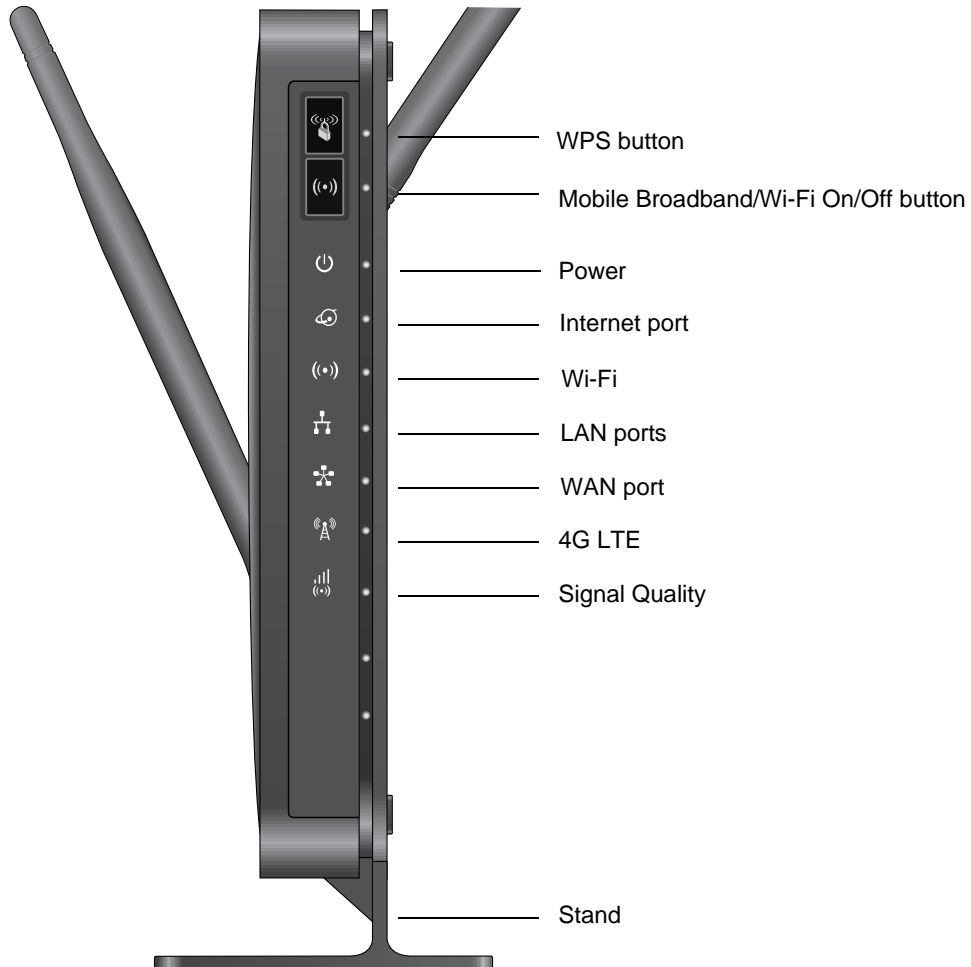


Table 1 describes each LED and button on the front panel of the router.

**Table 1. LED descriptions**










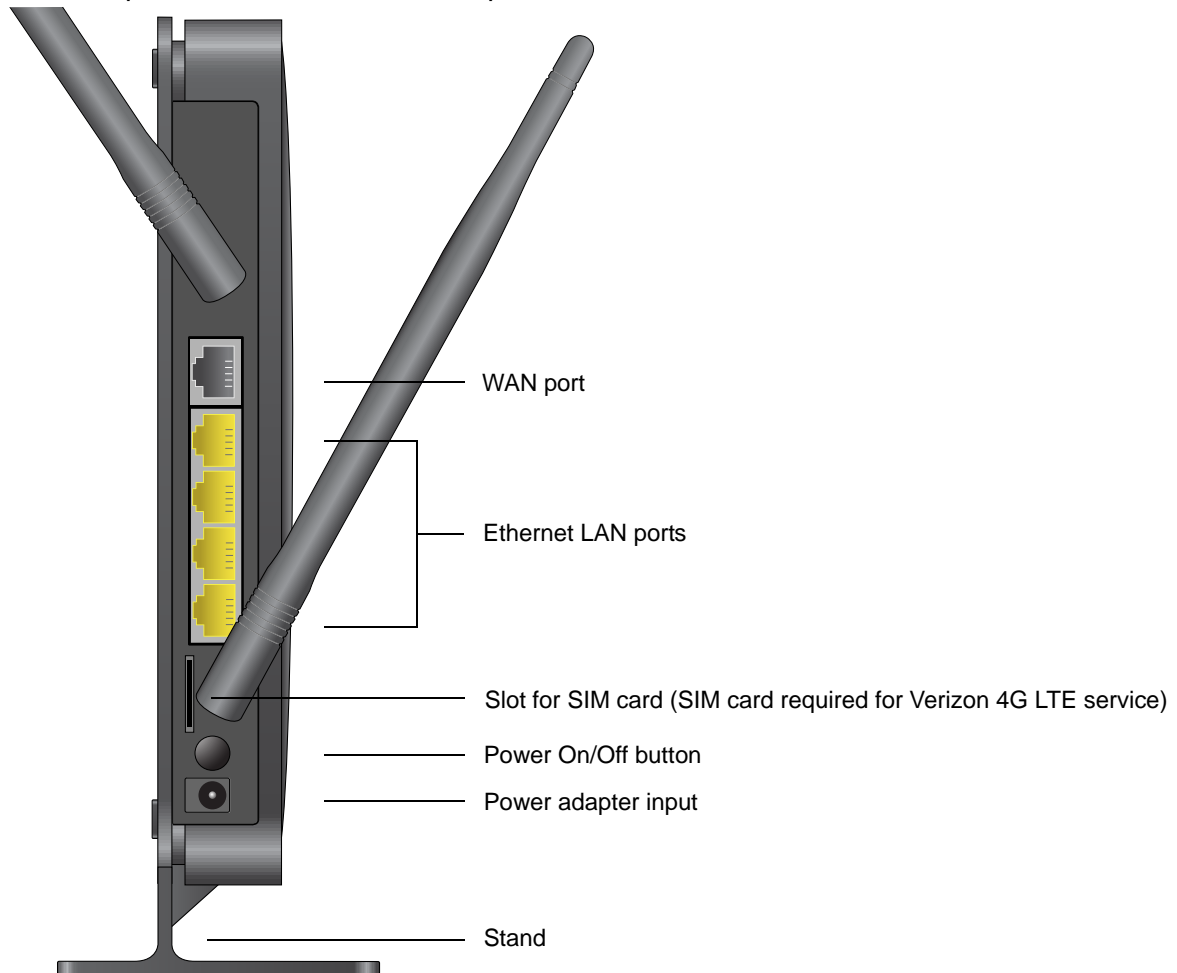
LED	Activity	Description
WPS 		Press the <b>WPS</b> button to open a 2-minute window for the router to connect with other WPS-enabled devices. For more information about this function, see <a href="#">Use Push 'N' Connect (WPS) to Configure Your Wireless Network</a> on page 36.
Wi-Fi 		This button can be used to control the Wi-Fi radio or both the Wi-Fi radio and mobile broadband radio. Use the router interface to select the options. The default is set for Wi-Fi 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	An Internet connection is established.
	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 WAN to mobile broadband occurred.
	Off	No Internet connection is detected.
Wi-Fi 	Solid blue	The Wi-Fi local port is initialized.
	Blinking blue	Data is being transmitted or received over the Wi-Fi 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.
4G LTE 	Solid blue	The router is in 4G LTE coverage.
	Off	No coverage is detected.

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.

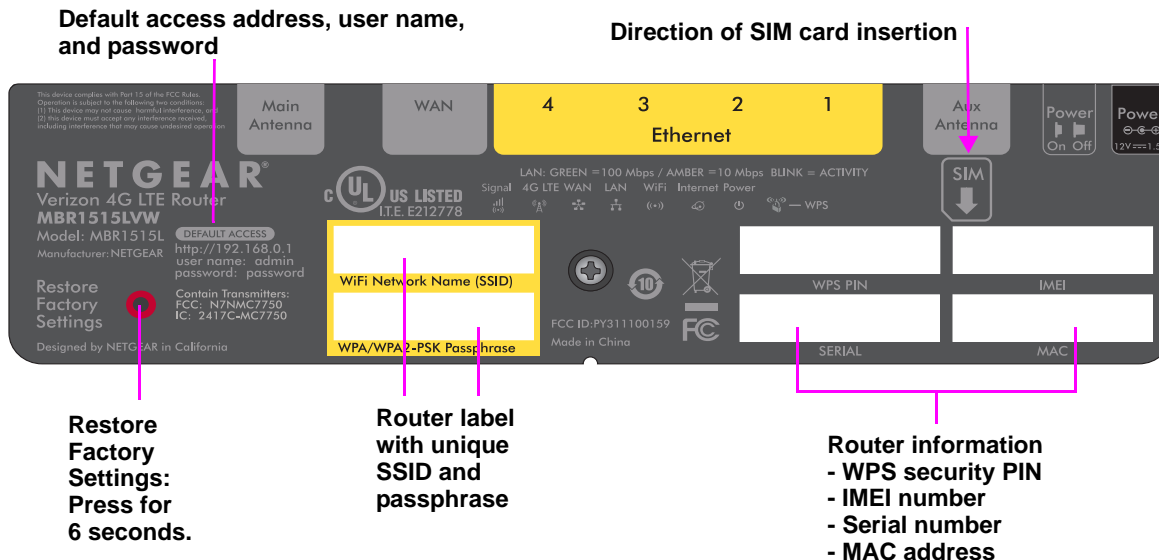
## Router Back Panel

The back panel of the router contains port connections.



## Router Label

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



## SSID and Passphrase

Computers and devices that connect to the router wirelessly and do not support WPS use this unique SSID and passphrase information to make the connection. See [Add Wireless Computers That Do Not Support WPS](#) on page 39 for more information.

## Restore Factory Settings



Insert a paperclip into the hole and press for 6 seconds. Pressing the Restore Factory Settings button causes the Power LED to blink briefly. After the button is held down for more than 6 seconds, the Power LED blinks amber and turns green as the router resets to the factory defaults. See [Factory Default Settings](#) on page 109 for the factory defaults.

## Power Your Router On

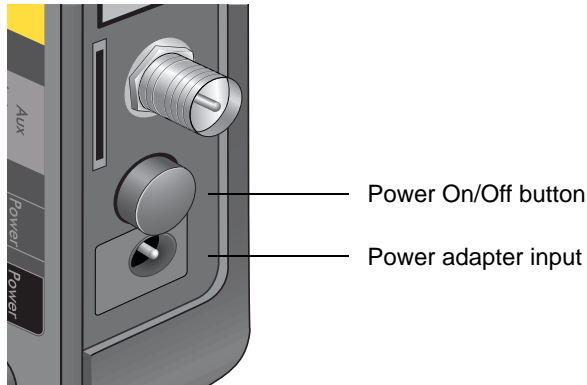
Place the router in a central location relative to where you want coverage in your home for optimal network performance. Here are some additional considerations:

- Avoid physical obstructions whenever possible that might weaken Wi-Fi signals.
- Avoid placing the router close to reflective or metal surfaces, such as mirrors, metal file cabinets, stainless steel countertops that can lessen both network range and performance.

- Place the router away from electrical equipment or appliances (microwave ovens) that can also generate Wi-Fi signal interference.

➤ **To power on your router:**

1. Plug the power adapter cord into the power adapter input on the rear of the router and insert the other end into an electrical outlet.
2. Press the **Power On/Off** button.



## How Do I Connect My Device to the Router?

1. From the device you want to connect with (smartphone, tablet, laptop computer, gaming device), go to your device setting or software that manages your wireless connections.
2. Scan for new or available devices to connect to.
3. The device scans for all wireless networks in your area. Look for your Wi-Fi network. (The SSID and passphrase are preconfigured and are printed on the side of your router.)
4. Select the name of your Wi-Fi network, which appears as “Verizon – MBR1515 – XXXX” (where X = last 4 digits of the MAC address), and connect.

---

**Note:** For a WPS (Wi-Fi Protected Setup) connection, sometimes referred to as Push 'N' Connect, press the **WPS** button on the router. Within 2 minutes, follow the software instructions on your device to complete the WPS process. See [WPS Button](#) on page 37.

---



## Log In to Your Router

After the initial router setup, you can use your web browser to log in to the router to view or change its settings.

---

**Note:** Your computer must be configured for DHCP. For help configuring DHCP, refer to the documentation that came with your computer.

---

When you have logged in and if you do not click Logout, after 60 minutes of no activity the router automatically logs you out.

---

**Note:** You can reset this automatic logout duration on the Set Password screen (see [Set Password](#) on page 55).

---

➤ **To log in to the router:**

1. Type **http://192.168.0.1** in the address field of your browser and press **Enter** to display the login window.



The screenshot shows a login dialog box with a light gray background. It has two text input fields: 'User name:' with 'admin' and a dropdown arrow, and 'Password:' with ten black dots. Below the password field is a checkbox labeled 'Remember my password' which is unchecked. At the bottom are two buttons: 'OK' and 'Cancel'.

2. Enter **admin** for the user name and your password (or the default, **password**).  
For information about how to change the password, see [Change the Built-In Password](#) on page 55.

---

**Note:** If you do not remember your password, you can restore the router to its factory default settings, which resets the password. See [Factory Default Settings](#) on page 109.

---

## Basic Setup: Configure Your Internet Settings

For you to connect to the network, an active broadband service account is required. The broadband service can be 4G LTE from Verizon or WAN Ethernet (such as DSL or cable broadband) from an ISP.

- For 4G LTE Mobile Broadband service, contact Verizon. Verizon provides a SIM card, data plan, and other relevant account setup information.
- If WAN Ethernet service is required, contact your ISP for your user name, password, and the network name.

You must also configure some or all of the settings described in the following sections, depending on how you have chosen to connect to the Internet:

- [Broadband Settings](#) on page 19 (required only if you are changing the Internet connection mode from mobile broadband to WAN Ethernet).
- [4G LTE Broadband Settings](#) on page 20 (not required if you are using a WAN Ethernet connection).
- [Wide Area Network \(WAN\) Ethernet Broadband Settings](#) on page 22 (not required if you are using a 4G LTE connection).

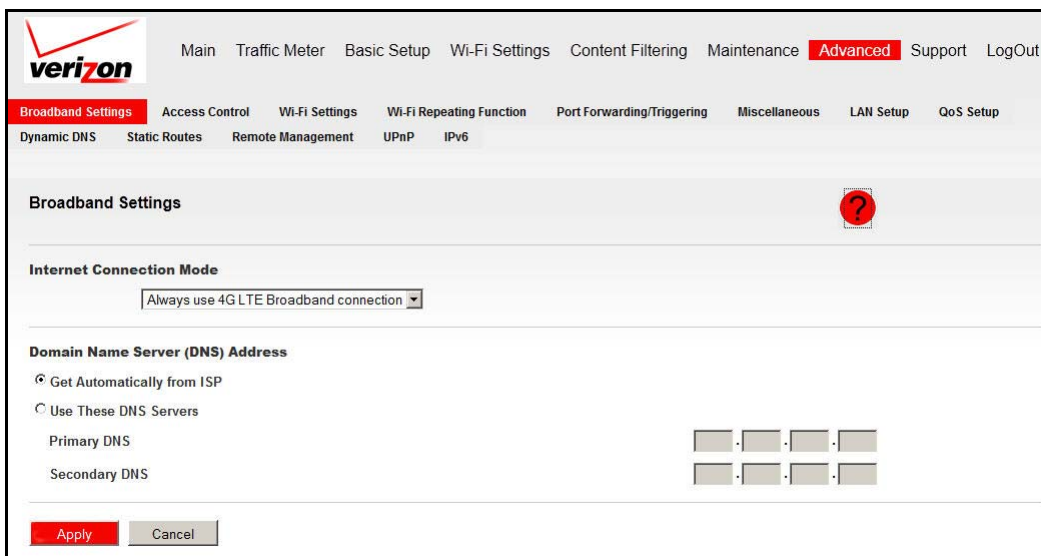
## Broadband Settings

---

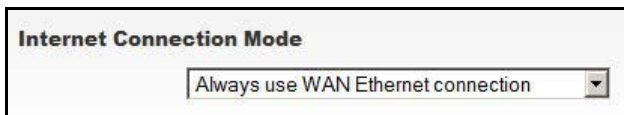
**Note:** The default Internet connection mode is 4G LTE Broadband. This setting is changed only if you are changing the Internet connection mode to WAN Ethernet Broadband.

---

- **To manually configure your broadband Internet settings:**
  1. Log in to the router as described in [Log In to Your Router](#) on page 17.
  2. From the main menu, select **Advanced > Broadband Settings**. The following screen displays:



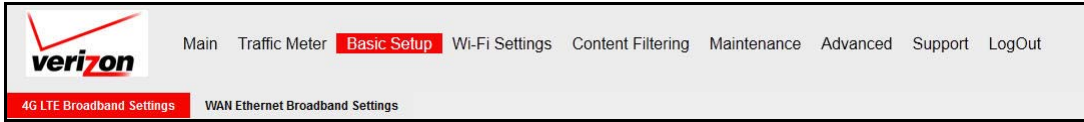
3. Change the Internet connection mode to **Always use WAN Ethernet connection**.



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

## 4G LTE Broadband Settings

- To manually configure your 4G LTE broadband Internet settings:
  1. Log in to the router as described in [Log In to Your Router](#) on page 17.
  2. From the main menu, select **Basic Setup** > **4G LTE Broadband Settings**.



The following screen displays:

The screenshot shows the '4G LTE Broadband Settings' configuration page. It includes a red question mark icon in the top right corner. The form contains the following fields and options:

- User Name: <none>
- Password: <none>
- Country: USA (dropdown menu)
- Internet Service Provider: Verizon (dropdown menu)
- Connect automatically at startup
- Reconnect automatically when connection is lost
- Wi-Fi Button Configuration:
  - Control Wi-Fi Only
  - Control Both Wi-Fi and 4G Broadband
  - Control 4G LTE Only
- Connection Status: NO SIM Card Detected
- Buttons: Connect, Disconnect, Apply (highlighted in red), Cancel, Refresh

---

**Note:** To connect to the 4G LTE network, an active broadband service account with Verizon is required. The user name, password, country, and Internet service provider elements are not writeable or changeable. These settings are selected and provided by default when a SIM card is inserted.

---

3. Adjust the settings as needed based on your Internet connection. The fields in this screen are described in the following table:

Fields and Check Boxes	Description
User Name	Internet account login user name.
Password	Internet account password for authentication.

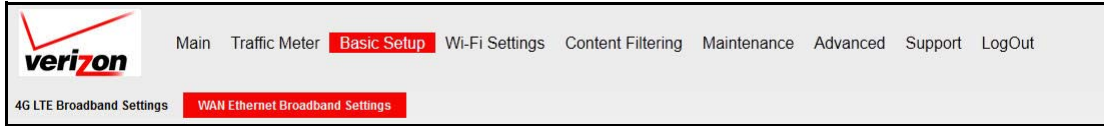
Fields and Check Boxes	Description
Country	Select your country from the drop-down list.
Internet Service Provider	Select your Internet service provider from the drop-down list.
Connect automatically at startup	When this check box is selected, the modem automatically connects to the network when powered up. This check box should be selected after login information is provided.
Reconnect automatically when connection is lost	When this check box is selected, the modem attempts to reconnect to the network when the connection is lost. Under normal situations, this setting should be selected.
Wi-Fi Button Configuration	<p>Select the option to determine the behavior of the Wi-Fi button on the front panel when it is pressed.</p> <ul style="list-style-type: none"> <li>• <b>Control Wi-Fi Only.</b> When you select this radio button, pressing the Wi-Fi button toggles the Wi-Fi function. If Wi-Fi is turned on, pressing the button turns off the Wi-Fi. Pressing it again turns on the Wi-Fi. This function is available only if the Wi-Fi function is enabled. The 4G broadband function is unaffected.</li> <li>• <b>Control Both Wi-Fi and 4G Broadband.</b> When you select this radio button, pressing the Wi-Fi button toggles both the Wi-Fi function and 4G broadband at the same time. If Wi-Fi is turned on, pressing the button turns off the Wi-Fi. At the same time, the 4G broadband connection is disconnected. If you press the button again, Wi-Fi is turned on and the router attempts to reestablish the 4G broadband connection. Depending on the coverage, 4G broadband coverage might or might not be connected successfully.</li> <li>• <b>Control 4G LTE Only.</b> When you select this radio button, pressing the Wi-Fi button toggles the 4G LTE function. If 4G LTE is turned on, pressing the button turns off the 4G LTE. Pressing it again turns on the 4G LTE. This function is available only if the 4G LTE function is enabled. The Wi-Fi function is unaffected.</li> </ul>
Connection status	Current WAN port status.

4. Available buttons are:

- **Connect.** Manually connect to the network.
- **Disconnect.** Disconnect from the current network.
- **Apply.** Apply the changes that you made.
- **Cancel.** Discard changes.
- **Refresh.** Update the connection status.

## Wide Area Network (WAN) Ethernet Broadband Settings

- To manually configure your WAN Ethernet Broadband Internet settings:
1. Log in to the router as described in [Log In to Your Router](#) on page 17.
  2. From the main menu, select **Basic Setup** > **WAN Ethernet Broadband Settings**.



The following question displays:

A screenshot of a question displayed on the router's configuration page. The question is "Does your Internet connection require a login?". There are two radio button options: "Yes" and "No". The "No" option is selected, indicated by a filled radio button.

Select the option based on the type of account you have with your ISP.

- If you need to enter login information every time you connect to the Internet, or you have a PPPoE account with your ISP, select **Yes**, and see [Yes, a Login Is Required](#) on page 23.
- Otherwise, select **No** and see [No, a Login Is Not Required](#) on page 25.

---

**Note:** If you have installed PPP software such as WinPoET (from Earthlink) or Enternet (from PacBell), then you have PPPoE. Select **Yes**. After selecting Yes and configuring your router, you do not need to run the PPP software on your computer to connect to the Internet.

---

*Yes, a Login Is Required*

➤ **To configure your Internet connection when a login is required:**

1. Adjust the settings as needed based on your Internet connection.

The screenshot shows the Verizon router's configuration interface. At the top, there are navigation links: Main, Traffic Meter, Basic Setup (highlighted in red), Wi-Fi Settings, Content Filtering, Maintenance, Advanced, Support, and LogOut. Below this, there are two tabs: '4G LTE Broadband Settings' and 'WAN Ethernet Broadband Settings' (highlighted in red). The main content area is titled 'Basic Settings' and contains a red question mark icon. Below the icon, the question 'Does your Internet connection require a login?' is displayed. Two radio buttons are present: 'Yes' (which is selected) and 'No'.

The screenshot shows the 'Internet Service Provider' configuration page. It includes several fields and options:
 

- Internet Service Provider:** A dropdown menu currently set to 'PPPoE'.
- Login:** A text input field containing the word 'guest'.
- Password:** An empty text input field.
- Service Name (If Required):** An empty text input field.
- Connection Mode:** A dropdown menu currently set to 'Dial on Demand'.
- Idle Timeout (In Minutes):** A text input field containing the number '5'.
- Internet IP Address:** Two radio buttons are present. The first is 'Get Dynamically from ISP' (selected), and the second is 'Use Static IP Address'. To the right of the second radio button are four IP address input fields containing '192', '168', '0', and '16' respectively.

 At the bottom of the form are three buttons: 'Apply' (highlighted in red), 'Cancel', and 'Test'.

The fields in this screen are described in the following table:

Fields and Check Boxes	Description
Internet Service Provider	Select the service that your ISP provides. <ul style="list-style-type: none"> <li>• Other (PPPoE) is the most common.</li> <li>• PPTP is used in Austria and other European countries.</li> <li>• Telstra BigPond is for Australia only.</li> </ul>
Login	This login name is usually the name that you use in your email address. For example, if your main mail account is JerAB@ISP.com, type JerAB in this field. Some ISPs (such as Mindspring, Earthlink, and T-DSL) require that you use your full email address when you log in. If your ISP requires your full email address, type it in the Login field.
Password	Type the password that you use to log in to your ISP.
Service Name (If Required)	If your ISP provided a service name, enter it here. Otherwise, this field can be left blank.

Fields and Check Boxes	Description
Connection Mode	<p>Set the connection mode to <b>Dial on Demand</b>, <b>Always On</b>, or <b>Manually Connect</b>.</p> <ul style="list-style-type: none"> <li>• With the default setting, <b>Dial on Demand</b>, a PPPoE connection automatically starts with outbound traffic to the Internet, and it automatically terminates if the connection is idle based on the value in the Idle Timeout field.</li> <li>• When the connection mode is set to <b>Always On</b>, the PPPoE connection automatically starts when the computer boots up, but the connection does not time out. The router keeps trying to bring up the connection after it is disconnected for some reason.</li> <li>• If you select <b>Manually Connect</b>, you must go to the Router Status screen and click the <b>Connect</b> button to connect to the Internet. The manual connection does not time out, and you have to click the <b>Disconnect</b> button on the Router Status screen to disconnect it.</li> </ul>
Idle Timeout (In Minutes)	<p>An idle Internet connection will be terminated after this time period. If this value is zero (0), the router keeps the connection alive by reconnecting immediately whenever the connection is lost.</p>
Internet IP Address	<p>If you log in to your service or your ISP did not provide you with a fixed IP address, the router finds an IP address for you automatically when you connect. Select <b>Get Dynamically from ISP</b>.</p> <p>If you have a fixed (static, permanent) IP address, your ISP has provided you with an IP address. Select <b>Use Static IP Address</b> and type in the IP address.</p>

2. The following buttons are available when you are done:

- **Apply.** Apply the changes that you made.
- **Cancel.** Discard changes.
- **Test.** Connect to the My Verizon website. If you connect successfully, your settings work, and you can click **Logout** to exit these screens.



*No, a Login Is Not Required*

➤ To configure your Internet connection when a login is not required:

1. Adjust the settings as needed based on your Internet connection.

The fields in this screen are described in the following table:

Fields and Check Boxes	Description
Account Name (If Required)	This name is also known as the host name or system name. For most users, type your account name or user name in this field. For example, if your main mail account is JerAB@ISP.com, type JerAB in this field. If your ISP has given you a specific host name, type it (for example, CCA7324-A).
Domain Name (If Required)	For most users, you can leave this field blank, unless the domain name is required by your ISP. You can type the domain name of your ISP. For example, if your ISP mail server is mail.xxx.yyy.zzz, you would type xxx.yyy.zzz as the domain name. If you have a domain name given to you by your ISP, type it in this field. (For example, Earthlink Cable might require a host name of home, and Comcast sometimes supplies a domain name.) If you have a cable modem, this domain name is usually the workgroup name.

Fields and Check Boxes	Description
Internet IP Address	<p>If you log in to your service or your ISP did not provide you with a fixed IP address, the router finds an IP address for you automatically when you connect. Select <b>Get Dynamically From ISP</b>.</p> <p>If you have a fixed (or static IP) address, your ISP has provided you with the required information. Select <b>Use Static IP Address</b> and type the IP address, subnet mask, and gateway IP address into the correct fields.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• <b>IP Address.</b> 24.218.156.183</li> <li>• <b>Subnet Mask.</b> 255.255.255.0</li> <li>• <b>Gateway IP Address.</b> 24.218.156.1</li> </ul>
Router MAC Address	<p>Your computer's local address is its unique address on your network. This is also referred to as the computer's MAC (Media Access Control) address.</p> <ul style="list-style-type: none"> <li>• Usually, select <b>Use Default MAC Address</b>.</li> <li>• If your ISP requires MAC authentication, select either <b>Use Computer MAC Address</b> to disguise the router's MAC address with the computer's own MAC address, or <b>Use This MAC Address</b> and manually type the MAC address for a different computer.</li> </ul> <p>The format for the MAC address is XX:XX:XX:XX:XX:XX. This value might be changed if Use Computer MAC Address is selected once a value has already been set for the Use This MAC Address selection.</p>

2. The following buttons are available when you are done:

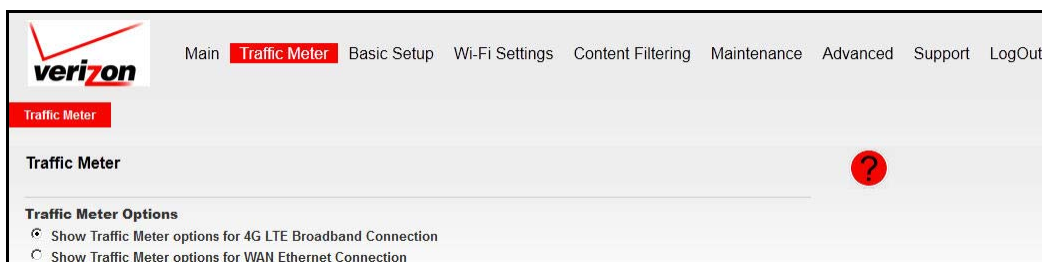
- **Apply.** Apply the changes that you made.
- **Cancel.** Discard changes.
- **Test.** Connect to the My Verizon website. If you connect successfully, your settings work, and you can click **Logout** to exit these screens.

## 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. You enable separate traffic meters for the mobile broadband connection and the Ethernet connection.

➤ **To monitor traffic on your router:**

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Traffic Meter**.



The following screen displays:

The screenshot displays the configuration page for the Traffic Meter. It includes several sections:

- Enable Traffic Meter for 4G LTE Broadband:** A checked checkbox. Below it, 'Traffic volume control by' is set to 'No limit'. There are input fields for 'Monthly limit' (0) in Mbytes and 'Round up data volume for each connection by' (0) in Mbytes. 'Connection time control' is selected, with a 'Monthly limit' input field set to 0 hours.
- Traffic Counter:** A section for restarting the counter at a specific time (00:00 am) on the 1st day of each month, with a 'Restart Counter Now' button.
- Traffic Control:** A section for setting a warning message (0 Mbytes/Minutes before the monthly limit is reached) and options for when the limit is reached: 'Turn the Internet LED to flashing green/amber', 'Disconnect and disable the Internet connection', and 'Email'.
- Internet Traffic Statistics:** A section showing start and current dates/times, and the current traffic volume left (No limit).

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

Buttons at the bottom include 'Refresh', 'Traffic Status', 'Apply', and 'Cancel'.

3. Select the appropriate Traffic Meter Options radio button for the type of Internet connection (for example, 4G LTE Broadband or WAN Ethernet) that you are setting up.
4. To enable the traffic meter, select the **Enable Traffic Meter** check box.

5. 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.
6. You can limit the amount of data traffic allowed per month:
  - **Monthly Limit.** Enter the monthly volume limit or connection time limit.
  - **Round up data volume for each connection by.** Some ISPs charge certain amount of extra data volume when users make a new connection. If this case, enter the extra data volume here.
7. Set the traffic counter to begin at a specific time and date.
8. 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 Port LED blinks.
  - The Internet connection is disconnected and disabled.
  - Send an email notification. For information about setting up email notification, see [Email](#) on page 46.
9. Set up Internet traffic statistics to monitor the data traffic.
10. Click the **Traffic Status** button if you want a live update on Internet traffic status on your router.
11. Click **Apply** to save your settings.

# Wi-Fi Settings

---

# 2

For a wireless connection, the SSID (also known as the wireless network name), and the wireless security settings must be the same for the router and wireless computers or wireless adapters. Verizon recommends that you use wireless security.

The router is preconfigured with WPA-PSK/WPA2-PSK mixed mode and uses a unique SSID and passphrase. This information is printed on the label on the bottom of the router. Use this information to set up your Wi-Fi computer and devices.

This chapter addresses the following:

- [\*Plan Your Wireless Network\*](#)
- [\*Manually Configure Your Wireless Settings\*](#)
- [\*Use Push 'N' Connect \(WPS\) to Configure Your Wireless Network\*](#)

---

**Note:** Computers can connect wirelessly at a range of up to 300 feet (100 meters). Internal obstructions could impede the signal. If you do not use wireless security, others outside your immediate area can access your network.

---

---

**Note:** To access online help, click the online help button ().

---

## Plan Your Wireless Network

The router comes with preset security. This means that the Wi-Fi 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 side of the unit (see [Router Label](#) on page 15).

---

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

---

**Verizon 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.

If you decide to change the preset wireless security settings, be aware of the following requirements:

- For compliance and compatibility between similar products in your area, the operating channel and region must be set correctly.
- To configure the wireless network, you can either specify the wireless settings, or you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security.
  - To manually configure the wireless settings, you must know the following:
    - SSID. The default SSID for the router is printed on the router label (see [Router Label](#) on page 15).
    - The wireless mode (802.11n, 802.11g, or 802.11b) that each wireless adapter supports.
    - Wireless security option. To successfully implement wireless security, check each wireless adapter to determine which wireless security option it supports.

See [Manually Configure Your Wireless Settings](#) on page 32.

- Push 'N' Connect (WPS) implements WPA/WPA2 wireless security on the router and your wireless computer or device at the same time. The wireless computer or device must be compatible with WPS. See [Use Push 'N' Connect \(WPS\) to Configure Your Wireless Network](#) on page 36.
- The Wi-Fi repeating function requires WEP encryption. See [Wi-Fi Repeating Function](#) on page 65.

## Wireless Placement and Range Guidelines

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

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

- Near the center of the area in which your computers operate.
- In an elevated location, such as a high shelf, where the wirelessly connected computers have line-of-sight access (even if through walls).
- Away from sources of interference, such as microwave ovens, and 2.4 GHz cordless phones (see [Interference Reduction Table](#) on page 112).
- Away from large metal surfaces.
- Place the router in the vertical position for the best coverage (as an example, see the image in [Router Back Panel](#) on page 14).
- If using multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use Channels 1 and 6, or 6 and 11).

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

## Wireless Security Options

Indoors, computers can connect over Wi-Fi networks at a maximum range of up to 300 feet (100 meters). Such distances can allow others outside your immediate area to access your network.

Unlike wired network data, your wireless data transmissions extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The Verizon 4G LTE Router provides highly effective security features, which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

Each router is preconfigured for WPA-PSK/WPA2-PSK mixed mode, and comes with a unique SSID and passphrase for each router.

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

- **Restrict access based on MAC address.** You can allow only trusted computers to connect so that unknown computers cannot wirelessly connect to the router. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn off the broadcast of the wireless network name (SSID).** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This approach nullifies wireless network “discovery” feature of some products, such as Windows XP, but the data is still exposed.

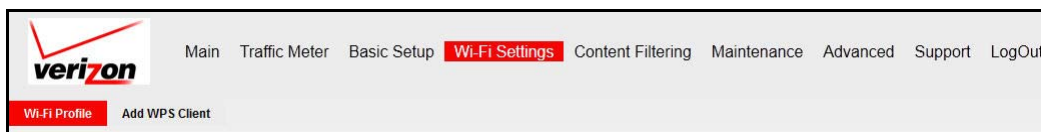
- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode is superseded by WPA-PSK and WPA2-PSK.
- **WPA-PSK (TKIP), WPA2-PSK (AES).** Wi-Fi Protected Access (WPA) using a pre-shared key to authenticate and generate the initial data encryption keys. The strong authentication along with dynamic per frame rekeying of WPA makes it almost impossible to compromise.

## Manually Configure Your Wireless Settings

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

### ➤ To view or manually configure the wireless settings:

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Wi-Fi Settings > Wi-Fi Profile**.



The following screen displays:



The settings for this screen are explained in the following table:

Settings		Description
Wireless Network	Name (SSID)	The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. When more than one wireless network exists, SSIDs provide a means for separating the traffic. To join a network, a wireless computer or device must use the SSID.
	Region	The location where the router is used.
	Channel	The wireless channel used by the gateway. The default is <b>Auto</b> . Do not change the channel unless you experience interference (as indicated by lost connections or slow data transfers). If this interference happens, you might need to try different channels to see which works best.
	Mode	The default is Up to 145 Mbps.
Security Options	None	Use this setting to establish wireless connectivity before implementing wireless security. Verizon recommends that you implement wireless security.
	WEP	Use encryption keys and data encryption for data security. You can select 64-bit or 128-bit encryption. See <a href="#">Configure WEP</a> on page 35.
	WPA-PSK (TKIP)	Allow only computers configured with WPA to connect to the router. See <a href="#">Configure WPA, WPA2, or WPA + WPA2</a> on page 34.
	WPA2-PSK (AES)	Allow only computers configured with WPA2 to connect to the router. See <a href="#">Configure WPA, WPA2, or WPA + WPA2</a> on page 34.
	WPA-PSK (TKIP) + WPA2-PSK (AES)	Allow computers configured with either WPA-PSK or WPA2-PSK security to connect to the router. See <a href="#">Configure WPA, WPA2, or WPA + WPA2</a> on page 34.
Passphrase	Use this network key to connect wirelessly to the router.	

3. Select the region in which the router operates.
4. For initial configuration and test, leave the other settings unchanged.
5. To save your changes, click **Apply**.
6. Set up and test your wireless devices and computers to make sure that they can connect wirelessly.

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

If your wireless devices and computers do not connect wirelessly, 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 (see [Attached Devices](#) on page 52)? If it does, 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 side of your router (see [Router Label](#) on page 15).

## Configure WPA, WPA2, or WPA + WPA2

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

Push 'N' Connect (WPS) implements WPA/WPA2 wireless security on the router and your wireless computer or device at the same time. The wireless computer or device must be compatible with WPS.

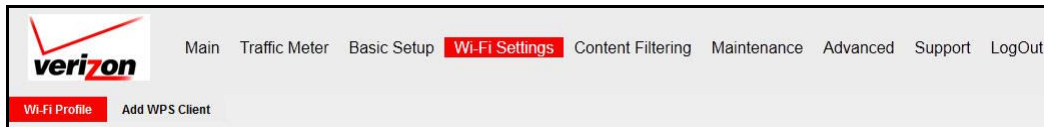
---

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

---

### ➤ To configure WPA or WPA2 in the router:

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Wi-Fi Settings > Wi-Fi Profile**.



3. On the Wi-Fi Profile screen in the Security Options section, select the radio button for the WPA or WPA2 option of your choice.

**Security Options**

None  
 WEP  
 WPA-PSK [TKIP]  
 WPA2-PSK [AES]  
 WPA-PSK [TKIP] + WPA2-PSK [AES]

---

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

4. For WPA-PSK or WPA2-PSK, enter the passphrase.
5. To save your settings, click **Apply**.

## Configure WEP

WEP encryption is not as strong as WPA and WPA2 encryption. But to use the Wi-Fi repeating function of the router (see [Wi-Fi Repeating Function](#) on page 65), WEP encryption is required.

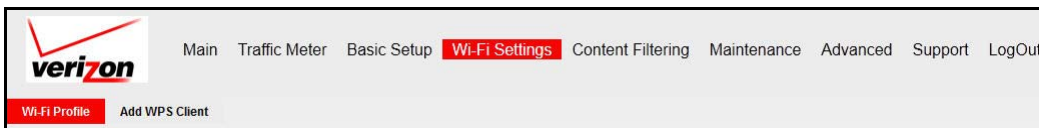
---

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

---

➤ **To configure WEP data encryption:**

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Wi-Fi Settings > Wi-Fi Profile**.



3. On the Wi-Fi Profile screen in the Security Options section, select the **WEP** (Wired Equivalent Privacy) radio button:

 A screenshot of the 'Security Options' section in the router's configuration interface. It features several radio button options: 'None', 'WEP' (which is selected), 'WPA-PSK [TKIP]', 'WPA2-PSK [AES]', and 'WPA-PSK [TKIP] + WPA2-PSK [AES]'. Below these options, there are two dropdown menus: 'Authentication Type' set to 'Automatic' and 'Encryption Strength' set to '64-bit'. Under the heading 'Security Encryption (WEP) Key', there is a 'Passphrase' field with a 'Generate' button, and four 'Key' fields (Key 1 through Key 4), each with a radio button next to it.

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

---

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

---

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

---


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

---

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

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

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

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

WPS considerations:

- The Push 'N' Connect feature is based on the WPS standard. All other Wi-Fi-certified and WPS-capable products should be compatible with products that implement Push 'N' Connect.

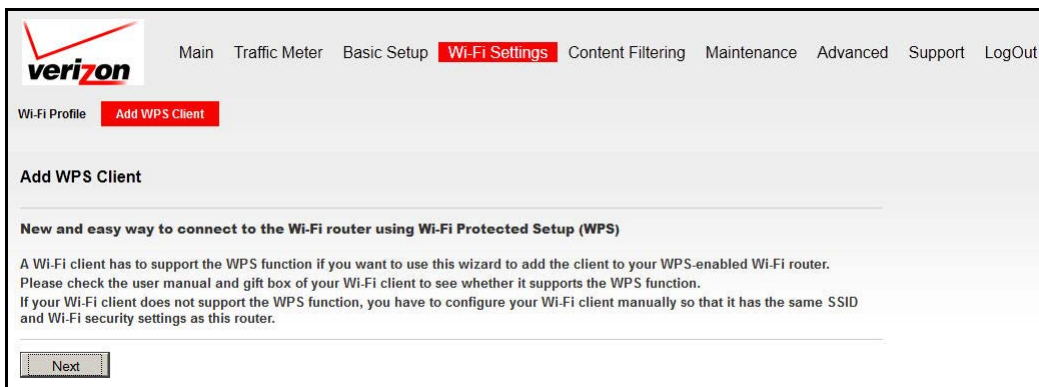
- If your wireless network includes a combination of WPS-capable devices and non-WPS-capable devices, Verizon suggests that you set up your wireless network and security settings manually first, and use WPS only for adding WPS-capable devices.

## WPS Button

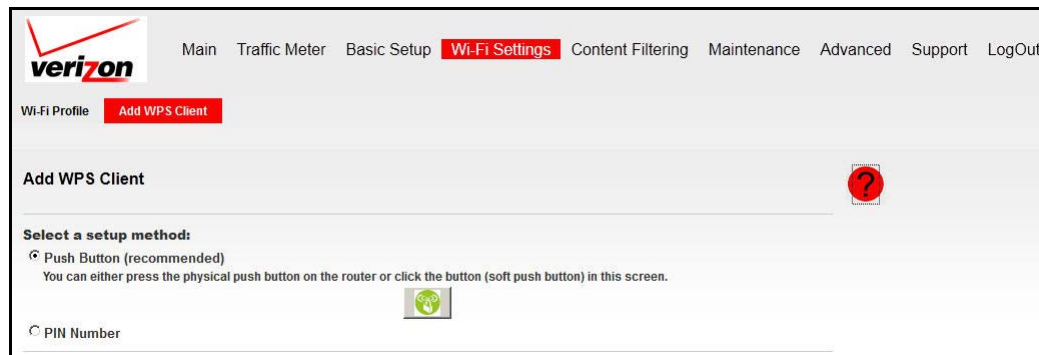
Any wireless computer or wireless adapter that connects to the router wirelessly is a client. The client must support a WPS button, and must have a WPS configuration utility.

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

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. On the main menu, select **Wi-Fi Settings > Add WPS Client**. The following screen displays:



3. Click **Next**. The following screen displays:



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

4. Either click the onscreen button (👉) or press the **WPS** button on the front of the router.  
The router tries to communicate with the client (the computer that wants to join the network) for 2 minutes.
5. Go to the client wireless computer, and run a WPS configuration utility. Follow the utility's instructions to click a WPS button.
6. Go back to the router screen to check for a message.

The router WPS screen displays a message confirming that the client was added to the wireless network. The router generates an SSID and implements WPA/WPA2 wireless security. The router keeps these wireless settings unless you change them, or you clear the **Keep Existing Wi-Fi Settings** check box in the Advanced Wi-Fi Settings screen (see [Advanced Wi-Fi Settings](#) on page 61).

- Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wi-Fi Settings screen. See [Manually Configure Your Wireless Settings](#) on page 32.

To access the Internet from any computer connected to your router, launch a browser. You should see the router's Internet Port LED blink, indicating communication to the ISP.

---

**Note:** If no WPS-capable client devices are located during the 2-minute time frame, the SSID does not change, and no security is set up.

---

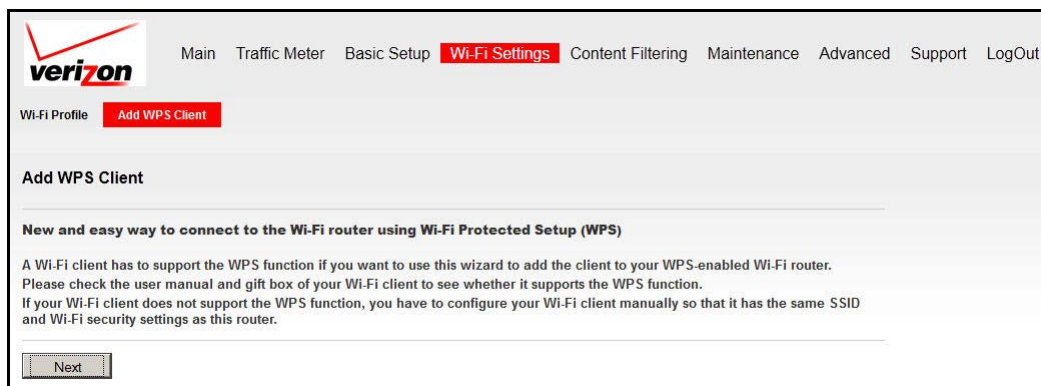
## WPS PIN Entry

Any wireless computer or device that connects to the router wirelessly is a client. The client must support a WPS PIN, and must have a WPS configuration utility.

The first time you add a WPS client, make sure that the **Keep Existing Wi-Fi Settings** check box on the Advanced Wi-Fi Settings screen is cleared (see [Advanced Wi-Fi Settings](#) on page 61). This setting is the default setting for the router and allows it to generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the router automatically selects this check box so that your SSID and wireless security settings stay the same if other WPS devices are added later.

### ➤ To use a PIN to add a WPS client:

- Log in to the router as described in [Log In to Your Router](#) on page 17.
- On the main menu, select **Wi-Fi Settings > Add WPS Client**. The following screen displays:



3. Click **Next** and select the **PIN Number** radio button. The following screen displays.

4. Go to the client wireless computer. Run a WPS configuration utility. Follow the utility's instructions to generate a PIN. Take note of the client PIN.
5. In the router Add WPS Client screen, enter the client PIN number and click **Next**.
- The router tries to communicate with the client for 4 minutes. If no WPS clients connect during this time, the router wireless settings do not change.
  - The router WPS screen confirms that the client was added to the wireless network. The router generates an SSID and implements WPA/WPA2 wireless security.
6. Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wi-Fi Settings screen. See [Manually Configure Your Wireless Settings](#) on page 32.

To access the Internet from any computer connected to your router, launch an Internet browser. You should see the router's Internet Port LED blink.

## Add Wireless Computers That Do Not Support WPS

If you set up your network with WPS, and now you want to add a computer that does not support WPS, you must manually configure that computer. For information about how to view the wireless settings for the router, see [Manually Configure Your Wireless Settings](#) on page 32.

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

---

**Note:** When you make these changes, all wireless computers and devices disconnect from network. You then have to set them up with the new wireless settings.

---

### ➤ To change wireless settings for the network:

1. Use an Ethernet cable to connect a computer to the router. That way you do not get disconnected when you change the wireless settings.

2. Log in to the router and select **Wi-Fi Settings** (see [Manually Configure Your Wireless Settings](#) on page 32).
3. Make the following changes:
  - Change the wireless network name (SSID) to a meaningful name.
  - On the WPA/PSK + WPA2/PSK screen, select a passphrase.
  - Make sure that the **Keep Existing Wi-Fi Settings** check box is selected in the Advanced Wi-Fi Settings screen so that your new settings are not erased if you use WPS.
4. Click **Apply** so that your changes take effect. Write down your settings.

All existing wireless clients are disassociated and disconnected from the router.
5. For the non-WPS devices that you want to connect, open the networking utility and follow the utility's instructions to enter the security settings that you selected in Step 3 (the SSID, WPA/PSK + WPA2/PSK security method, and passphrase).
6. For the WPS devices that you want to connect, follow the procedure [WPS Button](#) on page 37 or [WPS PIN Entry](#) on page 38.

The settings that you configured in Step 3 are broadcast to the WPS devices so that they can connect to the router.



# Content Filtering

---

# 3

The router provides various options for blocking Internet-based content and communications services. With its content filtering feature, the router prevents objectionable content from reaching your computers. You can control access to Internet content by screening for keywords within web addresses. Content filtering options include:

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

The router allows you to restrict access to Internet content based on web addresses and web address keywords. The following sections describe how to use the basic firewall features of the router to protect your network.

- [Block Sites](#)
- [Block Services](#)
- [Schedule](#)
- [Email](#)

---

**Note:** For information about the advanced content filtering features port forwarding and port triggering, see [Port Forwarding/Port Triggering](#) on page 66.

---

---

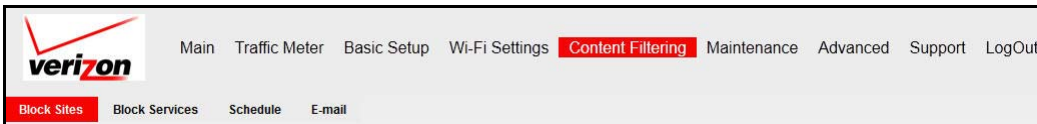
**Note:** To access online help, click the online help button (🔍).

---

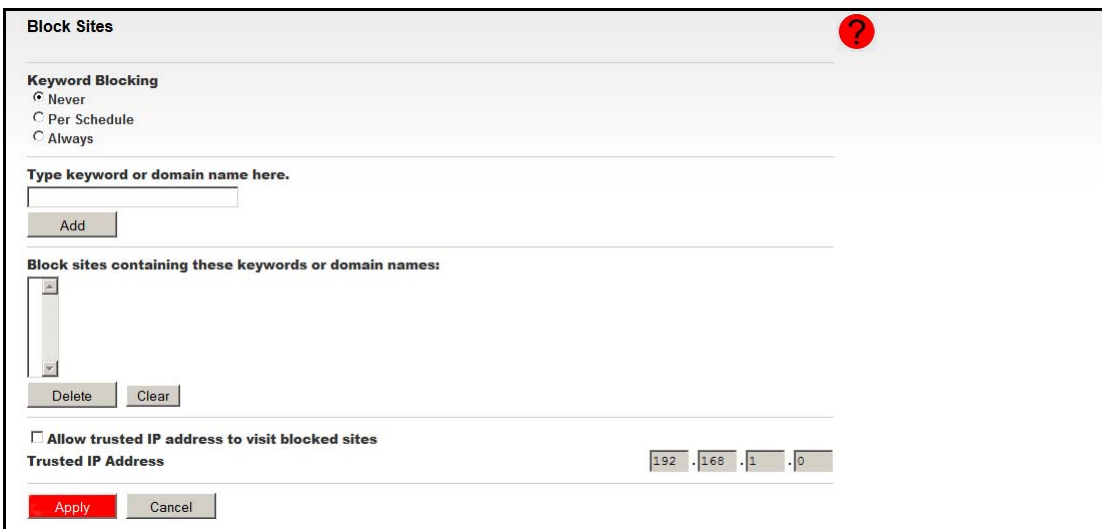
## Block Sites

➤ **To block sites:**

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Content Filtering > Block Sites**.



The following screen displays:



3. To enable keyword blocking, select one of the following:
  - **Per Schedule.** Turn on keyword blocking according to the settings on the Schedule screen. See [Schedule](#) on page 44.
  - **Always.** Turn on keyword blocking all the time, independent of the setting in the Schedule screen.
4. Enter the keyword or domain you want to block in the keyword field, click **Add Keyword** and click **Apply**.

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

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

Up to 32 entries are supported in the keyword list.

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

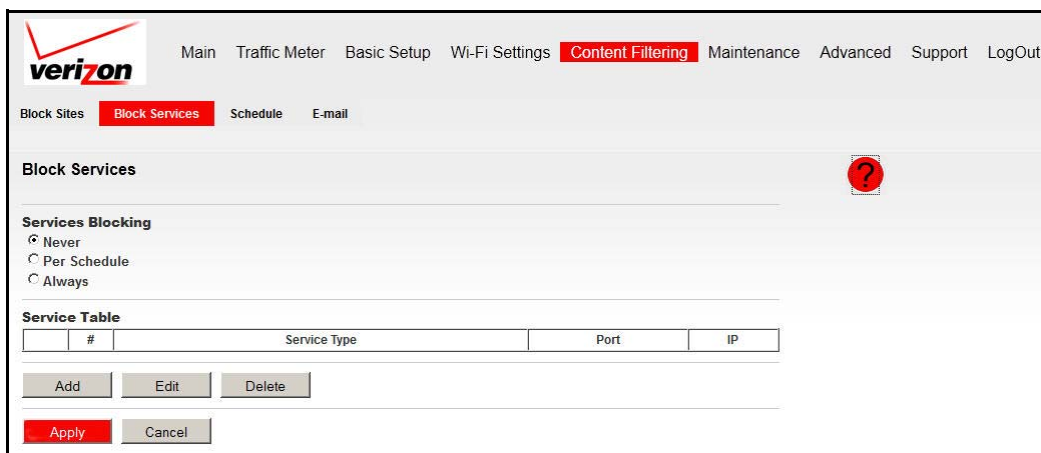
You can specify one trusted user, which is a computer that is exempt from blocking and logging. Since the trusted user is identified by an IP address, you should configure that computer with a fixed IP address.

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

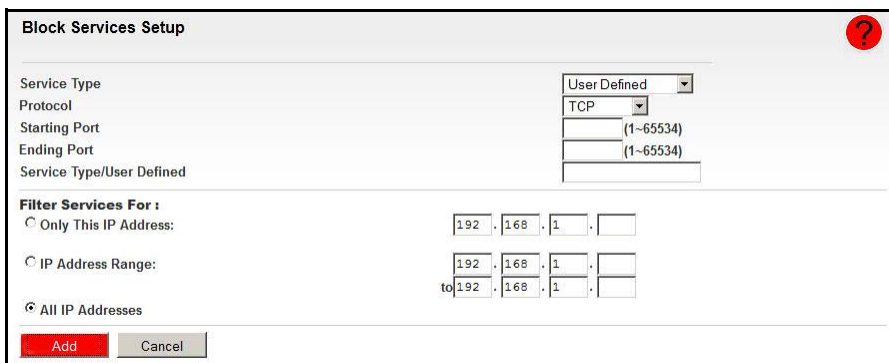
## Block Services

➤ **To block services:**

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Content Filtering > Block Services**.



3. Select one of the following:
  - **Per Schedule.** Turn on service blocking according to the settings in the Schedule screen. See [Schedule](#) on page 44.
  - **Always.** Turn on service blocking all the time, independent of the Schedule screen.
4. Click **Add**, and the following screen displays:



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

## Schedule

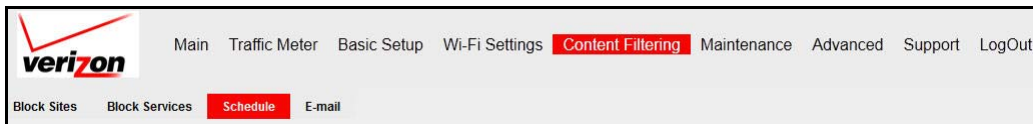
The router uses Network Time Protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet.

### Schedule Content Filtering

If you enabled keyword or service blocking in the Block Sites or Block Services screens, you can set up a schedule for when blocking occurs or when access is not restricted.

► **To schedule content filtering:**

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Content Filtering > Schedule**.



The following screen displays:

 A screenshot of the 'Schedule' configuration screen. The title is 'Schedule' with a red question mark icon in the top right. Under 'Days to Block', there are checkboxes for 'Every Day', 'Sunday', 'Monday', 'Tuesday', 'Wednesday', 'Thursday', 'Friday', and 'Saturday', all of which are checked. Under 'Time of day to block (use 24-hour clock)', there is a checked 'All Day' option. Below that are 'Start Blocking' and 'End Blocking' fields, each with 'Hour' and 'Minute' spinners. The 'End Blocking' field shows '24' in the hour spinner. Under 'Time Zone', there is a dropdown menu showing '(GMT-05:00) Bogota, Lima, Quito, Eastern Time (US & Canada)'. There is an unchecked checkbox for 'Automatically adjust for daylight savings time'. At the bottom, it shows 'Current Time: Tuesday, 14 Aug 2012 13:14:19' and two buttons: 'Apply' (highlighted in red) and 'Cancel'.

3. To block Internet keywords and services based on a schedule, select **Every Day**, or select one or more days. If you want to limit access completely for the selected days, select **All**

**Day.** Otherwise, to limit access during certain times for the selected days, fill in the Start Blocking and End Blocking fields.

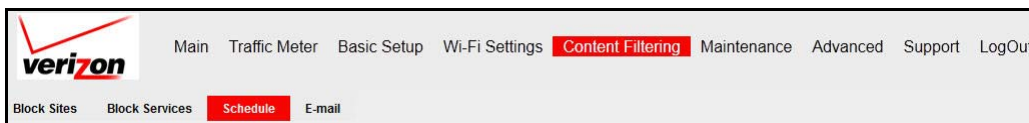
4. Enter the values in 24-hour time format. For example, 10:30 a.m. would be 10 hours and 30 minutes, and 10:30 p.m. would be 22 hours and 30 minutes. If you set the start time after the end time, the schedule will be effective through midnight the next day.
5. Click **Apply** to save your changes.

## Localize Your Time Zone

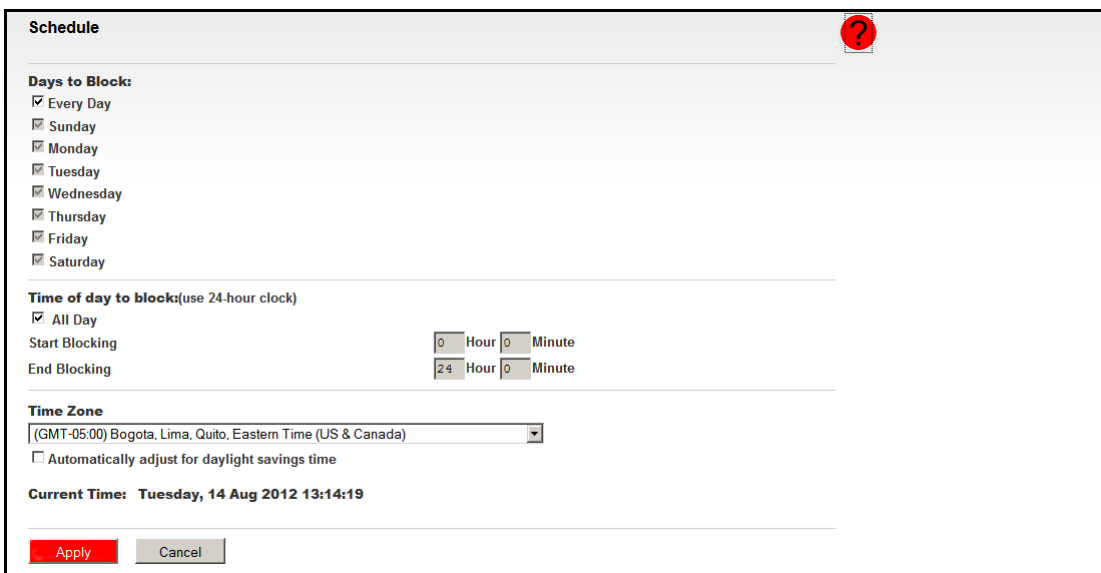
To localize the time for your log entries, you must specify your time zone.

➤ **To specify your time zone:**

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Content Filtering > Schedule**.



The following screen displays:



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

If your time zone uses daylight saving time, select the **Automatically adjust for daylight savings time** check box.

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

## Email

Set up the router so that you can receive logs and alerts by email.

➤ **To receive alerts and logs by email:**

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Content Filtering > E-mail**.

The screenshot shows the Verizon 4G LTE Router web interface. The top navigation bar includes: Main, Traffic Meter, Basic Setup, Wi-Fi Settings, **Content Filtering**, Maintenance, Advanced, Support, and LogOut. Below this, a sub-menu shows: Block Sites, Block Services, Schedule, and **E-mail**. The main content area is titled 'E-mail' and features a red question mark icon. The configuration options are as follows:

- Turn E-mail Notification On
- Send alerts and logs through e-mail**
  - Your Outgoing Mail Server: [Text Input]
  - Send to This E-mail Address: [Text Input]
  - My mail server requires authentication
    - User Name: [Text Input]
    - Password: [Text Input]
- Send Alert Immediately
 

When someone attempts to visit a blocked site
- Send logs according to this schedule**
  - None [Dropdown]
  - Day [Dropdown]
  - Time [Dropdown] a.m. p.m.

Buttons: Apply, Cancel

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

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

5. Specify when you want the alerts and logs sent:
  - **Send alert immediately.** Select this check box if you would like immediate notification of a significant security event, such as a known attack, port scan, or attempted access to a blocked site.
  - **Send logs according to this schedule.** Specifies how often to send the logs: **Hourly, Daily, Weekly, or When Full.**

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

If the Weekly, Daily, or Hourly option is selected and the log fills up before the specified period, the log is automatically emailed to the specified email address. After the log is sent, it is cleared from the 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.

6. Click **Apply** so that your changes take effect.

# Maintenance


---

# 4

This chapter describes how to perform network management tasks with your Verizon 4G LTE Router.

- *Router Status*
- *Attached Devices*
- *Back Up Settings*
- *Set Password*
- *Diagnostics*
- *Logs*

---

**Note:** To access online help, click the online help button (  ).

---

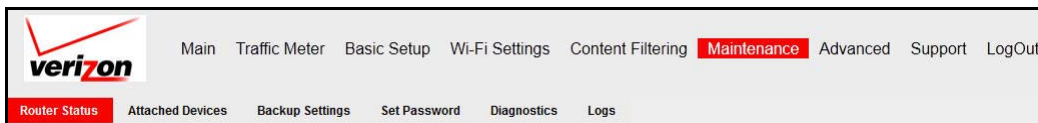


## Router Status

Use the Router Status screen to view the status of the router, show statistics, or view the connection status.

➤ **To view the router status:**

1. Log in to the router as described in *Log In to Your Router* on page 17.
2. From the main menu, select **Maintenance > Router Status**.



The following screen displays:

Main Traffic Meter Basic Setup Wi-Fi Settings Content Filtering **Maintenance** Advanced Support LogOut

**Router Status**
Attached Devices Backup Settings Set Password Diagnostics Logs

---

**Active Connection**

4G LTE Broadband **4G**

---

**Account Name**

MBR1515

**Firmware Version**

V1.2.2.69\_R2

---

**WAN Broadband**

**MAC Address** 84:1B:5E:D3:F9:09

**IP Address** 0.0.0.0

**Network Type** DHCPClient

**IP Subnet Mask** 0.0.0.0

**Gateway IP Address** 0.0.0.0

**Domain Name Server** 0.0.0.0

**Modem Identity**

**Modem SW version**

**Modem driver version**

**IMSI**

**MDN**

**UICC**

**Access Number** \*99\*\*\*\*3#

**IMEI**

**Operator**

**Network mode**

**Network band**

---

**LAN Port**

**MAC Address** 84:1B:5E:D3:F9:08

**IP Address** 192.168.1.1

**DHCP** ON

**IP Subnet Mask** 255.255.255.0

---

**Wi-Fi Port**

**Name (SSID)** Verizon-MBR1515-F908

**Region** United States

**Channel** Auto ( 8(P)+4(S) )

**Wi-Fi AP** On

**Broadcast Name** On

---

Connection Status
Refresh
Show Statistics

The following information is displayed:

- **Active Connection.** The selected broadband connection (for example, 4G LTE Broadband or WAN Ethernet).
- **Account Name.** The model of the router.
- **Firmware Version.** This field displays the router firmware version.
- **WAN Broadband.** See [Basic Setup: Configure Your Internet Settings](#) on page 18.
  - **MAC Address.** The MAC address used by the router's WAN port.
  - **IP Address.** The IP address used by the modem. If no address is shown, the router cannot connect to the Internet.
  - **Network Type.** DHCP Client.
  - **IP Subnet Mask.** The IP subnet mask used by the router's Internet port.
  - **Gateway IP Address.** The IP address used by the router.
  - **Domain Name Server.** The DNS server IP address used by the router. This address is obtained dynamically from the ISP.
  - **Modem Identity.** The modem in use.
  - **Modem SW version.** The software version of the modem.
  - **Modem driver version.** The driver version of the modem.
  - **IMSI.** International Mobile Subscriber Identity. The SIM card identity.
  - **MDN.** Mobile Directory Number.
  - **UICC.** Universal Integrated Circuit Card number.
  - **Access Number.** Service provider access number.
  - **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 value is dependent on coverage and distance from the cell site.
  - **Network band.** Current network band.
- **LAN Port.** See [LAN Setup](#) on page 74.
  - **MAC Address.** The Ethernet MAC address used by the router's LAN port.
  - **IP Address.** The LAN port IP address. The default is 192.168.0.1.
  - **DHCP.** If Off, the router does not assign IP addresses to computers on the LAN. If On, the router assigns IP addresses to computers on the LAN.
  - **IP Subnet Mask.** The LAN port IP subnet mask. The default is 255.255.255.0.
- **Wi-Fi Port.** See [Manually Configure Your Wireless Settings](#) on page 32.
  - **Name (SSID).** The service set ID, also known as the wireless network name.
  - **Region.** The country where the unit is set up for use.
  - **Channel.** The current channel, which determines the operating frequency.
  - **Wi-Fi AP.** Indicates if the access point feature is disabled or not. If not enabled, the Wi-Fi LED on the front panel is off.

- **Broadcast Name.** Indicates if the router is configured to broadcast its SSID.
3. Click the **Show Statistics** button on the Router Status screen to display router usage statistics:

System Up Time 1 day 00:20:20							
Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	100M/Full	53301	141308	0	79	191	00:00:00, 1 day 00:19:50
LAN1	Link Down	--	--	--	--	--	--
LAN2	Link Down	--	--	--	--	--	--
LAN3	Link Down	--	--	--	--	--	--
LAN4	Link Down	--	--	--	--	--	--
WLAN	300M	68093	64057	0	222	153	1 day 00:20:03

Poll Interval :  (secs)

The following information is displayed for each port:

- **Status.** The link status. LAN2, LAN3, and LAN4 are guest networks.
- **TxPkts.** The number of packets transmitted on this port since reset or manual clear.
- **RxPkts.** The number of packets received on this port since reset or manual clear.
- **Collisions.** The number of collisions on this port since reset or manual clear.
- **Tx B/s.** The average egress line utilization for this port.
- **Rx B/s.** The average ingress line utilization for this port.
- **Up Time.** The time elapsed since the last power cycle or reset.

You can also set the interval that the router uses to poll these statistics.

4. Click the **Connection Status** button on the Router Status screen to display the status of the Internet connection:

Mobile Broadband Status	
Connection Status	NO SIM Card Detected
Received Signal Quality(in dbm)	0
Bytes Transmitted	12092201
Bytes Received	27253480
Tx B/s	65
Rx B/s	187
System Uptime	1 day 00:19:22

Connection Status	
IP Address	192.168.0.16
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,23 Hours,41 minutes.

Poll Interval :  (secs)

The following information is displayed for each Internet connection mode:

- **Mobile Broadband Status.**
  - **Connection Status.** The status of the Internet connection.
    - **No SIM card detected.** No SIM card has been detected in the router.
    - **Detecting Modem.** The router is detecting the modem.
    - **Negotiating.** The modem is negotiating with the network.
    - **Attaching to Network.** The modem is connecting to the network.
    - **Scanning.** The modem is scanning for broadband wireless networks in your area.
    - **Connected.** The router is connected to the Internet.
  - **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 current connection session.
  - **Bytes Received.** The number of bytes received in the current connection session.
  - **Tx B/s.** The transmission rate.
  - **Rx B/s.** The receiving rate.
  - **System Uptime.** Time elapsed since the last reboot.
- **Connection Status.**
  - **IP Address.** The unique public address provided to the router by the wireless mobile network.
  - **Subnet Mask.** The subnet mask address provided to the router by the wireless mobile network.
  - **Default Gateway.** The IP address of the default gateway located within the wireless mobile network.
  - **DHCP Server.** The IP address of the DHCP server located within the wireless mobile network.
  - **DNS Server.** The IP address of the Domain Name Server located within the wireless mobile network.
  - **Lease Obtained.** A time notification of the router was provided with its unique public IP address.
  - **Lease Expires.** When the unique public IP address is due to expire. The router automatically attempts to obtain a new lease at time of expiry.

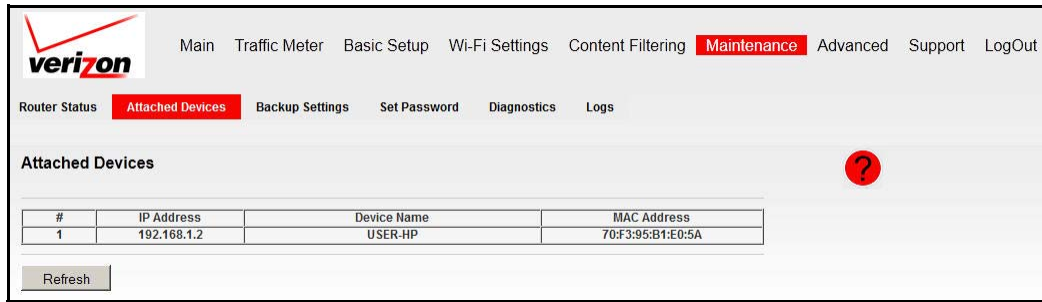
## Attached Devices

The Attached Devices screen shows all IP devices that the router discovered on the local network.

➤ **To view the attached devices:**

1. Log in to the router as described in [Log In to Your Router](#) on page 17.

- From the main menu, select **Maintenance > Attached Devices**.



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

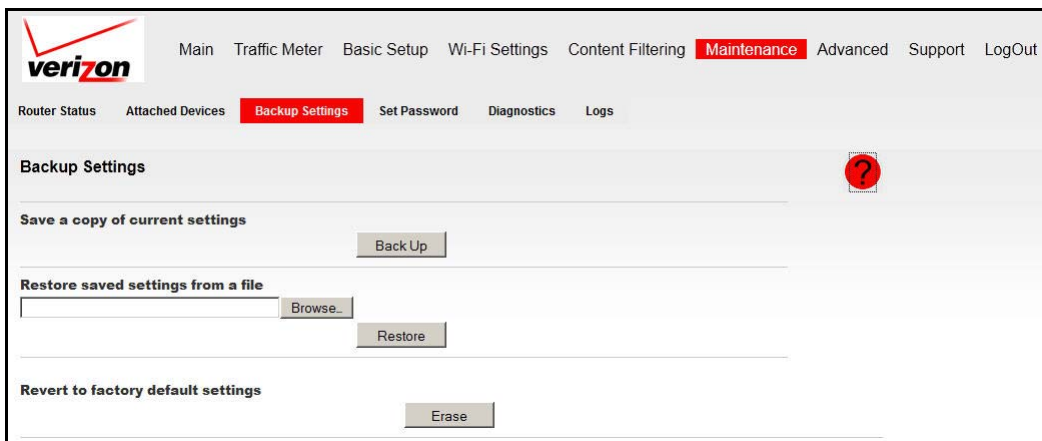
## Back Up Settings

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

### Back Up the Configuration to a File

- To back up the configuration to a file:

- Log in to the router as described in [Log In to Your Router](#) on page 17.
- From the main menu, select **Maintenance > Backup Settings**.

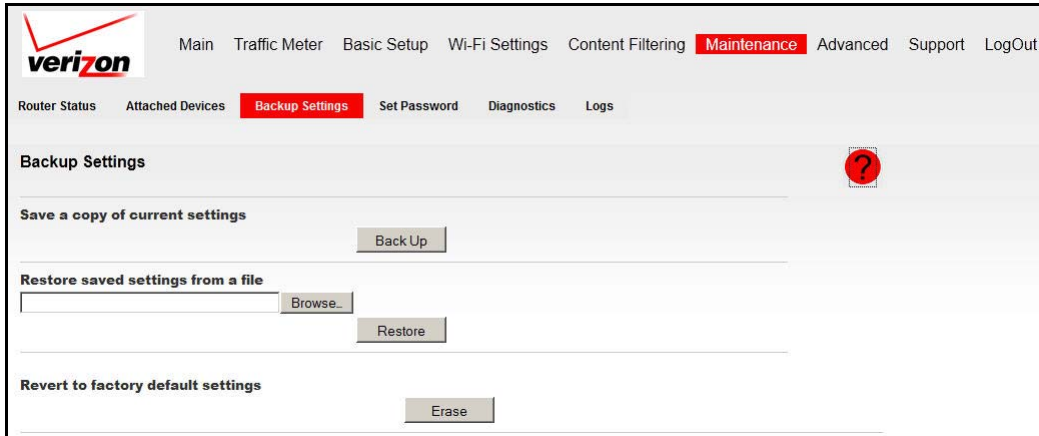


- Click **Save** to save a copy of the current settings. Store the .cfg file on a computer on your network.

## Restore the Configuration from a File

➤ To restore the configuration:

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Maintenance > Backup Settings**.



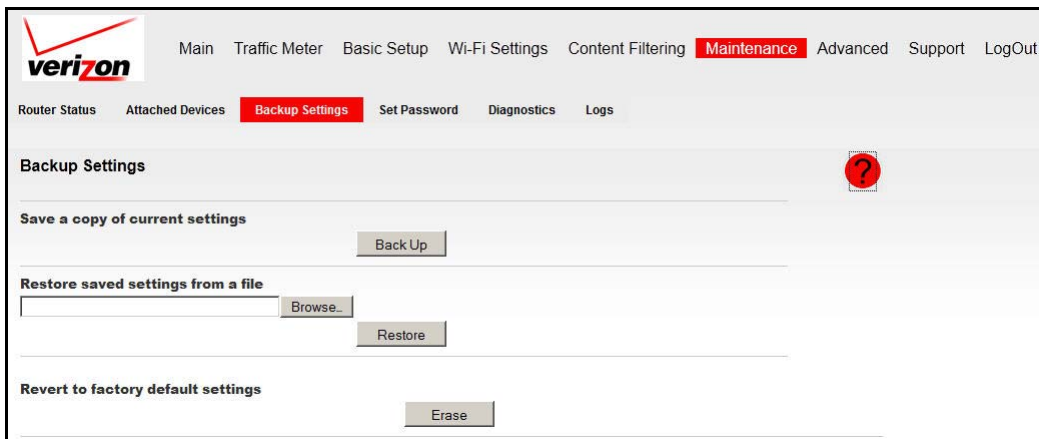
3. Enter the full path to the file on your network, or click **Browse** to locate the file.
4. When you have located the .cfg file, click **Restore** to upload the file to the router. The router reboots.

## Erase the Configuration

You can use this feature to erase the router's configuration settings and restore the factory default settings.

➤ To erase the configuration:

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Maintenance > Backup Settings**.



3. Click **Erase**. The router reboots.

After an erase procedure, the router password is **password**, the LAN IP address is **192.168.0.1**, and the router DHCP client is enabled. Also, the SSID and passphrase of the Wi-Fi link are restored to the unique factory settings. See [Router Label](#) on page 15. For the factory default settings, see [Factory Default Settings](#) on page 109.

---

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

---

## Set Password

For security reasons, the router has its own user name and password. Also, after a period of inactivity, the login automatically disconnects. The user name and password are not the same as a user name or password you might use to log in to your Internet connection.

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

## Change the Built-In Password

---

**Note:** If you changed the password and do not remember what it is, you can reset the router to its factory default settings. See [Restore the Default Configuration and Password](#) on page 103.

---

### ➤ To change the built-in password:

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Maintenance > Set Password**.

The screenshot shows the Verizon 4G LTE Router web interface. The top navigation bar includes links for Main, Traffic Meter, Basic Setup, Wi-Fi Settings, Content Filtering, Maintenance (highlighted in red), Advanced, Support, and LogOut. Below this is a sub-menu with Router Status, Attached Devices, Backup Settings, Set Password (highlighted in red), Diagnostics, and Logs. The main content area is titled 'Set Password' and features a red question mark icon. It contains three input fields: 'Old Password', 'Set Password', and 'Repeat New Password'. Below these fields is a text input for 'Administrator login times out after idle for' with a value of '60' minutes. At the bottom of the form are two buttons: 'Apply' (highlighted in red) and 'Cancel'.

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

---

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

---

## Change the Administrator Login Time-Out

For security, the administrator login to the router configuration times out after a period of inactivity. To change the login time-out period:

1. In the Set Password screen, type a number in the Administrator login times out field. The suggested default value is 60 minutes.
2. Click **Apply** to save your changes, or click **Cancel** to keep the current period.



## Diagnostics

The router has a diagnostics feature that helps you troubleshoot a network connection issue.

➤ **To use diagnostics:**

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Maintenance > Diagnostics**.

You can perform the following tests and actions:

- **Ping.** Ping an IP address.
- **Lookup.** A Domain Name Server (DNS) converts the Internet name such as [www.netgear.com](http://www.netgear.com) to an IP address. If you need the IP address of a server on the Internet, you can do a DNS lookup to find the IP address.
- **Display.** View the internal routing table. Typically, this information is used by technical support.
- **Reboot.** Shut down and restart the router. If you reboot the router, you lose your connection. To access the router, you have to log in again after it has finished rebooting.
- **Save.** Save diagnostic information.

## Logs

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

➤ **To view, send, or clear the logs:**

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Maintenance > Logs**.

verizon Main Traffic Meter Basic Setup Wi-Fi Settings Content Filtering **Maintenance** Advanced Support LogOut

Router Status Attached Devices Backup Settings Set Password Diagnostics **Logs**

Logs ?

**Current Time: Thursday, Sep 20, 2012 15:17:53**

```
[Admin login] from source 192.168.1.2, Thursday, Sep 20, 2012 14:36:12
[UPnP set event: Public_UPNP_C3] from source 192.168.1.2, Thursday, Sep 20, 2012 14:33:23
[UPnP set event: Public_UPNP_C3] from source 192.168.1.2, Thursday, Sep 20, 2012 14:32:49
[UPnP set event: Public_UPNP_C3] from source 192.168.1.2, Thursday, Sep 20, 2012 14:32:12
[UPnP set event: Public_UPNP_C3] from source 192.168.1.2, Thursday, Sep 20, 2012 14:31:35
[UPnP set event: Public_UPNP_C3] from source 192.168.1.2, Thursday, Sep 20, 2012 14:31:03
[UPnP set event: Public_UPNP_C3] from source 192.168.1.2, Thursday, Sep 20, 2012 14:30:27
[UPnP set event: Public_UPNP_C3] from source 192.168.1.2, Thursday, Sep 20, 2012 14:29:43
[UPnP set event: Public_UPNP_C3] from source 192.168.1.2, Thursday, Sep 20, 2012 14:29:00
[UPnP set event: Public_UPNP_C3] from source 192.168.1.2, Thursday, Sep 20, 2012 14:28:19
[UPnP set event: Public_UPNP_C3] from source 192.168.1.2, Thursday, Sep 20, 2012 14:27:41
[UPnP set event: Public_UPNP_C3] from source 192.168.1.2, Thursday, Sep 20, 2012 14:27:07
[UPnP set event: Public_UPNP_C3] from source 192.168.1.2, Thursday, Sep 20, 2012 14:26:29
[UPnP set event: Public_UPNP_C3] from source 192.168.1.2, Thursday, Sep 20, 2012 14:25:48
[UPnP set event: Public_UPNP_C3] from source 192.168.1.2, Thursday, Sep 20, 2012 14:25:07
[UPnP set event: Public_UPNP_C3] from source 192.168.1.2, Thursday, Sep 20, 2012 14:24:25
```

Refresh Clear Log Send Log Save Log

---

**Note:** You can enable email notification to receive these logs in an email message. See [Email](#) on page 46.

---



**WARNING:**

**Setting features that are described in this chapter requires advanced network knowledge and experience.**

This chapter describes how to configure the advanced features of your Verizon 4G LTE Router.

- *Access Control*
- *Advanced Wi-Fi Settings*
- *Wi-Fi Repeating Function*
- *Port Forwarding/Port Triggering*
- *Miscellaneous*
- *LAN Setup*
- *QoS Setup*
- *Dynamic DNS*
- *Static Routes*
- *Remote Management*
- *UPnP*
- *IPv6*

Broadband Settings are described in *Broadband Settings* on page 19.

---

**Note:** To access online help, click the online help button ( ? ).

---

## Access Control

Use access control to allow or block access to your network by computers and electronic devices. When a device is blocked, it is able to get an IP address from your router, but it is not able to communicate with other devices, nor is it able to connect to the Internet.

➤ **To set up access control:**

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Advanced > Access Control**.

**Access Control**

You can use Access Control to allow or block computers or electronic devices from accessing your network.

Turn on Access Control

Access Rule: This is a general rule. You can also allow or block individual devices.

Allow all new devices to connect

Block all new devices from connecting

allow block refresh

<input type="checkbox"/>	Status	Device Name	IP Address	MAC Address	Connection Type
<input type="checkbox"/>	Allowed	USER-HP	192.168.1.2	70:F3:95:B1:E0:5A	

▶ View list of allowed devices not currently connected to the network

▶ View list of blocked devices not currently connected to the network

Apply Cancel

The following settings are available:

- To enable access control, select the **Turn on Access Control** check box.  
Selecting this check box lets you control access to your network by computers and electronic devices. You have to select this check box before you can specify an access rule and use the Allow and Block buttons. When this check box is cleared, all devices are allowed to connect, even if a device is in the blocked list.
- Select the Access Rule radio button for the access rule that you want to apply to new devices that are attempting to connect to your network.  
The access rule does not affect previously blocked or allowed devices. It applies only to devices joining your network in the future, after you apply these settings. By default, the Allow all new devices to connect radio button is selected so that when you or your family buys a new device, the device is able to access your network without the need for you to configure its MAC address in this screen.

Verizon recommends that you keep this option selected. If you change this setting to the Block all new devices from connecting radio button, your new device is not able to access your network until you add its MAC address to the allowed list. For example, if

a new computer has both wireless and Ethernet network connections, each connection has its own MAC address, and you need to add both MAC addresses to the allowed list.

- c. To allow or block access for a specific device, select the check box of the specific device and then click the **Allow** or **Block** radio button to change its status.
3. Click **Apply** to save your settings.

## Advanced Wi-Fi Settings



### WARNING:

The Wi-Fi router is already configured with the optimum settings. Do not alter these settings unless directed by Verizon support. Incorrect settings disable the Wi-Fi router.

#### ➤ To change the advanced Wi-Fi settings:

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Advanced > Wi-Fi Settings**.

The screenshot shows the Verizon 4G LTE Router's web interface. The top navigation bar includes links for Main, Traffic Meter, Basic Setup, Wi-Fi Settings, Content Filtering, Maintenance, **Advanced**, Support, and LogOut. Below this, a secondary menu lists various settings categories, with **Wi-Fi Settings** highlighted in red. The main content area is titled "Advanced Wi-Fi Settings" and contains the following sections:

- Advanced Wi-Fi Settings:**
  - Enable Wi-Fi Router Radio
  - Enable SSID Broadcast
  - Fragmentation Length (256-2346):
  - CTS/RTS Threshold (1-2347):
  - Preamble Mode:
- WPS Settings:**
  - Router's PIN: **39282484**
  - Disable Router's PIN
  - Keep Existing Wi-Fi Settings
- Wi-Fi Card Access List:**

At the bottom of the page, there are two buttons: **Apply** (highlighted in red) and **Cancel**.

The following settings are available:

- **Advanced Wi-Fi Settings.** See [Wireless Station Access Control](#) on page 62.
  - **Enable Wi-Fi Router Radio.** Selected by default, this setting enables the wireless radio, which allows the router to work as a wireless access point. Turning off the wireless radio can be helpful for configuration, network tuning, or troubleshooting.
  - **Enable SSID Broadcast.** By default, the router is set to broadcast its wireless network name (SSID). See [Wireless Station Access Control](#) on page 62.

- **Fragmentation Length, CTS/RTS Threshold, and Preamble Mode.** These settings should be left at their default values.
- **WPS Settings.** See [Use Push 'N' Connect \(WPS\) to Configure Your Wireless Network](#) on page 36.
  - **Router's PIN.** The PIN number used for Push 'N' Connect.
  - **Disable Router's PIN.** By default, this check box is cleared. When the check box is selected, this setting allows the WPS clients to discover the router's PIN.
  - **Keep Existing Wi-Fi Settings.** By default, this check box is cleared. When the check box is selected, this setting allows the router to automatically generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the router automatically selects the Keep Existing Wi-Fi Settings check box so that your SSID and wireless security settings remain the same if other WPS-enabled devices are added later.
- **Wi-Fi Card Access List.** See [Restrict Access by MAC Address](#) on page 63.

## Wireless Station Access Control

By default, any wireless computer configured with the correct SSID and wireless security settings is allowed access to your wireless network. You can use wireless access point settings in the Advanced Wi-Fi Settings screen to further restrict wireless access to your network:

- **Turn off wireless connectivity completely.**

You can completely turn off the wireless portion of the router. For example, if you use your notebook computer to connect wirelessly to your router, and you take a business trip, you can turn off the wireless portion of the router while you are traveling. Other members of your household who use computers connected to the router with Ethernet cables can still use the router. To make this change, clear the **Enable Wi-Fi Router Radio** check box in the Advanced Wi-Fi Settings screen and click **Apply**.
- **Hide your wireless network name (SSID).**

By default, the router is set to broadcast its wireless network name (SSID). You can restrict wireless access to your network by not broadcasting the wireless network name (SSID). To make this change, clear the **Enable SSID Broadcast** check box on the Advanced Wi-Fi Settings screen and click **Apply**. Wireless devices do not see your router. You must configure your wireless devices to match the wireless network name (SSID) of the router.

---

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

---

## Restrict Access by MAC Address

For increased security, you can restrict access to the wireless network to allow only specific computers based on their MAC addresses. You can restrict access to only trusted computers so that unknown computers cannot connect wirelessly to the Verizon 4G LTE Router. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the Wi-Fi link is fully exposed.

---

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

---

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

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Advanced > Wi-Fi Settings** and click the **Set Up Access List** button. The following screen displays:

The screenshot shows the router's web interface. The top navigation bar includes 'Main', 'Traffic Meter', 'Basic Setup', 'Wi-Fi Settings', 'Content Filtering', 'Maintenance', 'Advanced' (highlighted), 'Support', and 'LogOut'. Below this, a secondary menu has 'Broadband Settings', 'Access Control', 'Wi-Fi Settings' (highlighted), 'Wi-Fi Repeating Function', 'Port Forwarding/Triggering', 'Miscellaneous', 'LAN Setup', and 'QoS Setup'. Under 'Access Control', there are links for 'Dynamic DNS', 'Static Routes', 'Remote Management', 'UPnP', and 'IPv6'. The main content area is titled 'Wi-Fi Card Access List' and features a red question mark icon. A checkbox labeled 'Turn Access Control On' is present and is not checked. Below the checkbox is a table with two columns: 'Device Name' and 'MAC Address'. Under the table are three buttons: 'Add', 'Edit', and 'Delete'. At the bottom of the page are two buttons: 'Apply' and 'Cancel'.

3. To enable access control, select the **Turn Access Control On** check box. Otherwise, access control is disabled by default so that any computer configured with the correct SSID can connect.

4. To add specific wireless devices and computers to the access list, click the **Add** button. The following screen displays:

The screenshot shows the Verizon 4G LTE Router MBR1515LVW web interface. The navigation menu includes: Main, Traffic Meter, Basic Setup, Wi-Fi Settings, Content Filtering, Maintenance, **Advanced**, Support, and LogOut. The sub-menu includes: Broadband Settings, Access Control, **Wi-Fi Settings**, Wi-Fi Repeating Function, Port Forwarding/Triggering, Miscellaneous, LAN Setup, and QoS Setup. The main content area is titled "Wi-Fi Card Access List" and features a red question mark icon. Below this is a section for "Available Wi-Fi Cards" with a table:

	Device Name	MAC Address
<input type="checkbox"/>	User-HP	70:f3:95:b1:e0:5a

Below the table is a "Wireless Card Entry" section with two input fields: "Device Name:" and "MAC Address:". At the bottom are three buttons: "Add", "Cancel", and "Refresh".

5. You can add devices to the list using either of the following methods:
- If the computer is in the Available Wi-Fi Cards table, select its radio button to capture its MAC address.
  - Use the Wireless Card Entry fields to enter the MAC address of the device that is to be added. The MAC address can usually be found on the bottom of the wireless device.
  - If no device name appears when you enter the MAC address, you can type a descriptive name for the computer that you are adding.
6. Click **Apply** to save these settings. Now, only devices on this list are allowed to connect wirelessly to the router.

---

**Note:** You can also restrict access using the Access Control screen. See [Access Control](#) on page 60.

---



## Wi-Fi Repeating Function

The following restrictions apply when you are using the Wi-Fi repeating function:

- The Wi-Fi security options WPA-PSK (TKIP), WPA2-PSK (AES), and WPA-PSK (TKIP) + WPA2-PSK (AES) are not available when you enable the Wi-Fi repeating function. See [Configure WEP](#) on page 35.
- The Wi-Fi repeating function cannot be used with Auto Channel. See [Manually Configure Your Wireless Settings](#) on page 32.

➤ **To configure the Wi-Fi repeating function:**

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Advanced > Wi-Fi Repeating Function**.

3. To use either bridge mode or repeater mode, select **Enable Wi-Fi Repeating Function**.
4. Select the mode you want for your environment:
  - **Wi-Fi Repeater.** In this mode, the MBR1515LVW communicates *only* with another Base Station–mode wireless station. You must enter the MAC address (physical address) of the other Base Station–mode wireless station in the field provided. WEP / WPA-PSK [TKIP] can (and should) be used to protect this communication.
  - **Wi-Fi Base Station.** Select this option only if this MBR1515LVW is the master for a group of Repeater-mode wireless stations. The other Repeater-mode wireless stations must be set to Wi-Fi Repeater-mode, using this MBR1515LVW's MAC address. They then send all traffic to this master, rather than communicating directly with each other. WEP can (and should) be used to protect this traffic. If this option is selected, you must enter the MAC addresses of the other access points in the fields provided.
5. Click **Apply** to save your settings.

## Port Forwarding/Port Triggering

By default, the router blocks inbound traffic from the Internet to your computers except for replies to your outbound traffic. 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 your router does not recognize their replies.

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 accesses 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.** The IP address of your computer.

**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 the public IP address of your router. This step 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 that is chosen by the router, such as 33333. This step 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 an active session for port number 33333 exists. Finding an active session, the router then modifies the message to restore the original address information that is 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.** The IP address of your computer.

**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 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 to multiple port numbers. Using the port triggering function of your router, you can tell the router to open more 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 allow incoming traffic also 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 an active session for port number 33333 exists. Finding an active session, the router restores the original address information that is 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 an active session for port 113 exists and is associated with your computer. The router replaces the destination IP address of the message with the IP address of your computer 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 ports 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 triggers 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 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 browser on a remote computer accesses 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 is 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. Usually you can determine this information by contacting the publisher of the application or the relevant user groups and news groups.

## 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 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 is never triggered.

## Set Up Port Forwarding

### ➤ To set up port forwarding:

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Advanced > Port Forwarding/Triggering**.

The screenshot shows the Verizon router's web interface. The top navigation bar includes 'Main', 'Traffic Meter', 'Basic Setup', 'Wi-Fi Settings', 'Content Filtering', 'Maintenance', 'Advanced' (highlighted), 'Support', and 'LogOut'. Below this, a secondary menu shows 'Port Forwarding/Triggering' as the active section. The main content area is titled 'Port Forwarding / Port Triggering' and contains a red question mark icon. Under 'Please select the service type.', the 'Port Forwarding' radio button is selected. Below this, there are fields for 'Service Name' (a dropdown menu showing 'Age-of-Empire') and 'Server IP Address' (a dotted IP field with '192', '168', '1', and a blank space, followed by an 'Add' button). At the bottom, there is a table with columns for '#', 'Service Name', 'Start Port', 'End Port', and 'Server IP Address'. Below the table are buttons for 'Edit Service', 'Delete Service', and 'Add Custom Service'.

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

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

The screenshot shows the 'Ports - Custom Services' dialog box. It has a 'Service Name' text field. Below it, 'Service Type' is a dropdown menu set to 'TCP/UDP'. 'Starting Port' and 'Ending Port' are dotted IP fields, both containing '(1-65534)'. 'Server IP Address' is a dotted IP field with '192', '168', '1', and a blank space. At the bottom are 'Apply' and 'Cancel' buttons.

The added service appears in the list.

## Set Up Port Triggering

### ➤ To set up port triggering:

1. Log in to the router as described in [Log In to Your Router](#) on page 17.

- From the main menu, select **Advanced > Port Forwarding/Triggering**. Then select the **Port Triggering** radio button to display the following screen:

verizon Main Traffic Meter Basic Setup Wi-Fi Settings Content Filtering Maintenance **Advanced** Support LogOut

Broadband Settings Access Control Wi-Fi Settings Wi-Fi Repeating Function **Port Forwarding/Triggering** Miscellaneous LAN Setup QoS Setup  
Dynamic DNS Static Routes Remote Management UPnP IPv6

**Port Forwarding / Port Triggering** ?

Please select the service type.

Port Forwarding  
 Port Triggering

Disable Port Triggering

Port Triggering Time-out(in minutes)

**Port Triggering Portmap Table**

#	Enable	Service Name	Service Type	Inbound Connection	Service User

Add Service Edit Service Delete Service

Apply Cancel

- Click **Add Service** and fill in the fields in the Port Triggering - Services screen. Then click **Apply**.

verizon Main Traffic Meter Basic Setup Wi-Fi Settings Content Filtering Maintenance **Advanced** Support LogOut

Broadband Settings Access Control Wi-Fi Settings Wi-Fi Repeating Function **Port Forwarding/Triggering** Miscellaneous LAN Setup QoS Setup  
Dynamic DNS Static Routes Remote Management UPnP IPv6

**Port Triggering - Services**

**Service**

Service Name

Service User

Service Type

Triggering Port

**Inbound Connection**

Connection Type:

Starting Port

Ending Port

Apply Cancel

The added service appears in the list.



## Miscellaneous

To change broadband Internet connection settings, use the Broadband Settings screen, as described in [Basic Setup: Configure Your Internet Settings](#) on page 18.

➤ **To view or change the WAN setup:**

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Advanced > Miscellaneous**.

The screenshot shows the 'Miscellaneous' settings page in the Verizon 4G LTE Router's web interface. The page has a navigation bar at the top with 'Advanced' highlighted. Below the navigation bar, there are several tabs, with 'Miscellaneous' selected. The settings include:

- Disable Port Scan and DoS Protection**
- Default DMZ Server** (IP address: 192.168.1.0)
- Respond to Ping on Internet Port**
- MTU Size (in bytes)** (Value: 1500)
- NAT Filtering** (Options:  Secured,  Open)
- Disable SIP ALG**

At the bottom of the page, there are 'Apply' and 'Cancel' buttons. A red question mark icon is located in the top right corner of the settings area.

3. Specify the following settings:

- **Disable Port Scans and DoS Protections.** This check box is cleared so that the firewall protects your LAN against port scans and denial of service attacks. This check box should be selected only in special circumstances.
- **Default DMZ Server.** This feature is sometimes helpful when you are using some online games and videoconferencing. Be careful when using this feature because it makes the firewall security less effective. See [Set Up a Default DMZ Server](#) on page 73.
- **Respond to Ping on Internet.** If you want the router to respond to a ping from the Internet, select this check box. This feature should be used only as a diagnostic tool, since it allows your router to be discovered. Do not select this check box unless you have a specific reason to do so.
- **MTU Size.** Maximum transmit unit (MTU) value. For most Ethernet networks, this setting is 1500 bytes, or 1492 bytes for PPPoE connections, or 1436 bytes for PPTP connections.
- **NAT Filtering.** This parameter is set to **Secured** to provide a secure firewall to protect computers on the LAN from attacks from the Internet. The Open setting is less secure.
- **Disable SIP ALG.** Some VoIP applications do not work well with SIP ALG. Selecting this check box might help your VoIP devices create or accept a call through the router.

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



## Set Up a Default DMZ Server



### WARNING:

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

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

Incoming traffic from the Internet is normally discarded by the router unless the traffic is a response to one of your local computers or a service that you have configured in the Port Forwarding/Port Triggering screen. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the default DMZ server.

### ➤ To assign a computer or server to be a default DMZ server:

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Advanced > Miscellaneous**.

The screenshot shows the Verizon router's web interface. At the top, there is a navigation bar with the Verizon logo and menu items: Main, Traffic Meter, Basic Setup, Wi-Fi Settings, Content Filtering, Maintenance, **Advanced**, Support, and LogOut. Below this is a sub-menu for the 'Advanced' section, including: Broadband Settings, Access Control, Wi-Fi Settings, Wi-Fi Repeating Function, Port Forwarding/Triggering, **Miscellaneous**, LAN Setup, and QoS Setup. The 'Miscellaneous' page is displayed, featuring a red question mark icon in the top right corner. The settings include:
 

- Disable Port Scan and DoS Protection
- Default DMZ Server, with an IP address field containing 192.168.1.0
- Respond to Ping on Internet Port
- MTU Size (in bytes) field containing 1500
- NAT Filtering section with radio buttons for Secured (selected) and Open
- Disable SIP ALG

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

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

## LAN Setup

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

The router is shipped preconfigured to use private IP addresses on the LAN side, and to act as a DHCP server. The router'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 Internet Engineering Task Force (IETF)–designated private address range for use in private networks, and should be suitable in most applications. If your network requires a different IP addressing scheme, you can make the changes in this screen.

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

### ➤ To view or change the LAN setup:

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Advanced > LAN Setup**.

LAN Setup

Device Name: MBR1515

LAN TCP/IP Setup

IP Address: 192 . 168 . 1 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

RIP Direction: Both

RIP Version: Disabled

Use Router as DHCP Server

Starting IP Address: 192 . 168 . 1 . 2

Ending IP Address: 192 . 168 . 1 . 254

Disable NAT/NAPT

Address Reservation

#	IP Address	Device Name	MAC Address

Add Edit Delete

**Note:** The default DHCP and TCP/IP values work for most users.

3. Specify the following settings:

- **Device Name.** This value is the name of the router.
- **LAN TCP/IP Setup.**
  - **IP Address.** The LAN IP address of the router.
  - **IP Subnet Mask.** The LAN subnet mask of the router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.
  - **RIP Direction.** RIP (Routing Information Protocol, RFC1058 and RFC1389) allows a router to exchange routing information with other routers. The RIP Direction selection controls how the router sends and receives RIP packets. Both is the default.
    - When set to Both or Out Only, the router broadcasts its routing table periodically.
    - When set to Both or In Only, it incorporates the RIP information that it receives.
  - **RIP Version.** This setting controls the format and the broadcasting method of the RIP packets that the router sends. (It recognizes both formats when receiving.) By default, Disabled is selected.
    - RIP-1 is universally supported. RIP-1 is probably adequate for most networks, unless you have an unusual network setup.
    - RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format.
      - RIP-2B uses subnet broadcasting.
      - RIP-2M uses multicasting.
- **DHCP Server.** For more information, see [DHCP Settings](#) on page 76.
  - **Use Router as a DHCP Server.** This check box is selected so that the router functions as a Dynamic Host Configuration Protocol (DHCP) server. See [DHCP Settings](#) on page 76.
  - **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.
- **Disable NAT/NAPT.** Disable network address and port translation.
- **Address Reservation.** For more information, see [Reserved IP Addresses](#) on page 76.

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.

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

## DHCP Settings

By default, the router functions as a Dynamic Host Configuration Protocol (DHCP) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the router's LAN. The assigned default gateway address is the LAN address of the router. IP addresses are assigned to the attached computers from a pool of addresses specified in this screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the router are satisfactory.

### *Use Router as DHCP Server*

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

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

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

- An IP address from the range you have defined.
- Subnet mask.
- Gateway IP address is the router's LAN IP address.
- Primary DNS server, if you entered a primary DNS address in the Broadband Settings screen; otherwise, the router's LAN IP address.
- Secondary DNS server, if you entered a secondary DNS address in the Broadband Settings screen.
- WINS server (Windows Internet Naming Service server) determines the IP address associated with a particular Windows computer. A WINS server records and reports a list of names and IP address of Windows computers on its local network. If you connect to a remote network that contains a WINS server, enter the server's IP address here. This procedure allows your computers to browse the network using the Network Neighborhood feature of Windows.

## Reserved IP Addresses

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

### ➤ **To reserve an IP address:**

1. Log in to the router as described in [Log In to Your Router](#) on page 17.

- From the main menu, select **Advanced > LAN Setup**. Then under Address Reservation, click the **Add** button. The following screen displays:

The screenshot shows the Verizon 4G LTE Router MBR1515LVW web interface. The navigation menu at the top includes: Main, Traffic Meter, Basic Setup, Wi-Fi Settings, Content Filtering, Maintenance, **Advanced**, Support, and LogOut. Below this, there are sub-menus: Broadband Settings, Access Control, Wi-Fi Settings, Wi-Fi Repeating Function, Port Forwarding/Triggering, Miscellaneous, **LAN Setup**, and QoS Setup. Under LAN Setup, there are links for Dynamic DNS, Static Routes, Remote Management, UPnP, and IPv6.

The main content area is titled "Address Reservation". It contains an "Address Reservation Table" with the following data:

	#	IP Address	Device Name	MAC Address
<input type="radio"/>	1	192.168.1.2	USER-HP	70:f3:95:b1:e0:5a

Below the table are input fields for:

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

At the bottom of the form are three buttons: **Add**, **Cancel**, and **Refresh**.

- In the IP Address field, type the IP address to assign to the computer or server. Choose an IP address from the router's LAN subnet, such as 192.168.0.x.
- Type the MAC address of the computer or server.

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

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

---

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

---

## QoS Setup

Quality of Service (QoS) is an advanced feature that can be used to prioritize some Internet applications and online gaming, and to minimize the impact when the bandwidth is busy.

► **To set up QoS:**

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Advanced > QoS Setup**.

3. Specify the following settings:
  - **Enable WMM Wi-Fi multimedia settings.** WMM (Wireless Multimedia) is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities depending on the kind of data. Time-dependent information, such as video or audio, has a higher priority than normal traffic. For WMM to function correctly, wireless clients must also support WMM.
  - **Turn Internet Access QoS On.** If you enable QoS, the QoS function works to prioritize Internet access traffic. For the applications that exist in the drop-down list (for example, Online Gaming, Ethernet LAN Port, or a specified MAC address), you can modify the priority level by clicking the **Edit** button. You can also click the **Delete** button to erase the priority rule. Otherwise, you can define the priority policy for online gaming, an application, a LAN port, or the computer's MAC address by clicking the **Setup QoS rule** button.
  - **Turn Bandwidth Control On.** To set up the total maximum uplink bandwidth, select this check box.
4. Click **Apply** to save the changes.

## QoS Priority Rule List

➤ To set up a QoS priority rule:

1. From the main menu, select **Advanced > QoS Setup**. Under the QoS Priority Rule List setting, click **Setup QoS rule**. The following screen displays:

**QoS Priority Rule list**

	#	QoS Policy	Priority	Description
<input type="radio"/>	1	MSN Messenger	High	MSN Messenger Applications
<input type="radio"/>	2	Yahoo Messenger	High	Yahoo Messenger Applications
<input type="radio"/>	3	IP Phone	Highest	IP Phone Applications
<input type="radio"/>	4	Vonage IP Phone	Highest	Vonage IP Phone Applications
<input type="radio"/>	5	NetMeeting	High	NetMeeting Applications
<input type="radio"/>	6	AIM	High	AIM Applications
<input type="radio"/>	7	Google Talk	Highest	Google Talk Applications
<input type="radio"/>	8	Netgear EVA	Highest	Netgear EVA Applications
<input type="radio"/>	9	SSH	High	SSH Applications
<input type="radio"/>	10	Telnet	High	Telnet Applications
<input type="radio"/>	11	VPN	High	VPN Applications
<input type="radio"/>	12	FTP	Normal	FTP Applications
<input type="radio"/>	13	SMTP	Normal	SMTP Applications
<input type="radio"/>	14	WWW	Normal	WWW Applications
<input type="radio"/>	15	DNS	Normal	DNS Applications
<input type="radio"/>	16	ICMP	Normal	ICMP Applications
<input type="radio"/>	17	eMule / eDonkey	Low	eMule / eDonkey Applications
<input type="radio"/>	18	Kazaa	Low	Kazaa Applications
<input type="radio"/>	19	Gnutella	Low	Gnutella Applications
<input type="radio"/>	20	BT / Azureus	Low	BT / Azureus Applications
<input type="radio"/>	21	Counter Strike	High	Online Gaming Counter Strike
<input type="radio"/>	22	Ages of Empires	High	Online Gaming Age of Empires
<input type="radio"/>	23	Everquest	High	Online Gaming Everquest
<input type="radio"/>	24	Quake 2	High	Online Gaming Quake 2
<input type="radio"/>	25	Quake 3	High	Online Gaming Quake 3
<input type="radio"/>	26	Unreal Tournament	High	Online Gaming Unreal Tournament
<input type="radio"/>	27	Warcraft	High	Online Gaming Warcraft

2. Select the radio button of the service you want to add to the QoS priority rules list, and click **Apply**.

## QoS Priority Rules

➤ To add QoS priority rules:

From the QoS Priority Rule list screen, click **Add Priority Rule**. The priority categories described in the following sections are available:

- [For Applications or Online Gaming](#) on page 80
- [For Ethernet LAN Ports](#) on page 81
- [For MAC Addresses](#) on page 81

## For Applications or Online Gaming

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

1. Select **Applications** or **On-line Gaming** from the Priority Category list.

The screenshot shows the Verizon router's web interface. The navigation bar includes: Main, Traffic Meter, Basic Setup, Wi-Fi Settings, Content Filtering, Maintenance, **Advanced**, Support, and LogOut. Below this, a secondary navigation bar includes: Broadband Settings, Access Control, Wi-Fi Settings, Wi-Fi Repeating Function, Port Forwarding/Triggering, Miscellaneous, LAN Setup, and **QoS Setup**. The main content area is titled "QoS - Priority Rules". Under the "Priority" section, the "QoS Policy for" field is empty. The "Priority Category" dropdown is set to "Applications". Below it, the "Applications" dropdown is set to "Add a new application". The "Priority" dropdown is set to "Normal". Under the "Specified Port Range" section, the "Connection Type" dropdown is set to "TCP/UDP". The "Starting Port" and "Ending Port" fields both contain "(1-65535)". At the bottom, there are "Apply" and "Cancel" buttons.

The screenshot shows the Verizon router's web interface, similar to the previous one. The navigation bars are the same. The main content area is titled "QoS - Priority Rules". Under the "Priority" section, the "QoS Policy for" field is empty. The "Priority Category" dropdown is set to "Online Gaming". Below it, the "Applications" dropdown is set to "Add a new game". The "Priority" dropdown is set to "Normal". Under the "Specified Port Range" section, the "Connection Type" dropdown is set to "TCP/UDP". The "Starting Port" and "Ending Port" fields both contain "(1-65535)". At the bottom, there are "Apply" and "Cancel" buttons.

2. Select the Internet application or game for which you want to set the priority from the relevant list.
3. Select the priority level: **Highest**, **High**, **Normal**, or **Low**.
4. You can also type the name in the QoS Policy field for this rule if you prefer.
5. Click **Apply**.



### For Ethernet LAN Ports

➤ To set up the priority for LAN port:

1. Select **Ethernet LAN Port** from the Priority Category list.

The screenshot shows the 'QoS - Priority Rules' configuration page. The 'Priority Category' is set to 'Ethernet LAN Port'. The 'QoS Policy for' field is 'LAN Port 1'. The 'Priority' is set to 'Normal'. There are 'Apply' and 'Cancel' buttons at the bottom.

2. Select 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 in the QoS Policy field for this rule if you prefer.
5. Click **Apply**.

### For MAC Addresses

➤ To set up the priority for a specified computer identified by its MAC address:

1. Select **MAC Address** from the Priority Category list.

The screenshot shows the 'QoS - Priority Rules' configuration page for MAC addresses. The 'Priority Category' is set to 'MAC Address'. The 'QoS Policy for' field is 'Pri\_MAC\_B1E05A'. Below is a 'MAC Device List' table with one entry for 'USER-HP' with MAC address '70:F3:95:B1:E0:5A'. There are 'Add', 'Edit', 'Delete', and 'Refresh' buttons above the 'Apply' and 'Cancel' buttons.

	QoS Policy	Priority	Device Name	MAC Address
<input checked="" type="radio"/>	Pri_MAC_B1E05A	Normal	USER-HP	70:F3:95:B1:E0:5A

2. Click the **Refresh** button to update the list of computers already connected to the router.
3. Select the entry's radio button.
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 in the QoS Policy field for this rule if you prefer.
7. Click the **Edit** button.
8. Click **Apply**.

➤ **To add the priority for specified computer identified by its MAC address:**

1. Select **MAC Address** from the Priority Category list.

The screenshot shows the 'QoS - Priority Rules' configuration page. The 'Priority Category' is set to 'MAC Address'. Below this, there is a table titled 'MAC Device List' with the following data:

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

Below the table, there are input fields for 'MAC Address', 'Device Name', and 'Priority' (set to 'Normal'). At the bottom, there are buttons for 'Add', 'Edit', 'Delete', 'Refresh', 'Apply', and 'Cancel'.

2. Enter the MAC address for the computer for which you are specifying the priority rule.
3. You can also type a name that is easy to remember in the Device Name fields.
4. Select the priority level: **Highest**, **High**, **Normal**, or **Low**.
5. You can also type a name in the QoS Policy field for this rule if you prefer.
6. Click the **Add** button.
7. Click **Apply**.

## Dynamic DNS

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you do not know in advance what your IP address is, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service to register your domain to their IP address, and forward traffic directed at your domain to your frequently changing IP address.

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

**WARNING:**

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

➤ **To configure Dynamic DNS:**

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Advanced > Dynamic DNS**.

3. Access the website of one of the Dynamic DNS service providers whose URLs appear in the Service Provider drop-down list, and register for an account.

For example, for dyndns.org, visit [www.dyndns.org](http://www.dyndns.org).

4. Select the **Use a Dynamic DNS Service** check box.
5. Select the URL of your Dynamic DNS service provider.
6. Fill in the Host Name, User Name, and Password fields.

The Dynamic DNS service provider might call the host name a domain name. If your URL is [myName.dyndns.org](http://myName.dyndns.org), your host name is [myName](http://myName). The password can be a key for your Dynamic DNS account.

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

## Static Routes

Static routes provide more routing information to your router. Under normal circumstances, the router has adequate routing information after it has been configured for Internet access, and you do not need to configure more static routes. You have to configure static routes only for unusual cases such as multiple routers or multiple IP subnets on your network.

### Static Route Example

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.0.100.
- Your company's network is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the router, and a second static route was created to your local network for all 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company's firewall.

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

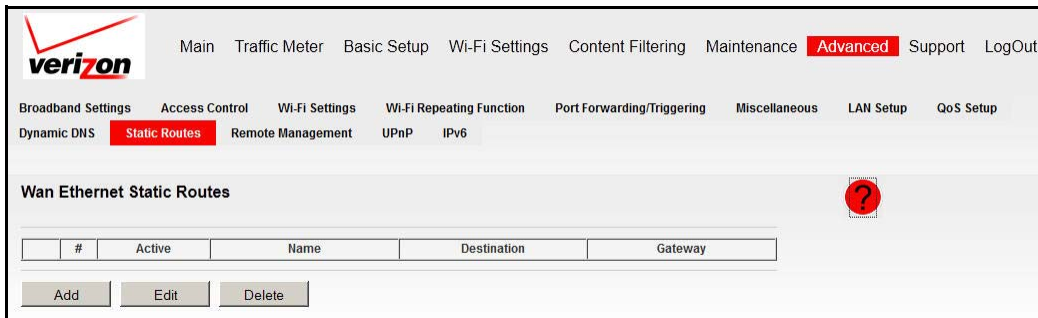
In this example:

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

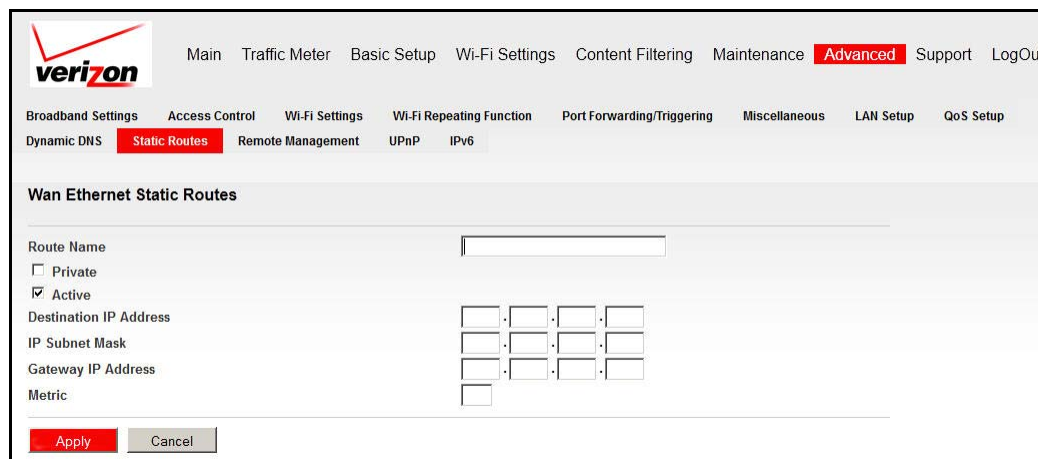
#### ➤ To configure static routes:

1. Log in to the router as described in [Log In to Your Router](#) on page 17.

- From the main menu, select **Advanced > Static Routes**.



- Select the radio button of the static route you want to configure.
- Click **Add** or **Edit** to display the following screen:



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

## Remote Management

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

**Tip:** Be sure to change the router's default password to a secure password. The ideal password contains no dictionary words from any language, and is a mixture of letters (both uppercase and lowercase), numbers, and symbols. Your password can be up to 30 characters. See [Set Password](#) on page 55.

➤ **To configure remote management:**

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Advanced > Remote Management**.

3. Select the **Turn Remote Management On** check box.
4. Specify which external addresses are allowed to access the router's remote management. For security, restrict access to as few external IP addresses as practical:
  - To allow access from any IP address on the Internet, select **Everyone**.
  - To allow access from a range of IP addresses on the Internet, select **IP Address Range**. Enter a beginning and ending IP address to define the allowed range.
  - To allow access from a single IP address on the Internet, select **Only This Computer**. Enter the IP address that is allowed access.
5. Specify the port number that is used for accessing the router menu.

Access normally uses the standard HTTP service port 80. For greater security, enter a different port number. Choose a number from 1024 through 65535, but do not use the

number of any common service port. The default is 8080, which is a common alternate for HTTP.

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

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

## UPnP

Universal Plug and Play (UPnP) helps devices such as Internet appliances and computers access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Advanced > UPnP**.

UPnP

Turn UPnP On

Advertisement Period (in minutes)

Advertisement Time to Live (in hops)

**UPnP Portmap Table**

Active	Protocol	Int. Port	Ext. Port	IP Address
YES	UDP	50858	50858	192.168.0.4

Apply Cancel Refresh

3. Specify the following settings:
  - **Turn UPnP On.** UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If this feature is disabled, the router does not allow any device to control the resources automatically, such as port forwarding (mapping), of the router.
  - **Advertisement Period.** The advertisement period is how often the router advertises (broadcasts) its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of more network traffic. Longer durations might compromise the freshness of the device status but can significantly reduce network traffic.
  - **Advertisement Time To Live.** The time to live for the advertisement is measured in hops for each UPnP packet sent. The time to live hop count is the number of steps allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, it might be necessary to increase this value a little.
  - **UPnP Portmap Table.** The UPnP Portmap table displays the IP address of each UPnP device that is accessing the router and which ports (internal and external) that device has opened.
4. Click **Refresh** to update the Portmap table and to show the active ports that are opened by UPnP devices.
5. Click **Apply** to save the new settings to the router.



## IPv6

The IPv6 screen allows you to configure and check the status of your IPv6 Internet connection.

➤ **To configure the Internet connection type:**

1. Log in to the router as described in [Log In to Your Router](#) on page 17.
2. From the main menu, select **Advanced > IPv6**.

The screenshot shows the Verizon 4G LTE Router's IPv6 configuration page. The navigation menu at the top includes Main, Traffic Meter, Basic Setup, Wi-Fi Settings, Content Filtering, Maintenance, **Advanced**, Support, and LogOut. Below the navigation menu, there are several tabs: Broadband Settings, Access Control, Wi-Fi Settings, Wi-Fi Repeating Function, Port Forwarding/Triggering, Miscellaneous, LAN Setup, and QoS Setup. Under the Broadband Settings tab, there are sub-tabs: Dynamic DNS, Static Routes, Remote Management, UPnP, and **IPv6**. The main content area is titled "Basic Settings" and features a red question mark icon. The "Internet Connection Type" dropdown menu is currently set to "Disabled". At the bottom of the form, there are "Apply" and "Cancel" buttons.

The default setting is Disabled, which turns off the IPv6 function.

3. Select the IPv6 Internet connection type you want to use, which is provided by your ISP.
  - **6to4 Tunnel**. If your ISP does not provide a specific IPv6 connection, select **6to4 Tunnel**.

The screenshot shows the Verizon 4G LTE Router's IPv6 configuration page with the "Internet Connection Type" dropdown menu set to "6to4 Tunnel". Below this, the "Remote 6to4 Relay Router" section has the "Auto" radio button selected, with a dotted IP address field. The "LAN Setup" section has "Router's IPv6 Address On LAN" set to "Not Available". Under "IP Address Assignment", the "Auto Config" radio button is selected. There is also an unchecked checkbox for "Use This Interface ID" with a dotted IP address field. At the bottom of the form, there are "Apply" and "Cancel" buttons. A red question mark icon is present in the top right corner of the configuration area.

This screen specifies the remote relay router to which your router creates the 6to4 tunnel. If your ISP provides the address of its own relay router, you can put it here. You can also leave it as Auto, and the router uses any address that is available.

---

**Note:** The 6to4 tunnel connection needs the IPv4 Internet connection to be up first.

---

In the LAN Setup section, enter the requested information:

- **Router's IPv6 Address on LAN.** This value shows the IPv6 address acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (\_\_) under the IPv6 address.
- **IP Address Assignment.** You can select how you want to assign IPv6 addresses to the devices on the LAN (for example, your home network). You can select either the Use DHCP Server or Auto Config option to assign IPv6 addresses. Using a DHCP server might pass more information to LAN devices, but some IPv6 systems might not support the DHCv6 client function. Auto Config is selected by default.
- **Use This Interface ID.** You can enable this option and specify the interface ID you want for the IPv6 address for the router's LAN interface. If you do not specify an ID here, the router generates one automatically from its MAC address.
- **Auto Detect.** If you are not clear about the IPv6 connection, select **Auto Detect**, and let the router decide the correct type for you.

Enter the requested information:

- **Connection Type.** This value indicates the connection type detected.
- **Router's IPv6 Address on WAN.** This value shows the IPv6 address acquired for the router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (\_\_) under the IPv6 address.

- **Router's IPv6 Address on LAN.** This value shows the IPv6 address acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (\_\_) under the IPv6 address.
- **IP Address Assignment.** You can select how you want to assign IPv6 addresses to the devices on the LAN (for example, your home network). You can select either the Use DHCP Server or Auto Config option to assign IPv6 addresses. Using a DHCP server might pass more information to LAN devices, but some IPv6 systems might not support the DHCv6 client function. Auto Config is selected by default.
- **Use This Interface ID.** You can enable this option and specify the interface ID you want for the IPv6 address for the router's LAN interface. If you do not specify an ID here, the router generates one automatically from its MAC address.
- **DHCP.** If your ISP indicates that your IPv6 connection is DHCP, select **DHCP**.

Enter the requested information:

- **User Class.** Most users should not need to fill in this field, but if your ISP has given you a specific host name, enter it here.
- **Domain Name.** This value is not needed for most users. You can type the domain name of your ISP. For example, if your ISP mail server is mail.xxx.yyy.zzz, you would type xxx.yyy.zzz as the domain name. If you have a domain name given to you by your ISP, type it in this field. (For example, Earthlink Cable might require a host name of home, and Comcast sometimes supplies a domain name.)

---

**Note:** This value is the domain name for the IPv6 connection. The domain name for the IPv4 connection is not specified here.

---

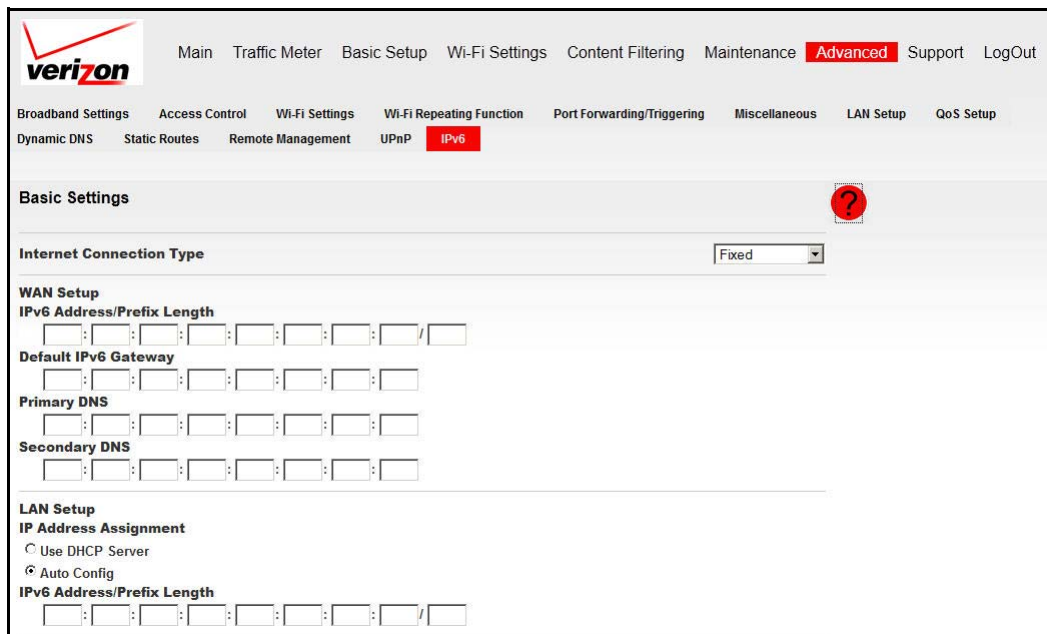
- **Router's IPv6 Address on WAN.** This value shows the IPv6 address acquired for the router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline ( ) under the IPv6 address.
- **Router's IPv6 Address on LAN.** This value shows the IPv6 address acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also roughly indicated by the underline ( ) under the IPv6 address.
- **IP Address Assignment.** You can select how you want to assign IPv6 addresses to the devices on the LAN (for example, your home network). You can select either the Use DHCP Server or Auto Config option to assign IPv6 addresses. Using a DHCP server might pass more information to LAN devices, but some IPv6 systems might not support the DHCv6 client function. Auto Config is selected by default.
- **Use This Interface ID.** You can enable this option and specify the interface ID you want for the IPv6 address for the router's LAN interface. If you do not specify an ID here, the router generates one automatically from its MAC address.
- **PPPoE.** If your ISP indicates that your IPv6 connection is PPPoE, select **PPPoE**.

The screenshot shows the Verizon 4G LTE Router MBR1515LVW Advanced Settings page. The 'Basic Settings' section is highlighted with a red question mark icon. The 'Internet Connection Type' is set to 'PPPoE'. The 'Login', 'Password', and 'Service Name' fields are empty. The 'Connection Mode' is set to 'Always On'. The 'Router's IPv6 Address On WAN' is 'Not Available'. The 'LAN Setup' section shows 'Router's IPv6 Address On LAN' as 'Not Available'. The 'IP Address Assignment' section has 'Auto Config' selected. The 'Use This Interface ID' checkbox is unchecked.

Enter the requested information:

- **Login.** This value is usually the name that you use in your email address. For example, if your main mail account is JerAB@ISP.com, type JerAB in this field. Some ISPs (like Mindspring, Earthlink, and T-DSL) require that you use your full email address when you log in. If your ISP requires your full email address, type it in the Login field.
- **Password.** Type the password that you use to log in to your ISP.
- **Service Name.** If your ISP provided a service name, enter it here. Otherwise, leave this field blank.

- **Connection Mode.** This setting specifies when the router should establish the PPPoE connection. Currently the connection mode is always on in order to provide a steady IPv6 connection. The router never disconnects the connection, and in case the connection is broken (for example, the cable or DSL modem is turned off somehow), the router brings up the connection right after the PPPoE connection is available.
- **Router's IPv6 Address on WAN.** This value shows the IPv6 address acquired for the router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline ( ) under the IPv6 address.
- **Router's IPv6 Address on LAN.** This value shows the IPv6 address acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also roughly indicated by the underline ( ) under the IPv6 address.
- **IP Address Assignment.** You can select how you want to assign IPv6 addresses to the devices on the LAN (for example, your home network). You can select either the Use DHCP Server or Auto Config option to assign IPv6 addresses. Using a DHCP server might pass more information to LAN devices, but some IPv6 systems might not support the DHCv6 client function. Auto Config is selected by default.
- **Use This Interface ID.** You can enable this option and specify the interface ID you want for the IPv6 address for the router's LAN interface. If you do not specify an ID here, the router generates one automatically from its MAC address.
- **Fixed.** If your ISP indicates that your IPv6 connection is Fixed IP, select **Fixed**.



Enter the requested information:

- **Fixed.** The fixed IPv6 connection is rarely used. If you need this type of connection, your ISP provides you with the IPv6 address configurations.

- WAN Setup:
  - **IPv6 Address/Prefix Length.** This value specifies the IPv6 address and prefix length of the router's WAN interface.
  - **Default IPv6 Gateway.** This value specifies the IPv6 address of the default IPv6 gateway, which is supposed to be on the router's WAN interface.
  - **Primary/Secondary DNS Server.** These values specify the DNS servers that resolve IPv6 domain name records for you. If these fields are not specified, the router uses the DNS servers configured for the IPv4 Internet connection (on the Broadband Settings screen).
  - **IP Address Assignment.** You can select how you want to assign IPv6 addresses to the devices on the LAN (for example, your home network). You can select either the Use DHCP Server or Auto Config option to assign IPv6 addresses. Using a DHCP server might pass more information to LAN devices, but some IPv6 systems might not support the DHCv6 client function. Auto Config is selected by default.
- LAN Setup:
  - **IPv6 Address/Prefix Length.** This setting specifies the IPv6 address and prefix length of the router's LAN interface.
- **Auto Config.** If your ISP indicates that your IPv6 connection is Auto Config, select **Auto Config**.

The screenshot shows the 'Advanced' settings page for the Verizon 4G LTE Router. The navigation menu includes: Main, Traffic Meter, Basic Setup, Wi-Fi Settings, Content Filtering, Maintenance, **Advanced**, Support, and LogOut. The sub-menu includes: Broadband Settings, Access Control, Wi-Fi Settings, Wi-Fi Repeating Function, Port Forwarding/Triggering, Miscellaneous, LAN Setup, and QoS Setup. The 'IPv6' sub-menu is active. The 'Basic Settings' section contains:
 

- Internet Connection Type:** A dropdown menu set to 'Auto Config'.
- DHCP User Class (if Required):** An empty text input field.
- DHCP Domain Name (if Required):** An empty text input field.
- Router's IPv6 Address On WAN:** Not Available.

 The 'LAN Setup' section contains:
 

- Router's IPv6 Address On LAN:** Not Available.
- IP Address Assignment:** Radio buttons for 'Use DHCP Server' (unselected) and 'Auto Config' (selected).
- Use This Interface ID:** An unchecked checkbox followed by four empty input fields for IP address components.

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

Enter the requested information:

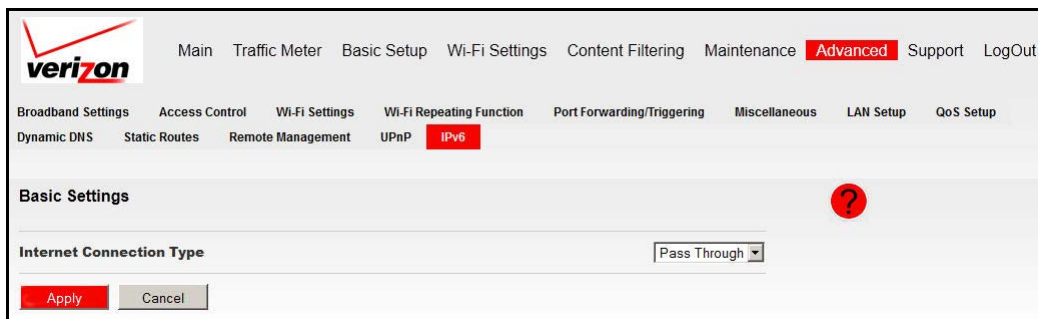
- **DHCP User Class.** Most users should not need to fill in this field, but if your ISP has given you a specific host name, enter it here.
- **DHCP Domain Name.** This value is not needed for most users. Type the domain name of your ISP. For example, if your ISP mail server is mail.xxx.yyy.zzz, you would type xxx.yyy.zzz as the domain name.



If you have a domain name given to you by your ISP, type it in this field. (For example, Earthlink Cable might require a host name of home, and Comcast sometimes supplies a domain name.)

This value is the domain name for the IPv6 connection, and the domain name for the IPv4 connection is not specified here.

- **Router’s IPv6 Address on WAN.** This value shows the IPv6 address acquired for the router’s WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline ( ) under the IPv6 address.
- **Router’s IPv6 Address on LAN.** This value shows the IPv6 address acquired for the router’s LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline ( ) under the IPv6 address.
- **IP Address Assignment.** You can select how you want to assign IPv6 address to the devices on the LAN (that is, your home network). You can use either the DHCP Server or Auto Config to assign IPv6 address. Using DHCP server might pass more information to LAN devices, but some IPv6 systems do not support the DHCPv6 client function. Auto Config is used by default.
- **Use This Interface ID.** You can enable this option and specify the interface ID you want for the IPv6 address for the router’s LAN interface. If you do not specify an ID here, the router generates one automatically from its MAC address.
- **Pass Through.** If your ISP explicitly indicates that your IPv6 connection is not DHCP, PPPoE, or Fixed IP, or your ISP indicates that it is IPv6 auto config, select **Pass Through**.



4. Click **Apply** to save the new settings to the router.
5. Click **Status Refresh** to update the screen and see the information about the current IPv6 connection.

# Troubleshooting


---

# 6

This chapter gives information about troubleshooting your Verizon 4G LTE 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 97.
- Have I connected the router correctly?  
Go to [Basic Functioning](#) on page 97.
- I cannot access the router's configuration with my browser.  
Go to [Troubleshoot Access to the Router Main Menu](#) on page 99.
- I have configured the router but I cannot access the Internet.  
Go to [Troubleshoot Your Connection](#) on page 100.
- I cannot connect to a specific IP address.  
Go to [Troubleshoot a TCP/IP Network Using the Ping Utility](#) on page 102.
- The router shows the wrong the date and time.  
Go to [Problems with Date and Time](#) on page 103.
- I want to clear the configuration and start over again.  
Go to [Restore the Default Configuration and Password](#) on page 103.

---

**Note:** To access online help, click the online help button (  ).

---





## 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 lit.
2. After approximately 10 seconds, verify the following:
  - a. The Power LED is still solid green. An amber LED indicates that the unit has failed its power-on self-test (POST).
  - b. The Internet Port LED is lit.
  - c. The Wi-Fi LED is lit. The Wi-Fi radio is on by default.
  - d. The Ethernet LAN Port LED is lit when any local ports are connected.
 

If a LAN port's LED is lit, a link has been established to the connected device. If a LAN port is connected to a 100 Mbps device, verify that the port's LED is green. If the port is 10 Mbps, the LED is amber.
  - e. The Ethernet WAN Port LED is lit when the router is connected to a wired modem.
  - f. The Signal Quality LED is lit when the router has detected a mobile broadband signal.
    - A blue LED indicates excellent coverage.
    - A green LED indicates good coverage.
    - An amber LED indicates marginal coverage.

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

LED		Action
Power 	Power LED is off.	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Check that you are using the power adapter supplied for this product.</li> <li>• If the error persists, you might have a hardware problem and should contact technical support.</li> </ul>
	Power LED is amber.	POST (power-on self-test) in progress. Wait for this test to complete.
Internet Port 	Internet Port LED is off.	Be sure the SIM card that you received is in the router. SIM cards from other devices do not function in the router, and this SIM card does not function in other devices.
	Internet Port LED is amber.	The router cannot connect to the Internet. Check the Internet connection option being used. <ul style="list-style-type: none"> <li>• For the mobile broadband connection option, check the Signal Quality LED.</li> <li>• For the Ethernet connection option, check the WAN Port LED.</li> </ul>
	Internet Port LED is blinking amber and green.	The traffic meter feature is enabled, and the limit set has been reached.

## Verizon 4G LTE Router MBR1515LVW

LED		Action
Wi-Fi 	Wi-Fi LED is off.	The Wi-Fi radio has been turned off. If you want a Wi-Fi connection with the router, press the <b>Wi-Fi</b> button to turn the Wi-Fi radio back on.
	Wi-Fi LED is not blinking.	If this LED does not blink when you are attempting to send data over the Wi-Fi link, log in to the router menu using the Ethernet LAN connection and check your router's wireless (Wi-Fi) configuration.
LAN Ports 	LAN Ports LED is off.	If this LED does not light when an Ethernet connection is made, check the following: <ul style="list-style-type: none"> <li>• Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.</li> <li>• Make sure that power is turned on to the connected hub or workstation.</li> </ul>
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: <ul style="list-style-type: none"> <li>• Make sure that the Ethernet cable connections are secure at the router and at the modem.</li> <li>• Make sure that power is turned on to the modem.</li> </ul>
4G LTE 	4G LTE LED is off.	The router cannot detect a 4G LTE signal.
Signal Quality 	Signal Quality LED is off or amber.	If this LED does not light when the Mobile Broadband connection option is used, check the following: <ul style="list-style-type: none"> <li>• Check with your ISP to ensure that good coverage exists in the area.</li> <li>• Ensure that your mobile broadband account is active.</li> <li>• Ensure that the SIM card is inserted correctly into the router.</li> <li>• Locate the router near a window or other area of the building. Make sure that the Signal Quality LED is lit, indicating that mobile broadband coverage exists with the router.</li> <li>• 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 that it is entered correctly.</li> </ul>

## 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 Mac OS generate and assign an IP address when 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 procedure sets the router's IP address to 192.168.0.1. This procedure is explained in [Restore the Default Configuration and Password](#) on page 103.
- 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.

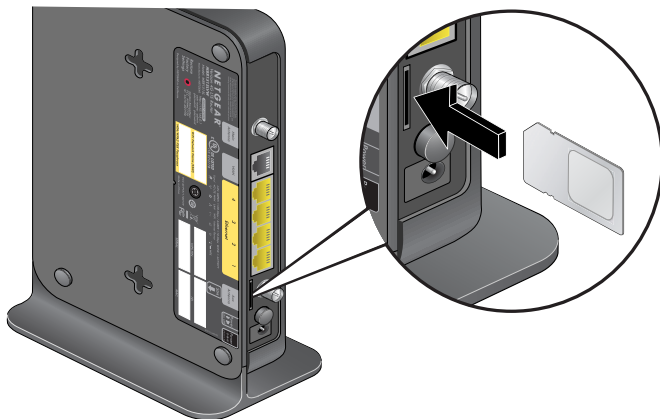
## Troubleshoot Your Connection

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

### Connecting to the Internet

If unable to connect to Internet, check the following:

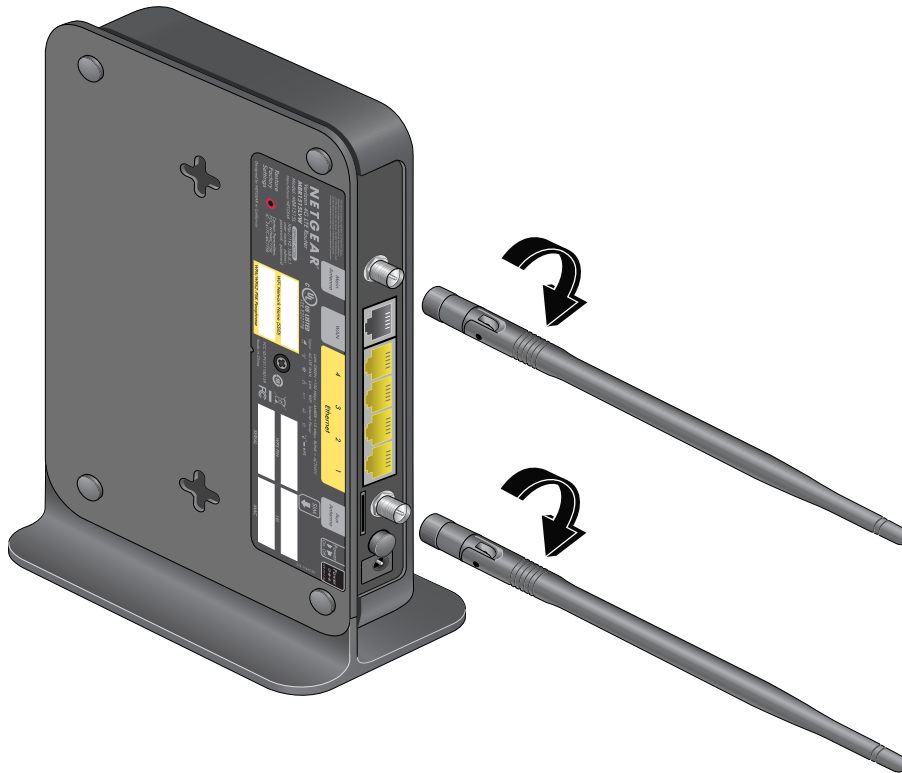
1. The Internet account is active.



If you have not inserted the included 4G LTE SIM card 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 blue Signal Quality LED indicates excellent coverage.
    - A green Signal Quality LED indicates good coverage.
    - An amber Signal Quality LED indicates marginal coverage.
    - An unlighted Signal Quality LED indicates no coverage.
  - b. Maintain recommended minimum distances between the router and household appliances to reduce interference (see [Interference Reduction Table](#) on page 112).

5. Install the external antennas for improved 4G LTE signal strength:



External antennas are shipped with the router and have to be installed. If you have not installed them yet, do so now. See [Assemble the Router](#) on page 7.

## 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 computer running Windows 95 or later:**
1. From the Windows toolbar, click the **Start** button, and select **Run**.
  2. In the field provided, type **ping** followed by the IP address of the router, as in this example:  
**ping 192.168.0.1**
  3. Click **OK**.

You should see a message like this one:

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

If the path is working, you see this message:

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

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

```
Request timed out
```

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

- Wrong physical connections
  - Make sure that the LAN Port LED is lit. If the LED is off, follow the instructions in [Connecting to the Internet](#) on page 100.
  - Check that the corresponding link LEDs are lit 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.

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 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 Broadband 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 so, you must configure your router to clone or spoof the MAC address from the authorized computer. See the *Verizon 4G LTE Router MBR1515L Installation Guide*.

## Problems with Date and Time

The E-mail screen displays the current date and time of day. The 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 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 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 **192.168.0.1**. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase feature (see [Erase the Configuration](#) on page 54).
- 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 109.



# List of Acronyms

---



ACS	Auto Configuration Server
AES	Advanced Encryption Standard
ALG	Application Layer Gateway
AP	Access Point
APN	Access Point Name
CDMA	Code Division Multiple Access
CHAP	Challenge Handshake Authentication Protocol
CIFS	Common Internet File System
CLI	Command Line Interface
CLI	Calling Line Identification
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CQI	Channel Quality Indicator
CWI	Call Waiting Indication
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System (or Service)
DTMF	Dual Tone Multi Frequency (signaling)
EDGE	Enhanced Data rates for Global Evolution
EON	End Of Number
FSK	Frequency-Shift Keying
FTP	File Transfer Protocol
FWT	Fixed Wireless Terminal

FXS	Foreign eXchange Station
G3	Group 3 (Fax protocol)
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
HSPA+	High Speed Packet Access Evolution
ICMP	Internet Control Message Protocol
IDT	Inter Digit Time
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LED	Light Emitting Diode
MVBR	Mobile Voice Broadband Router
MCC	Mobile Country Code
MNC	Mobile Network Code
NAT	Network Address Translation
PAP	Password Authentication Protocol
PIN	Personal Identification Number
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PRL	Preferred Roaming List
PSK	Pre-Shared Key

PSTN	Public Switched Telephony Network
PUK	Personal Unblocking Key
QoS	Quality of Service
RIP	Routing Information Protocol
RSCP	Received Signal Code Power
RSSI	Received Signal Strength Indicator
RTSP	Real Time Streaming Protocol
SFQ	Stochastic Fair Queuing
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMB	Server Message Block
SMS	Short Message Service
SNTP	Simple Network Timing Protocol
SSH	Secure Shell
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
UMTS	Universal Mobile Telecommunications Service
USB	Universal Serial Bus
VAD	Voice Activity Detection
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WCDMA	Wideband CDMA
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity

WLAN	Wireless LAN
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup
WEB GUI	Web User Interface

# Factory Default Settings

---



Use the Restore Factory Settings button on the side of your router to reset all settings to their original factory default settings. This procedure is called a hard reset. To perform a hard reset, press and hold the **Restore Factory Settings** button for 6 seconds. Your router returns 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	192.168.0.1
	Subnet mask	255.255.255.0
	RIP direction	None
	RIP version	Disabled
	RIP authentication	None
	DHCP server	Enabled
	DHCP starting IP address	192.168.0.2
	DHCP ending IP address	192.168.0.254
	DMZ	Disabled
	Time zone	PST for North America
	Daylight saving time adjustment	Disabled

## Verizon 4G LTE Router MBR1515LVW

Feature (continued)		Default Behavior (continued)
Firewall	Inbound communication from the Internet	Disabled (except traffic on port 80, the HTTP port)
	Outbound communication to the Internet	Enabled (all)
	Source MAC filtering	Disabled
Mobile Broadband	Internet service provider	Verizon
Wi-Fi	Wireless communication	Enabled
	SSID name	See label on the side of the 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 varies. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.)
	Country/region	United States
	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

# Compliance Notification

---



## 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 Verizon 4G LTE Router MBR1515LVW 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.

**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

## Numerics

4G LTE LED [13](#)

## A

access [55](#)

- restricting by MAC address [31](#), [63](#)
- router password [55](#)

access control [62](#)

accessing remote computer [66](#)

administrator login [56](#)

attached devices [52](#)

## B

back panel [14](#)

blocking

- inbound traffic [66](#)
- keywords and sites [42](#)
- services [43](#)

## C

compliance, adapters [111](#)

configuration backup [53](#)

connection status [51](#)

control buttons [12](#)

## D

date and time [103](#)

daylight savings time [45](#), [103](#)

Denial of Service (DoS) [41](#)

DHCP [17](#), [76](#)

diagnostics [57](#)

DMZ server [73](#)

DNS servers [66](#)

Dynamic DNS, configuring [82](#)

## E

email notification [46](#), [58](#)

Ethernet broadband settings [22](#)

## F

factory defaults [15](#), [54](#)

front panel [12](#)

## I

inbound traffic, allowing or blocking [66](#)

interference [31](#)

Internet Port LED [13](#)

Internet Relay Chat (IRC) [67](#)

Internet traffic statistics [28](#)

IP addresses

- attached devices [53](#)

- autogenerated [99](#)

- DMZ server [73](#)

- IPv6 address assignments [90](#)

- LAN setup [74](#)

- port forwarding [70](#)

- remote management [86](#)

- reserved [76](#)

- troubleshooting [102](#)

- trusted user, setting [43](#)

- UPnP devices [88](#)

IPv6 connections, configuring [89](#)

## K

keywords, blocking [42](#)

## L

label [15](#)

LAN setup [74](#)

LED descriptions [13](#)

logging in and out [17](#)

login not required [25](#)

login required [23](#)

logs, sending [46](#)

## M

MAC address [103](#)

- location of [64](#)

- restricting access [31](#)

manual configuration **18**  
metric (static route) **85**  
mobile broadband settings **20**

## N

NAT (Network Address Translation) **66**  
network management **48**  
Network Time Protocol (NTP) **44, 103**

## P

password  
    changing **55**  
    restoring **103**  
placement **31**  
port forwarding **66, 68, 69**  
port triggering **66, 67, 69**  
ports, LAN and WAN **13**  
Power LED **13**  
preset security, about **30**  
Push 'N' Connect **36**

## Q

Quality of Service (QoS) **78**

## R

range **31**  
remote management **86**  
reserved IP addresses **76**  
restoring factory defaults **15, 54**  
restricted access **63**

## S

security **30**  
showing statistics **51**  
signal quality **14**  
SMTP **46**  
static routes **84**  
status LEDs **12, 97**

## T

TCP/IP network, troubleshooting **102**  
technical support **2**  
time of day **103**  
time out, login **56**  
time zone **45**

time-stamping **45**  
trademarks **2**  
traffic counter **28**  
traffic meter **27**  
traffic status **28**  
troubleshooting **96**  
trusted host **43**

## U

Universal Plug and Play (UPnP) **88**

## W

WAN Port LED **13**  
WAN setup **72**  
websites, blocking **42**  
WEP **32, 35**  
Wi-Fi, LED and button **13**  
WINS **76**  
wireless access control **62**  
wireless configuration **29**  
wireless repeat function **65**  
wireless security **31**  
wireless settings **32**  
WPA **32, 34**  
WPA + WPA2 **34**  
WPA2 **32, 34**  
WPS **13, 36**  
    PIN entry **38**  
    unsupported **39**