



User Guide

**Verizon 4G LTE
Broadband Router**

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 guide, visit the Verizon support website at:

<http://support.verizonwireless.com/clc/>

Statement of Conditions

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

Contents

Chapter 1 Setting Up Your Router

Hardware Features	6
Router Front Panel	6
Router Back Panel	8
Router Label	9
Assemble the Router	9
Insert the SIM Card	10
Attach the Antennas	10
Place the Router	12
Connect Wi-Fi Devices to Your Router	13
Sign In to Your Router	13
Configure Your Internet Settings	15
4G LTE Broadband Settings	16
WAN Ethernet Broadband Settings	18

Chapter 2 Plan Your Network and Configure Wireless Settings

Plan Your Wireless Network	24
Router Placement	24
Range Guidelines	25
Enhance Your Wi-Fi Security	25
Configure WPA, WPA2, or WPA + WPA2	27
Configure WEP	28
Join Your Wireless Network	30
Manual Method	30
Wi-Fi Protected Setup Method	30
WPS Wizard for Adding Wi-Fi Connections	31
Add Wireless Devices That Do Not Support WPS	32
Advanced Wi-Fi Settings	33
Restrict Connectivity by MAC Address	35

Chapter 3 Set Parental Controls

Block Sites	38
Block Services	39
Schedule Content Filtering	41
Control Connected Devices Access	42

Chapter 4 Manage Your Network

Set Password	45
------------------------	----

Change the Default Password	45
Change the Administrator Sign In Time-Out.	46
Back Up or Restore Router Settings	46
Back Up the Configuration to a File	46
Restore the Configuration from a File.	47
Reset Default Settings	48
Traffic Meter	49
Router Status	50
View Connected Devices	55
View Access Logs	56
Perform Diagnostics	56

Chapter 5 Advanced Router Settings

Wi-Fi Repeating Function	59
Port Forwarding/Port Triggering	60
Remote Computer Access Basics	60
Port Triggering to Open Incoming Ports	61
Port Forwarding to Permit External Host Communications	63
How Port Forwarding Differs from Port Triggering	64
Set Up Port Forwarding	64
Set Up Port Triggering	65
Miscellaneous WAN Settings	67
Set Up a Default DMZ Server.	69
LAN Setup	70
DHCP Settings	72
Reserved IP Addresses	72
Quality of Service Setup.	73
QoS Priority Rule List	74
Set Up QoS for Internet Access	75
Dynamic DNS	81
Static Routes	82
Remote Management	85
Universal Plug and Play	86

Chapter 6 Troubleshooting

Basic Functioning	89
Troubleshoot Access to the Router Main Menu	91
Troubleshoot Your Connection.	92
Connecting to the Internet	92
Troubleshoot Internet Browsing	93
Troubleshoot a TCP/IP Network Using the Ping Utility.	94
Test the LAN Path to Your Router	94
Test the Path from Your Computer to a Remote Device	95
Problems with Date and Time	95
Restore the Default Configuration and Password	95

Appendix A Factory Defaults

Appendix B Notification of Compliance

Index


Setting Up Your Router

1

This chapter describes how to set up your Verizon 4G LTE Broadband Router and establish an Internet connection.

- *Hardware Features*
- *Assemble the Router*
- *Place the Router*
- *Connect Wi-Fi Devices to Your Router*
- *Sign In to Your Router*
- *Configure Your Internet Settings*

Note: For more information about the topics that are covered in this guide, visit the support website at support.verizonwireless.com/clc

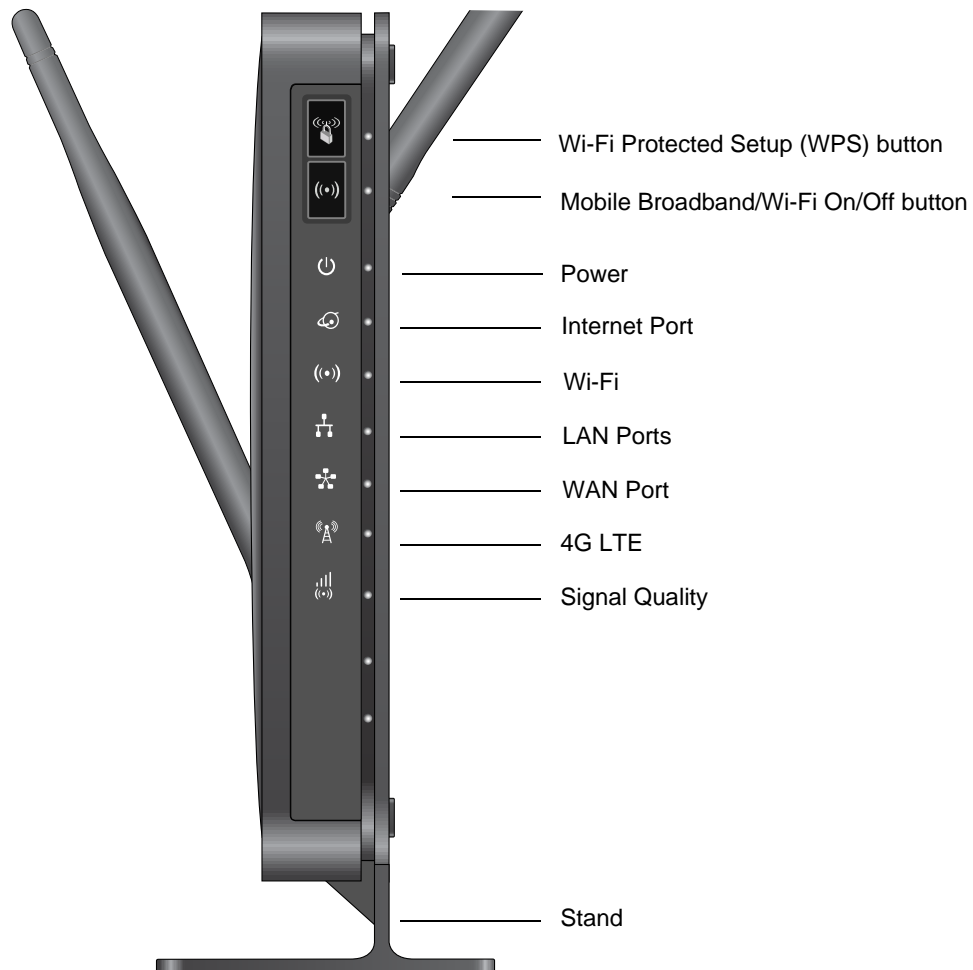
Note: For online help, click  .

Hardware Features

This section outlines the physical aspects of your router.

Router Front Panel

The router front panel contains control buttons and status LEDs. To verify status and connections, use the LEDs.



The following table describes each LED and button on the front panel of the router.

Table 1. LED descriptions


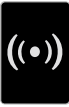







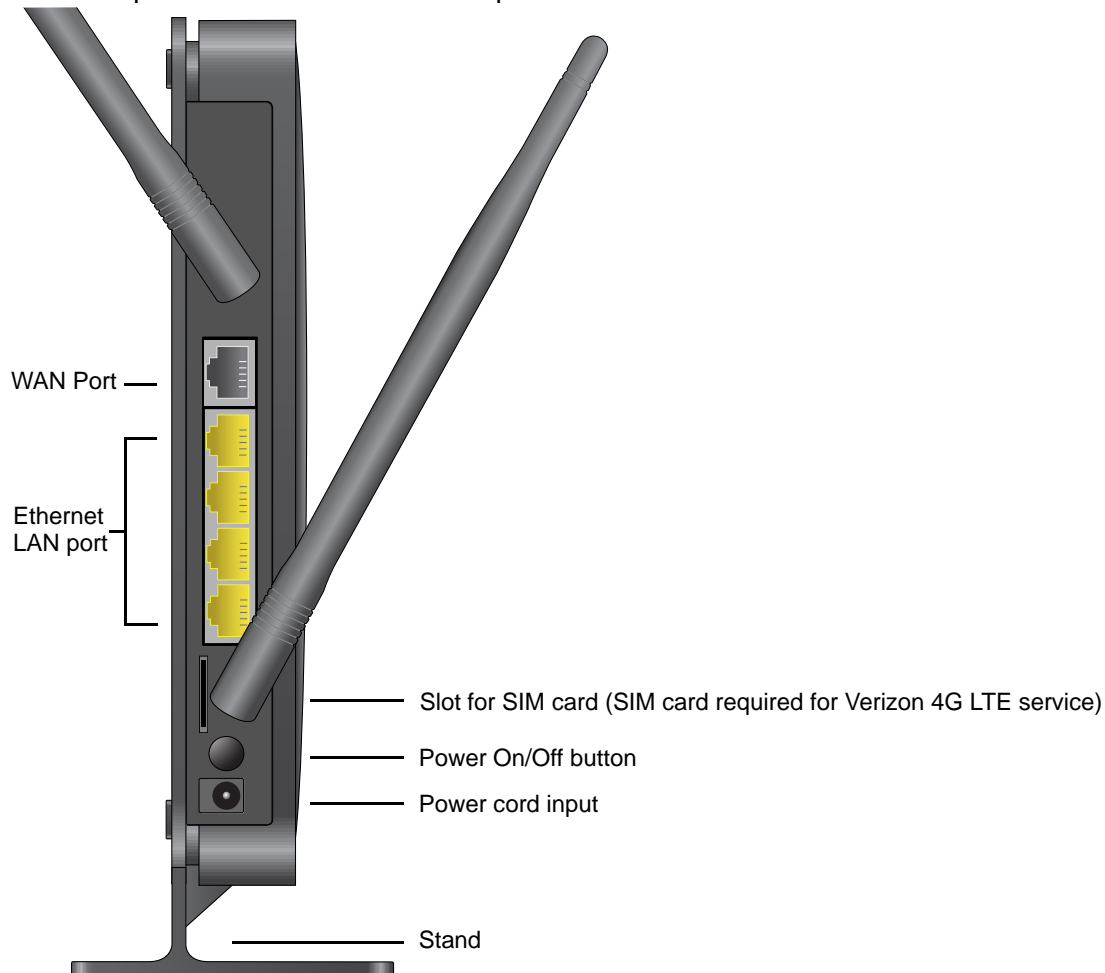
LED	Activity	Description
WPS 	Wi-Fi Protected Setup (WPS) lets you connect to a secure Wi-Fi network without typing its password. Press the Wi-Fi Protected Setup (WPS) button on the router and, within two minutes, connect other Wi-Fi devices with WPS capability. For more information about this function, see <i>Join Your Wireless Network</i> on page 30.	
Wi-Fi 	Press this button to turn off the Wi-Fi connection. Wi-Fi and 4G LTE are turned on by default settings..	
Power 	Solid green	The router is turned on and operating normally.
	Solid amber	POST (power-on self-test) is in progress.
	Off	Router power is off.
Internet Port 	Solid green	An Internet connection is established.
	Solid amber	Traffic meter limit has been reached, and traffic is blocked. Users can set this feature.
	Blinking green	Data is being transmitted over the Internet connection.
	Blinking amber	Traffic meter limit has been reached, but traffic is not blocked. Users can set this feature.
	Blinking green and amber	Failover from wide area network (WAN) to mobile broadband occurred.
	Off	No Internet connection is detected.
Wi-Fi 	Blinking blue	Data is being transferred over the Wi-Fi link.
	Off	The wireless Internet is turned off.
LAN Ports 	Solid green	The local area network (LAN) Ethernet ports have detected wired links with computers or other Ethernet devices.
	Blinking	Data is being transmitted.
	Off	No link is detected on these ports.
WAN Port 	Solid green	The wide area network (WAN) Ethernet port has detected an active link.
	Blinking	Data is being transmitted or received.
	Off	No link is detected on this port.

Table 1. LED descriptions (continued)

LED	Activity	Description
	Solid blue	4G LTE coverage is established for the router.
	Off	No 4G LTE coverage is detected.
	Solid blue	A strong signal is detected.
	Solid green	A good signal is detected.
	Solid amber	A weak signal is detected.
	Off	No signal or service failure is detected.

Router Back Panel

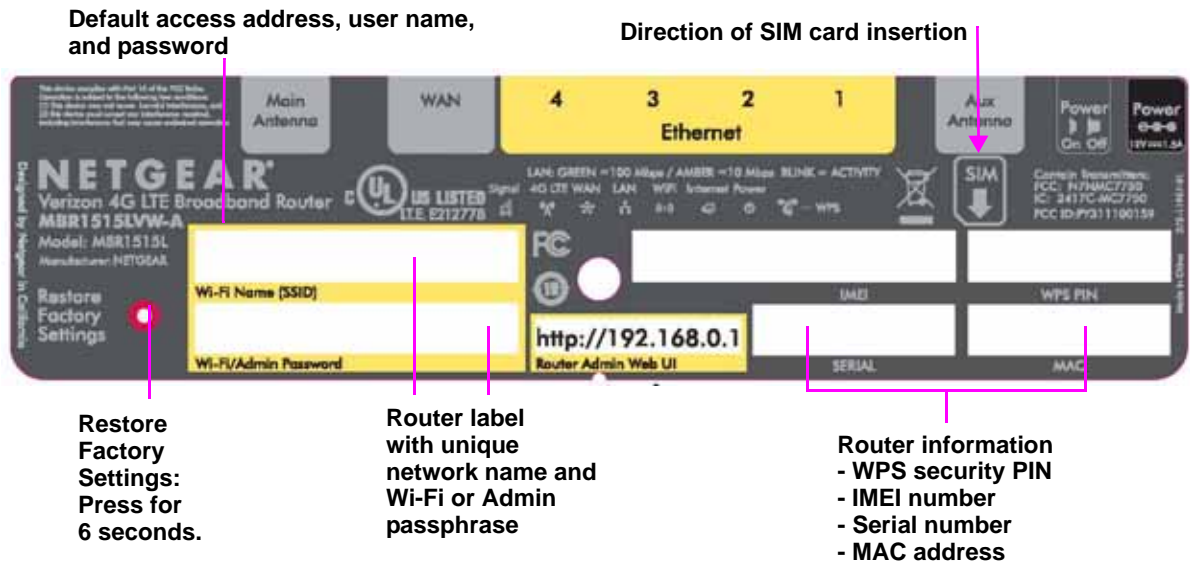
The back panel of the router contains port connections.



Router Label

Your router's label indicates:

- MAC address
- Serial number
- WPS security PIN
- IMEI number
- Factory default sign in information.
- Wi-Fi Name and password unique to each router



Wi-Fi Name and Password

Computers, smartphones and tablets that connect to the router wirelessly and do not support Wi-Fi Protected Setup (WPS) use a unique network name and password information to connect. For more information, see *Add Wireless Devices That Do Not Support WPS* on page 32.

Restore Factory Settings



Insert a paperclip into the hole and press for six seconds. Pressing the Restore Factory Settings button causes the Power LED to blink amber and turn green as the router resets to the factory default settings. See *Factory Defaults* on page 96.

Assemble the Router

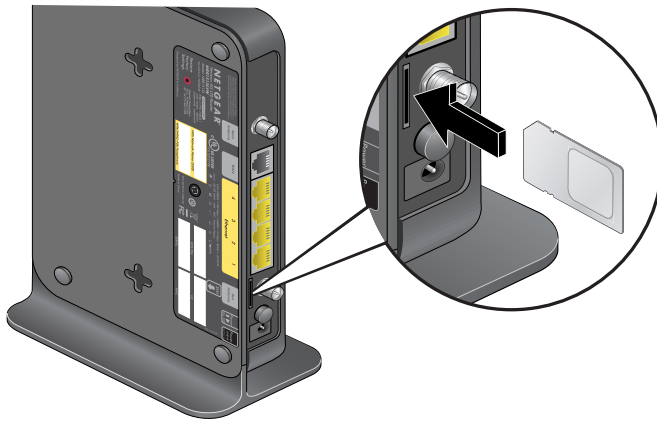
To assemble the router, insert the SIM card and attach the antennas.

Insert the SIM Card

1. Install the 4G LTE SIM card.

Note: The SIM 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 card into the slot with the gold contacts facing the back of the router and the cut-off corner facing inward.

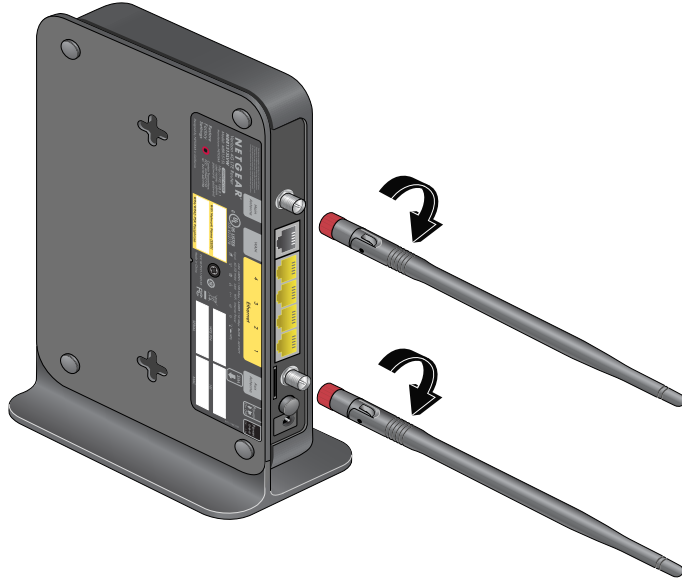


To remove, gently press the SIM card inward to release, and remove it from the slot.

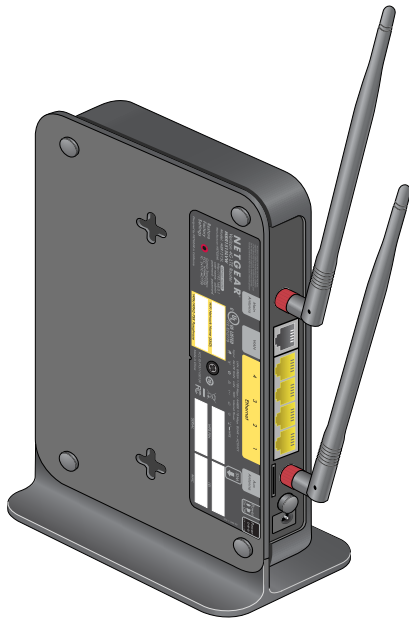
Attach the Antennas

Your router comes with two detachable antennas. These two external antennas are required for proper 4G LTE service.

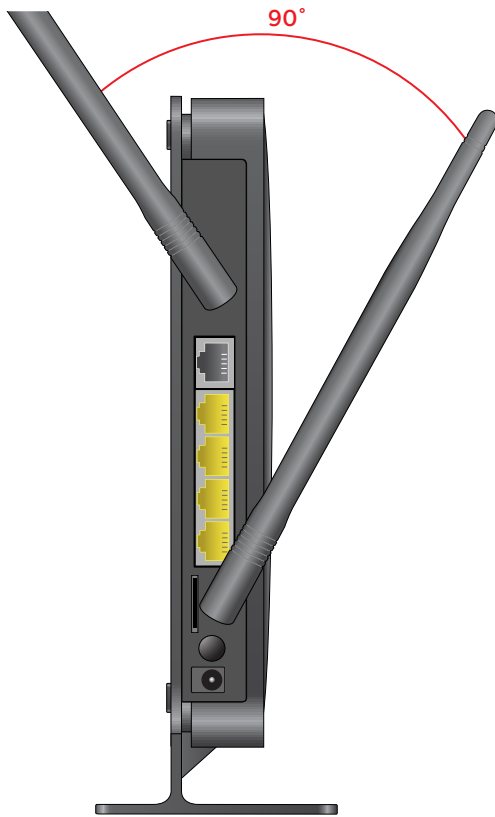
1. Align the antennas with the antenna posts on your router .



2. Mount and secure the antennas on the threaded antenna posts by twisting the red, textured connectors.
3. Swivel the antennas in any direction for best fit.



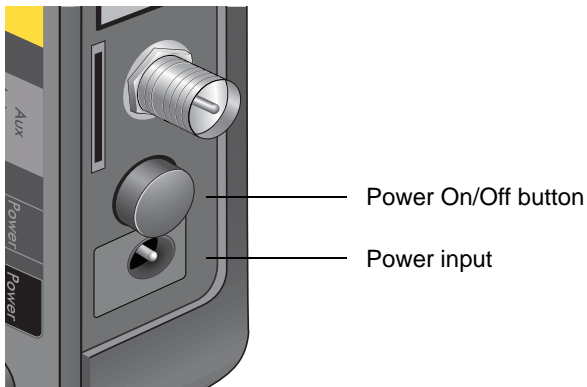
4. For best 4G LTE reception, position external antennas at right angles to each other.



Place the Router

1. Place your router in a central area. Here are some additional tips:
 - Position your router upright and near a power outlet in an easily accessible area.
 - Locate your router indoors where you receive a strong mobile broadband signal (preferably near a window) for best 4G LTE coverage.
 - Avoid physical obstructions whenever possible.
 - Avoid placing your router close to reflective or metal surfaces, such as:
 - Mirrors
 - Metal file cabinets
 - Stainless steel countertops
 - Place your router away from electrical equipment or appliances (microwave ovens) that can also generate Wi-Fi signal interference.
2. Connect the power cord to the power input on the rear of the router and plug it into an outlet.

3. Press the **Power On/Off** button.



Connect Wi-Fi Devices to Your Router

After you have assembled your router and powered it on, connect your smartphones, tablets, computers, or gaming consoles to the router.

➤ **To connect Wi-Fi devices to your router:**

1. Go to your computer, smartphone or tablet's settings or software managing wireless connections.
2. Scan for new or available Wi-Fi networks.
3. Locate your router's Wi-Fi network.

The Wi-Fi name and password are printed on your router. The Wi-Fi device scans for all wireless networks in your area.

4. Select your Wi-Fi network and connect.

The name appears as "Verizon – MBR1515 – XXXX" (where X = last four digits of the MAC address).

Note: For a WPS (Wi-Fi Protected Setup) connection, sometimes referred to as Push 'N' Connect, press the **WPS** button on the router. Follow your computer, smartphone or tablet's instructions to finish the WPS process.

Sign In to Your Router

After setting up your router, use your web browser to sign in to the router to view or change its settings.

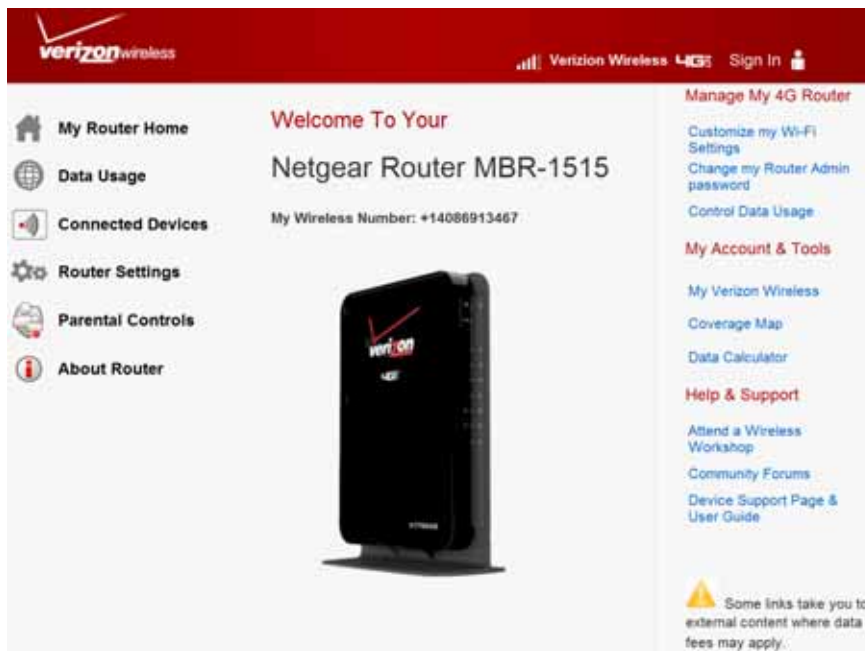
Note: Your computer must be configured for Dynamic Host Configuration Protocol (DHCP). For help configuring DHCP, see your computer's manual.

If you remain inactive for five minutes during online setup, you will be automatically signed out.

Note: You can reset the automatic sign out duration on the **Set Password** screen (see *Change the Administrator Sign In Time-Out* on page 46).

- **To sign in to the router:**
1. Goto <http://192.168.0.1>.

The following screen appears.



2. In the upper right corner, click **Sign In**.

The following screen appears.

The image shows the login interface for a Verizon 4G LTE Broadband Router. At the top is a red banner with the Verizon Wireless logo. Below the banner, the title "Verizon 4G LTE Broadband Router" is displayed. The main instruction is "Sign In to continue. Please enter your Admin Password." There is a text input field for the "Admin Password" and a red "Sign In" button. Below the password field, it says "Administrator login times out after idle for 5 minutes" with a dropdown menu currently set to "5". At the bottom, there is a link that says "I Forgot the Admin Password".

3. Enter the Wi-Fi **Admin Password** printed on your router's label.
4. In the **Administrator login times out after idle for** field, enter your desired number of minutes after which the router signs out of the webpage.
5. Click **Sign In**.

To learn how to change the password, see *Change the Default Password* on page 45.

Note: If you forget your password, restore your router to its factory default settings, which resets the password. See *Factory Defaults* on page 96.

Configure Your Internet Settings

To connect to the Internet, you need an active broadband service account. The broadband service can be 4G LTE from Verizon or WAN Ethernet (such as DSL or cable broadband) from any internet service provider.

If WAN Ethernet service is required, contact your internet service provider for:

- Your user name
- Password
- Network name

You will also configure some or all of the settings described in the sections listed below:

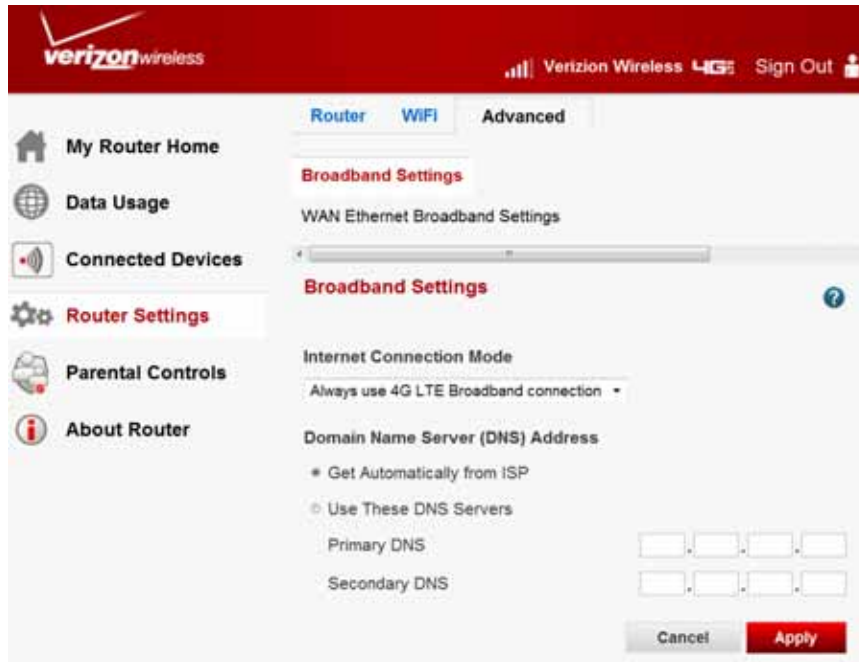
- *The default Internet connection mode is 4G LTE broadband* on page 16 (only if you are changing the Internet connection mode from mobile broadband to WAN Ethernet).
- *4G LTE Broadband Settings* on page 16 (not required if you are using a WAN Ethernet connection).
- *WAN Ethernet Broadband Settings* on page 18 (not required if you are using a 4G LTE connection).

Note: The default Internet connection mode is 4G LTE broadband.

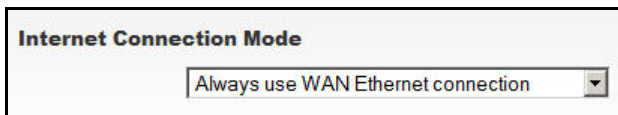
➤ **To switch between 4G LTE broadband and WAN Ethernet mode:**

1. Sign in to the web user interface.
2. From the main menu, select **Router Settings > Advanced > Broadband Settings**.

The following screen appears:



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



4. Specify how DNS servers are assigned.
Select either **Get Automatically from ISP** or **Use These DNS Servers**.
If you select **Use These DNS Servers**, enter server addresses.
5. Click **Apply**.

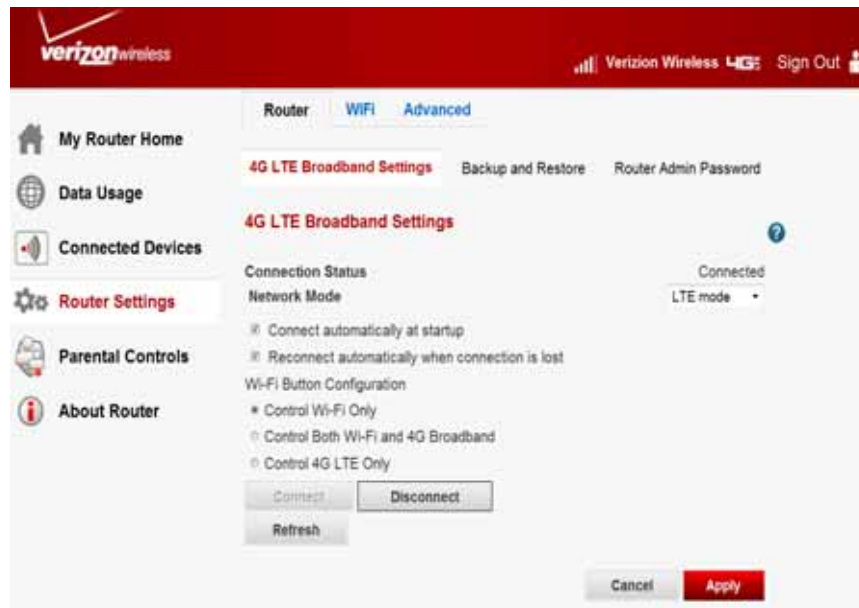
4G LTE Broadband Settings

➤ **To manually configure your 4G LTE broadband Internet settings:**

1. Sign in to the web user interface.

- From the main menu, select **Router Settings > Router > 4G LTE Broadband Settings**.

The following screen appears:



Note: To connect to the 4G LTE network, you need an active Verizon broadband service account.

- Adjust the settings as needed.

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

Settings	Description
Connection Status	Indicates a SIM card is present
Network Mode	Select one of the following: <ul style="list-style-type: none"> Auto. The router evaluates the signal strength and connects using 4G LTE. LTE mode. The router connects only in 4G LTE mode.
Connect automatically at startup	If selected, the router automatically connects to the network. This should be selected after sign in information is provided.

Settings	Description
Reconnect automatically when connection is lost	If selected, the router attempts to reconnect to the network if the connection is lost. This option is normally selected.
Wi-Fi Button Configuration	<p>The Wi-Fi button will:</p> <ul style="list-style-type: none"> • Control Wi-Fi Only. Pressing the Wi-Fi button toggles the Wi-Fi function on and off. If the Wi-Fi function is enabled, The 4G LTE broadband function is unaffected. • Control Both Wi-Fi and 4G LTE Broadband. Pressing the Wi-Fi button toggles both the Wi-Fi function and 4G LTE broadband on and off, at the same time. Depending on the coverage, 4G LTE broadband coverage might or might not be connected successfully. • Control 4G LTE Only. Pressing the Wi-Fi button toggles the 4G LTE function on and off, if the function is enabled. Wi-Fi function is unaffected.

4. Select one of the following:
 - **Connect:** Manually connect to the network.
 - **Disconnect:** Disconnect from the current network.
 - **Refresh:** Update the connection status.
 - **Cancel:** Discard changes.
 - **Apply:** Apply the changes that you made.

WAN Ethernet Broadband Settings

- To manually configure your WAN Ethernet Broadband Internet settings:
1. Sign in to the web user interface.
 2. From the main menu, select **Router Settings > Advanced> WAN Ethernet Broadband Settings**.



3. Select the Internet connection based on your Internet service provider account.

- If you need to enter log in information every time you connect to the Internet, or you have a Point-to-Point protocol over Ethernet (PPPoE) account with your Internet service provider, select **Yes**. See *Yes, a Login Is Required* on page 19.
- Otherwise, select **No**. See *No, a Login Is Not Required* on page 21.

Note: If you have installed Point-to-Point (PPP) software such as WinPoET (from Earthlink) or Enternet (from PacBell), then you have PPPoE. Select **Yes**. After 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.

The screenshot shows the 'WAN Ethernet Broadband Settings' configuration page. At the top, the title 'WAN Ethernet Broadband Settings' is in red, followed by a help icon. The first section asks 'Does your Internet connection require a login?' with radio buttons for 'Yes' (selected) and 'No'. Below this, the 'Internet Service Provider' dropdown is set to 'PPPoE'. The 'Login' field contains 'guest', and the 'Password' field is empty. The 'Service Name (If Required)' field is also empty. The 'Connection Mode' dropdown is set to 'Dial on Demand', and the 'Idle Timeout(In Minutes)' field is set to '5'. The 'Internet IP Address' section has radio buttons for 'Get Dynamically from ISP' (selected) and 'Use Static IP Address'. The static IP address fields are empty. At the bottom, there are 'Test', 'Cancel', and 'Apply' buttons.

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

Settings	Description
Internet service provider	Select your ISP service type: <ul style="list-style-type: none"> • Other (PPPoE) is the most common. • PPTP (Austria and other European countries). • Telstra BigPond (Australia only).
Login	This is usually the name that you use in your email address. For example, if your main mail account is JerAB@ISP.com, enter JerAB in this field. Some ISPs (such as Mindspring, Earthlink, and T-DSL) use your full email address when you sign in.
Password	Enter your ISP login password.
Service Name (If Required)	If your ISP provided a service name, enter it here. Otherwise, leave this field blank.
Connection Mode	Set the connection mode to Dial on Demand , Always On , or Manually Connect . <ul style="list-style-type: none"> • Dial on Demand. A PPPoE connection automatically starts with outbound activity to the Internet. It automatically closes if the connection is idle based on the value in the Idle Timeout field. • Always On. The PPPoE connection automatically starts when the computer boots up, but the connection does not time out. The router will keep trying to connect after it is disconnected. • Manually Connect. If selected, connect to the Internet by going to the Router Settings screen and click Connect. This connection does not time out; you must click the Disconnect button on the Router Settings screen to disconnect.
Idle time-out (In Minutes)	After the time period has passed, your connection will end. If this value is zero (0), the router keeps the connection alive by reconnecting immediately if the connection is lost.
Internet IP Address	<ul style="list-style-type: none"> • Get Dynamically for ISP. If you sign 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. • Use Static IP Address. If you have a fixed (or static IP) address and your ISP has provided you with an IP address, enter in the IP address.

2. Click one of the following buttons:

- **Test:** Connect to the My Verizon website.

If you connect successfully and your settings work, click **Sign out** to exit these screens.

- **Cancel:** Discard changes.
- **Apply:** Apply any changes made.

No, a Login Is Not Required

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

1. Adjust the settings as needed.

WAN Ethernet Broadband Settings

Does your Internet connection require a login?

☐ Yes

☒ No

Account Name (If Required)

Domain Name (If Required)

Internet IP Address

☒ Get Dynamically from ISP

☐ Use Static IP Address

IP Address

IP Subnet Mask

Gateway IP Address

Router MAC Address

☒ Use Default Address

☐ Use Computer MAC Address

☐ Use This MAC Address

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

Settings	Description
Account Name (if necessary)	This name is also known as the host name or system name. Enter your account name or user name in this field. For example, if your main mail account is JerAB@ISP.com, enter JerAB in this field. Enter your ISP-assigned host name, if given (for example, CCA7324-A).
Domain Name (if necessary)	Leave this field blank unless your ISP requires the domain name. If you have a domain name given to you by your ISP, enter 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 router, this domain name is usually the workgroup name. For example, if your ISP mail server is mail.xxx.yyy.zzz, enter xxx.yyy.zzz as the domain name.

Settings	Description
Internet IP Address	<ul style="list-style-type: none"> • Get Dynamically From ISP. If you sign 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. • Use Static IP Address. If you have a fixed (or static IP) address and your ISP has provided you with an IP address, enter the address, subnet mask, and gateway IP address into the correct fields. For example: <ul style="list-style-type: none"> - IP Address. 24.218.156.183 - Subnet mask. 255.255.255.0 - Gateway IP Address. 24.218.156.1
Router MAC Address	<ul style="list-style-type: none"> • Use Default MAC Address. Your computer's local address is its unique address on your network. • Use Computer MAC Address. Select if your ISP requires MAC authentication. This disguises the router's MAC address with the computer's own MAC address. • Use This MAC Address. Select if you want to manually enter the MAC address for a different computer. 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.

2. Click one of the following buttons:

- **Test:** Connect to the My Verizon website.
- **Cancel:** Discard changes.
- **Apply:** Apply any changes.

If you connect successfully and your settings work, click **Sign out** to exit these screens.

Plan Your Network and Configure Wireless Settings

2


For a wireless connection, your router and computer, smartphone or tablet will need to have the same Wi-Fi network name and security settings. Verizon recommends that you use wireless security.

Your router is preset with security features and uses a unique Wi-Fi network name and password. This information is printed on the router label and will be used to set up your Wi-Fi capable computers, smartphones and tablets.

This chapter covers the following topics:

- *Plan Your Wireless Network*
- *Enhance Your Wi-Fi Security*
- *Join Your Wireless Network*
- *Advanced Wi-Fi Settings*
- *Restrict Connectivity by MAC Address*

Note: The wireless range is 300 feet (100 meters), but can be weakened by walls or other obstructions. We recommend using wireless security to prevent unauthorized connections to your network.

Note: For online help, click  .

Plan Your Wireless Network

Your router is preset with a:

- Wi-Fi network name
- Password
- Security option

The default Wi-Fi network name and password appear on the router label (see *Router Label* on page 9).

Note: The default Wi-Fi network name and password are uniquely generated for every router.

Verizon recommends that you do not change your default security settings. If you do decide to change your default security settings, please make a note of your new settings.

Note: If you use a computer connected through Wi-Fi to change the Wi-Fi network name or other wireless security settings, you are disconnected when you click **Apply**. To avoid a disconnection, use a computer with a wired LAN connection to the router.

If you change the default security settings, be aware of the following:

- For compliance and compatibility between similar products in your area, the operating channel and region must be set correctly.
- To configure the wireless network, either choose the wireless settings, or use Wi-Fi Protected Setup (WPS) to automatically set the Wi-Fi network name and turn on security.
- To change the wireless settings, you must know the:
 - **Wi-Fi network name:** The default network name is printed on the router label (see *Router Label* on page 9).
 - **Wireless security option:** Check your computer, smartphone or tablet's documentation for a list of supported options.

Router Placement

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

- Near the center of your computer area.
- In an elevated spot, such as a high shelf, where all wirelessly connected computers and devices have line-of-sight access (even if through walls).

- Away from sources of interference (see *Interference Reduction Table* on page 100).
- Away from large metal surfaces.
- In the vertical position (as an example, see the figure in *Router Back Panel* on page 8).

Range Guidelines

Your wireless router has an indoor range of 300 feet (100 meters). Such distances can allow unauthorized connections to your network.

Verizon recommends using the security features of your wireless router. Without using the router's security features, your wireless data transmissions can be received by anyone within range.

Enhance Your Wi-Fi Security

You can enhance the security of your wireless network in several ways:

- **Restrict connectivity based on MAC address:** Allows only trusted computers to connect; unknown computers cannot wirelessly connect to the router, but the data sent over the wireless link is fully exposed.
- **Turn off the broadcast of the Wi-Fi network name:** Only users who have the correct network name can connect. This approach blocks any wireless network “discovery” features but the data is still exposed.
- **Wired Equivalent Privacy (WEP):** Data encryption provides data security. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. Only WPA-PSK and WPA2-PSK supersede this data encryption mode.
- **WPA-PSK (TKIP), WPA2-PSK (AES):** Wi-Fi Protected Access (WPA) using a pre-shared key to authenticate and create the initial data encryption keys, making it almost impossible to compromise.
- Each router is preconfigured for WPA-PSK/WPA2-PSK mixed mode.

Note: Connect your computer directly to the router with an Ethernet cable before changing the network name or wireless security.

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

1. Sign in to the web user interface.
2. From the main menu, select **Router Settings > Wi-Fi > Wi-Fi Profile**.

The following screen appears:

The screenshot shows the Verizon Wireless router's web interface. At the top, there's a red header with the Verizon logo and 'Verizon Wireless 4G LTE' status. Below the header, there are tabs for 'Router', 'WIFI', and 'Advanced'. The 'WIFI' tab is selected. On the left, there's a sidebar with icons for 'My Router Home', 'Data Usage', 'Connected Devices', 'Router Settings' (highlighted), 'Parental Controls', and 'About Router'. The main content area is titled 'Wi-Fi Settings' and includes a 'Wi-Fi Profile' section with links for 'Add WPS Client' and 'Advanced Wi-Fi Settings'. The settings are as follows:

- WiFi name:** Verizon-MBR1515-F766
- WiFi password:** 60400790 (8-63 characters or 64 hex digits)
- Channel:** Auto
- Mode:** 802.11 b/g/n
- Security Options:**
 - ☐ None
 - ☐ WEP
 - ☐ WPA-PSK [TKIP]
 - ☒ WPA2-PSK [AES]
 - ☐ WPA-PSK [TKIP] + WPA2-PSK [AES]

At the bottom right, there are 'Cancel' and 'Apply' buttons.

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

Settings		Description
Wireless network	Wi-Fi network name (SSID)	The wireless network name can contain up to 32 case-sensitive characters. When more than one wireless network exists, network names provide a means for separating the traffic. To join a network, the user will need to know the network name.
	Wi-Fi password	The 8 – 63 character or 64 hex digit Wi-Fi password (any combination of 0-9, a-f, or A-F) used to connect wirelessly to your router.
	Channel	The wireless channel used by the gateway. The default is Auto. Do not change the channel unless you experience interference (as indicated by lost connections or slow data transfers). If this happens, try a different channel. If you are using multiple access points, set adjacent access points to use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is five channels (for example, use Channels 1 and 6, or 6 and 11).
	Mode	Available settings are 802.11 b/g/n (default) or 802.11 b/g.

Settings		Description
Security Options	None	Use this setting to establish wireless connectivity before setting up wireless security.
	WEP	Use encryption keys and data encryption for data security. You can select 64 bit or 128-bit encryption. See <i>Configure WEP</i> on page 28.
	WPA-PSK (TKIP)	Allow only computers configured with WPA to connect to your router. See <i>Configure WPA, WPA2, or WPA + WPA2</i> on page 27.
	WPA2-PSK (AES)	Allow only computers configured with WPA2 to connect to your router. See <i>Configure WPA, WPA2, or WPA + WPA2</i> on page 27.
	WPA-PSK (TKIP) + WPA2-PSK (AES)	Allow computers configured with either WPA-PSK or WPA2-PSK security to connect to your router. See <i>Configure WPA, WPA2, or WPA + WPA2</i> on page 27.

3. Modify any desired Wi-Fi settings.
4. Click **Apply**.
5. Set up and test your Wi-Fi capable computer, smartphone or tablet to make sure that they can connect wirelessly.

If you cannot connect wirelessly, check the following:

- You might be connected to a different router. Check your settings to see if they are set to automatically connect to the first open network.
- You might not be connecting to the router because it is interfering with other wireless computers, smartphones or tablets. To avoid this, try changing the channel.

For more information about available security options, see *Configure WPA, WPA2, or WPA + WPA2* on page 27. Otherwise, continue to *Join Your Wireless Network* on page 30.

Configure WPA, WPA2, or WPA + WPA2

Both Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (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.

Consult your computer, smartphone or tablet's documentation for instructions when changing WPA settings.

Wi-Fi Protected Setup (WPS), or Push "N" Connect, implements WPA/WPA2 wireless security on the router and your WPS-compatible wireless computer, smartphone or tablet at the same time.

Note: If you are using a wireless connection to configure wireless security settings, you will be disconnected when you click **Apply**. To modify your router settings, you will need to set up your wireless device to match the new security settings and reconnect to the network.

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

1. Sign in to the web user interface.
2. From the main menu, select **Router Settings > Wi-Fi > Wi-Fi Profile**.

3. Under Security Options, choose either WPA-PSK or WPA2-PSK.
4. Enter a Wi-Fi password.
5. Click **Apply**.

Configure WEP

Wired Equivalent Privacy (WEP) encryption is not as strong as WPA and WPA2 encryption. However, you must use WEP encryption to use the Wi-Fi repeating function of the router (see *Wi-Fi Repeating Function* on page 59).

Note: If you are using a wireless connection to configure wireless security settings, you will be disconnected when you click **Apply**. To modify your router settings, you will need to set up your wireless computer, smartphone or tablet to match the new security settings and reconnect to the network.

➤ **To configure WEP data encryption:**

1. Sign in to the web user interface.
2. From the main menu, select **Router Settings > Wi-Fi > Wi-Fi Profile**.
3. In the Security Options section, select **WEP**:

The screenshot shows the 'Security Options' configuration page. Under 'Security Options', 'WEP' is selected with a radio button. Below this, the 'Security Encryption (WEP)' section contains two dropdown menus: 'Authentication Type' set to 'Automatic' and 'Encryption Strength' set to '64-bit'. The 'Security Encryption (WEP) Key' section includes a 'Passphrase' field with a 'Generate' button, and four 'Key' fields (Key 1 through Key 4). 'Key 1' is selected with a radio button. At the bottom, there are 'Apply' and 'Cancel' buttons.

4. Select an Authentication Type.

Authentication is separate from data encryption. Select a type 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 your Encryption Strength:

- **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.

Either 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. Computers, smartphones and tablets must use the passphrase or keys to use your router.

Note: Not all computers, smartphones and tablets support WEP passphrase key generation.

- **Key 1–Key 4:** Manually enter the four data encryption keys. Enter 10 hexadecimal digits (any combination of 0–9, a–f). These values are *not* case-sensitive. The values must be identical on all computers and access points in your network.
7. Select the default key.

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

Join Your Wireless Network

To join the network, use any of the following methods:

- Manual
- Wi-Fi Protected Setup
- Wi-Fi Protected Setup wizard (via the router)

Manual Method

Choose the network that you want and type its password to connect.

➤ **To connect manually:**

1. On your computer, smartphone or tablet, open your wireless connections program.


All Wi-Fi networks in your area will be listed.

2. Select your network.

The unique Wi-Fi network name and password are on the router label. If you changed these settings, look for the network name you assigned.

3. Enter the router password and click **Connect**.

Wi-Fi Protected Setup Method

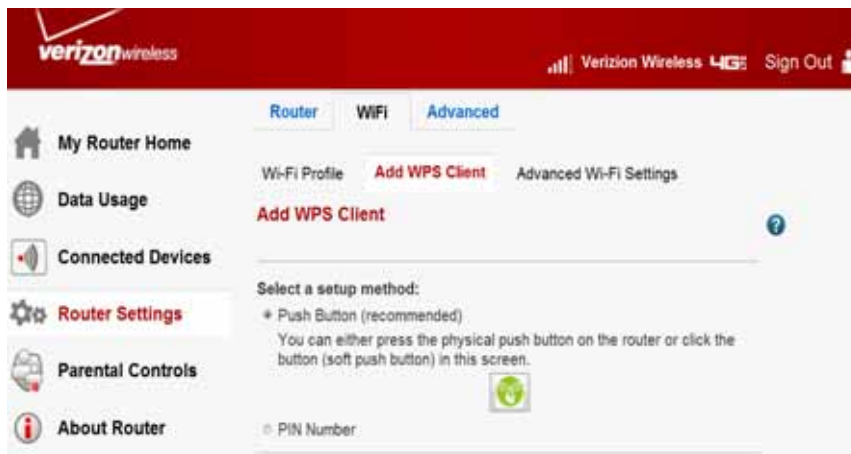
Wi-Fi Protected Setup (WPS) lets you connect to a secure Wi-Fi network by pressing a button or entering a PIN instead of typing its password. WPS works only with WPA2 or WPA wireless security, and is not always compatible with older Wi-Fi routers. Compatible routers usually have the  WPS symbol on it.

WPS Wizard for Adding Wi-Fi Connections

The WPS Wizard helps you add a wireless computer, smartphone or tablet to your Wi-Fi network without typing the Wi-Fi password.

➤ **To use the WPS Wizard to add your computer, smartphone, or tablets:**

1. Sign in to the web user interface.
2. Select **Router Settings > WiFi > Add WPS Client**.
3. Click **Next**.



4. Select which setup method you want to use:
 - **Push button:** Either click the **WPS** symbol on this screen, or press the **WPS** button on the side of the router. Within two minutes, go to the wireless computer, smartphone or tablet and press its **WPS** button to join the network without entering a password.
 - **PIN Number:** The screen adjusts.



Enter the client security PIN, and click **Next**.

Within two minutes, use the computer, smartphone or tablet's WPS software to join the network.

Note: If no WPS-capable client devices are located during the two-minute time frame, the Wi-Fi network name does not change, and no security is set up.

Add Wireless Devices That Do Not Support WPS

If you set up your network with WPS, and now want to add a non-WPS device, you must manually change it.

Because WPA randomly creates the Wi-Fi network name and password, 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. However, you must set up the WPS-compatible computer, smartphone or tablet again.

Note: When you make changes like these, all wireless connections are lost from the network and require setup with the new wireless settings.

➤ To change wireless settings for the network:

1. Connect a computer to the router using an Ethernet cable, preventing a disconnection when changing the wireless settings.
2. Sign in to the web user interface.
3. Select **Router Settings > Wi-Fi > Wi-Fi Profile**.
4. Make the following changes:
 - Change the Wi-Fi network name.
 - Specify a Wi-Fi password.
 - Select **Router Settings > Wi-Fi > Advanced Wi-Fi Settings** and make sure that **Keep Existing Wi-Fi Settings** is selected so that your new settings are not erased if you use WPS. For more information, see *Advanced Wi-Fi Settings* on page 33.
5. Click **Apply**.

All previously connected wireless devices are forgotten and disconnected from the router.
6. To connect any computers, smartphones or tablets, open the networking application and enter the security settings that you selected in Step 4 (the network name, security method, and Wi-Fi password).
7. Connect via WPS.

See *Join Your Wireless Network* on page 30.

The settings that you configured in Step 4 are broadcast to your computer, smartphone or tablet so that they can connect to the router.

Advanced Wi-Fi Settings

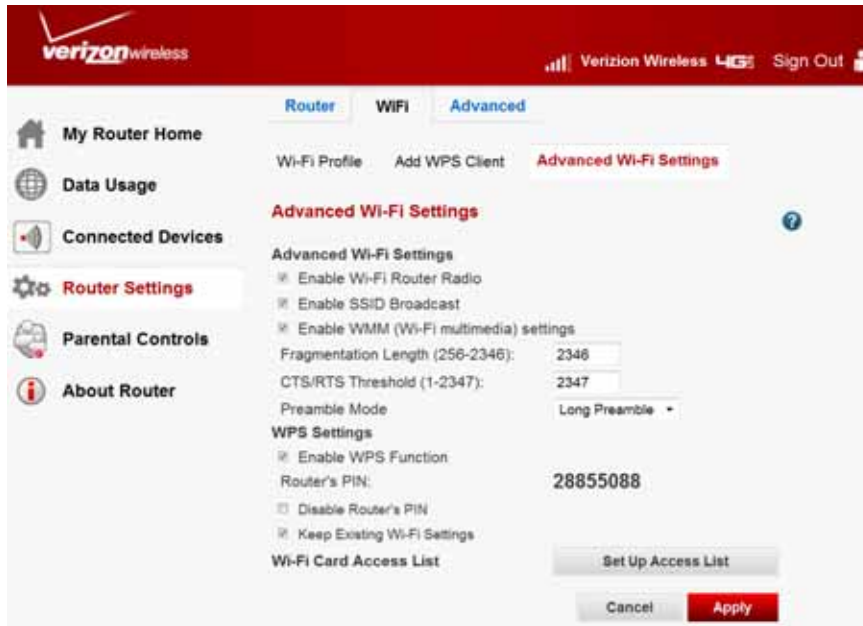
By default, any wireless device configured with the correct Wi-Fi network name and wireless security settings is allowed to connect to your wireless network. Use the options in the **Advanced Wi-Fi Settings** screen to further restrict wireless access to your network.

- **Turn off wireless connectivity completely:**
You can completely turn off the wireless portion of your router. For example, if you are traveling, you can turn off the wireless portion of the router but still allow other household members who use computers to remain connected to the router with Ethernet cables. To make this change, deselect **Enable Wi-Fi Router Radio** in the **Advanced Wi-Fi Settings** screen and click **Apply**.
- **Hide your Wi-Fi network name:**
By default, the router is set to broadcast its Wi-Fi network name. Restrict wireless connections to your network by not broadcasting the network name. To make this change, deselect **Enable SSID Broadcast** on the **Advanced Wi-Fi Settings** screen and click **Apply**. Others will not be able to see your router's wireless network, but can still connect to your router's wireless network if their wireless settings are configured to match the hidden Wi-Fi network name.

Note: The Wi-Fi network name of any wireless computer, smartphone or tablet must match the name you set in the router. If they don't match, you won't be able to establish a wireless connection.

- **To change the advanced Wi-Fi settings:**
1. Sign in to the web user interface.
 2. From the main menu, select **Router Settings > Wi-Fi > Advanced Wi-Fi Settings**.

3. The following screen appears.



Specify the following settings:

- **Advanced Wi-Fi Settings:**
 - **Enable Wi-Fi Router Radio:** Selected by default to turn on the wireless radio, allowing the router to broadcast the Internet wirelessly. 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 Wi-Fi network name.
 - **Enable WMM (Wi-Fi Multimedia) settings:** WMM prioritizes wireless data packets from different applications. For an application to receive the benefits of WMM, both it and your computer, smartphone or tablet have to have WMM turned on.
 - **Fragmentation Length, CTS/RTS Threshold, and Preamble Mode:** Reserved for Wi-Fi testing and advanced configuration.
- **WPS Settings:**
 - **Enable WPS Function:** By default, this is checked.
 - **Router's PIN:** The PIN number used for WPS.
 - **Disable Router's PIN:** By default, this is inactive. When this is selected, this feature allows the WPS computer, smartphone or tablet to discover the router's PIN.
 - **Keep Existing Wi-Fi Settings:** By default, this is inactive. When this feature is selected, it allows the router to automatically generate the Wi-Fi network name and security settings when it implements WPS. Afterwards, the router automatically selects **Keep Existing Wi-Fi Settings** so that your Wi-Fi network name and security settings remain the same if other WPS-capable computers, smartphones or tablets are added later.

- **Wi-Fi Card Access List:** See *Restrict Connectivity by MAC Address* on page 35.

Restrict Connectivity by MAC Address

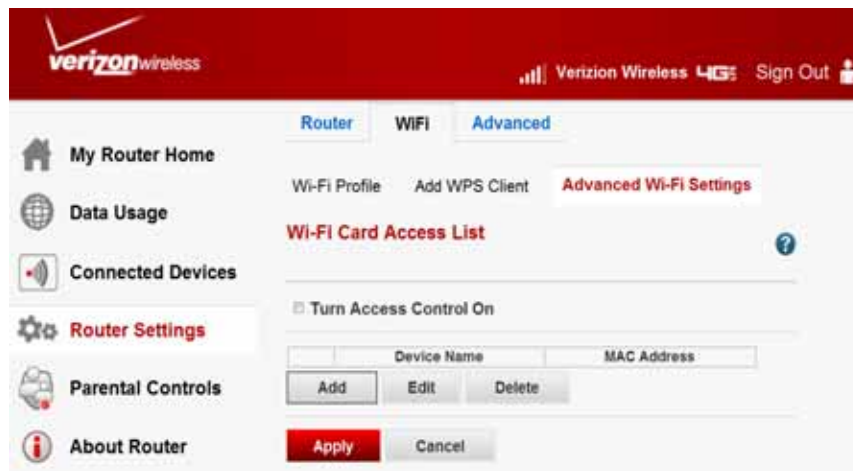
You can increase your network security by allowing only computers you specify based on their MAC address to connect to the router. This prevents unauthorized connections, but does not prevent data sent over the Wi-Fi connection from being viewed.

Note: If you configure the router through a wireless connection, add your computer's MAC address to the Wi-Fi Card Access List. Otherwise, you lose your wireless connection when you click **Apply**. Connect to the router from a wired computer, or from a connection that is on the Wi-Fi Card Access List, to make any further changes.

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

1. Sign in to the web user interface.
2. From the main menu, select **Router Settings > Wi-Fi > Advanced Wi-Fi Settings** and click **Set Up Access List**.

The following screen appears:



3. To enable access control, select **Turn Access Control On**.
Otherwise, access control is turned off by default so that any computer configured with the correct Wi-Fi network name can connect.
4. To add specific Wi-Fi capable computers, smartphones or tablets to the connections list, click **Add**.

The following screen appears:



5. Add computers, smartphones and tablets to the list using any of the following methods:
 - If the computer is in the **Available Wi-Fi Cards** table, select it to capture its MAC address.
 - In the **Wireless Card Entry** field, enter the MAC address. If a name does not appear write a description instead.
6. Click **Add**.

Now, only computers, smartphones and tablets on this list are allowed to connect wirelessly to the router.

Note: You can also restrict access or connectivity using the Access Control screen. See *Control Connected Devices Access* on page 42.

Set Parental Controls

3


Your router provides various options for blocking Internet-based content and communications services. With parental controls features, your router prevents unwanted content from reaching your computers. Parental control options include:

- Keyword blocking of HTTP traffic.
- Outbound service blocking. Limits access from your Local Area Network (LAN) to Internet locations or services that you specify as off-limits.
- Denial of service (DoS) protection. Detects and stops DoS attacks.
- Blocking unwanted traffic from the Internet to your LAN.

Your router lets you 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 your router to protect your network.

- *Block Sites*
- *Block Services*
- *Schedule Content Filtering*
- *Control Connected Devices Access*

Note: For information about the advanced content filtering features port forwarding and port triggering, see *Port Forwarding/Port Triggering* on page 60.

Note: For help, click  .

Block Sites

Your router lets you restrict access to Internet content based on web addresses.

➤ **To block sites:**

1. Sign in to the web user interface.
2. From the main menu, select **Parental Controls > Block Sites**.

The following screen appears:

3. To turn on **Keyword Blocking**, select one of the following:
 - **Never:** Keyword blocking is always off, independent of scheduled settings.
 - **Per Schedule:** Keyword blocking turns on according to a schedule. See *Schedule Content Filtering* on page 41.
 - **Always:** Keyword blocking is always on, independent of scheduled settings.
4. Enter the keyword or domain you want to block in the provided field.

Some examples of blocked keywords are shown below.

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

Up to 32 entries are supported in the keyword list.

5. Click **Add**.
6. Click **Apply**.
7. (Optional) Delete unwanted keywords or domains.
 - a. Select the keyword from the list.
 - b. Click **Delete**.
 - c. Click **Apply**.
8. (Optional) Specify a trusted user.

Specify one trusted user, which is a computer that is exempt from blocking and signing in. Because an IP address identifies the trusted user, you should configure that computer with a fixed IP address.

- a. Select **Allow trusted IP address to visit blocked sites**.
- b. Enter that computer's IP address in the provided field.
- c. Click **Apply**.

Block Services

You can restrict Internet availability for specific users based on their IP addresses.

➤ To block services:

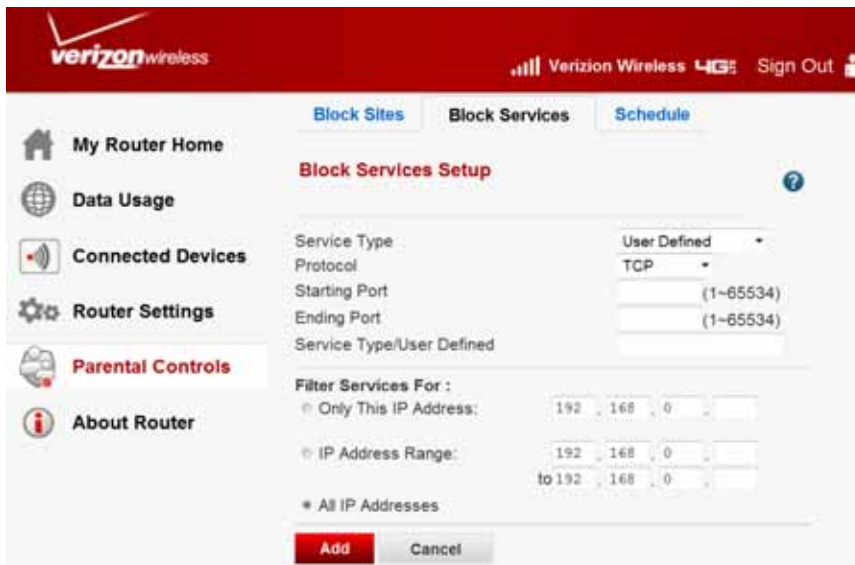
1. Sign in to the web user interface.

2. From the main menu, select **Parental Controls > Block Services**.



3. Select one of the following:
 - **Never**: Service blocking is always off, independent of scheduled settings.
 - **Per Schedule**: Service blocking turns on according to a schedule. See *Schedule Content Filtering* on page 41.
 - **Always**: Service blocking is always on, independent of scheduled settings.
4. Click **Add**.

The following screen appears:



5. To create a custom service, do one of the following:
 - Select a service from the **Service Type** list.
 - Select **User Defined** and, in the **Service/Type User Defined** field, enter a name for the service you want to block.
6. Click **Add** to create the service.

The service is listed in the **Service Table** on the **Block Services** screen.

7. Click **Apply**.

Schedule Content Filtering

If you turned on keyword or service blocking in the **Block Sites** or **Block Services** screens, you can schedule for when blocking occurs or when access is not restricted.

Your router uses Network Time Protocol (NTP) to find the current time and date.

- **To schedule content filtering:**
 1. Sign in to the web user interface.
 2. From the main menu, select **Parental Controls > Schedule**.

The following screen appears:

The screenshot shows the Verizon Wireless router web interface. The top navigation bar includes the Verizon logo, signal strength, 'Verizon Wireless', '4G LTE', and a 'Sign Out' button. The left sidebar contains a menu with 'My Router Home', 'Data Usage', 'Connected Devices', 'Router Settings', 'Parental Controls' (highlighted), and 'About Router'. The main content area is titled 'Schedule' and contains the following settings:

- Days to Block:** A list of days with checkboxes: Every Day (checked), Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.
- Time of day to block:(use 24-hour clock)**
 - All Day:** A checkbox that is checked.
 - Start Blocking:** Input fields for Hour (0) and Minute (0).
 - End Blocking:** Input fields for Hour (24) and Minute (0).
- Time Zone:** A dropdown menu showing '(GMT-05:00) Bogota, Lima, Quito, Eastern Time (US & Canada)'.
- Automatically adjust for daylight savings time:** A checkbox that is checked.
- Current Time:** Friday, 14 Jun 2013 14:07:49.

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

3. To block Internet keywords and services based on a schedule, select any of the following:
 - **Every Day:** Block access every day.
 - **One or more days:** Limits access completely for the selected days.
 - **All Day:** Limits access completely for the selected days.
 - **Start Blocking/End Blocking:** Limits access during specific times for the selected days.

Set the time of day to block 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.

4. Click **Apply**.

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

➤ **To specify your time zone:**

1. Sign in to the web user interface.
2. From the main menu, select **Parental Controls > Schedule**.

The following screen appears:

3. Select your time zone.

Use this setting for the block schedule according to your local time zone and for time-stamping log entries.

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

4. Click **Apply**.

Control Connected Devices Access

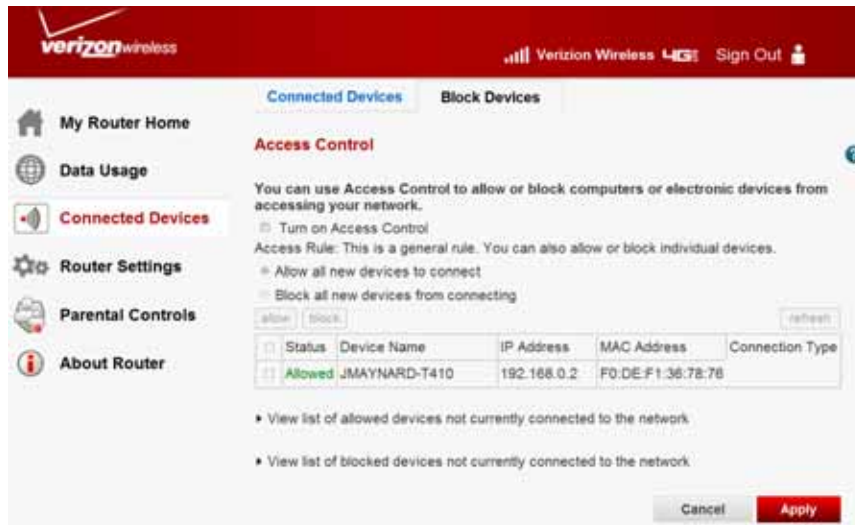
Use access control to allow or block computers, smartphones or tablets from connecting to your network. When a computer, smartphone or tablet is blocked:

- It IS able to get an IP address from your router.

- It is NOT able to communicate with other computers, smartphones or tablets.
- It is NOT able to connect to the Internet.

➤ **To set up access control:**

1. Sign in to the web user interface.
2. From the main menu, select **Connected Devices > Block Devices**.



3. To turn on access control, select **Turn on Access Control**.

This lets you control connections to your network. You will need to select this check box before you can create an access rule and use the Allow and Block buttons. When not selected, all computers, smartphones and tablets are allowed to connect, even if they are in the blocked list.

4. Select the access rule to apply to new computers, smartphones or tablets attempting to connect to your network.
 - **Allow all new devices to connect:** This is the default setting. It lets your new computer, smartphone or tablet connect to your network without the need to configure its MAC address.
 - **Block all new devices from connecting.** When this option is selected, your new computer, smartphone or tablet is not able to connect to your network until you add its MAC address to the allowed list. If a new computer has both wireless and Ethernet network connections, each connection has its own MAC address that needs to be added to the allowed list.

Note: The access rule does not affect previously blocked or allowed computers, smartphones or tablets. It applies only to those joining your network after you apply these settings.


5. Click **Apply**.

4 Manage Your Network

4

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

- *Set Password*
- *Back Up or Restore Router Settings*
- *Traffic Meter*
- *Router Status*
- *View Connected Devices*
- *View Access Logs*
- *Perform Diagnostics*

Note: For help, click  .

Set Password

For security reasons, the router has its own user name and password, and will automatically disconnect if it has not been used in a while.

Verizon recommends that you change your router password to a more secure password. The ideal password should follow these standards:

- Contain no dictionary words from any language
- Be a mixture of uppercase and lowercase letters, numbers, and symbols.

Your password can be up to 30 characters.

Change the Default Password

Note: If you changed the password and do not remember what it is, reset the router to its factory default settings. See *Restore the Default Configuration and Password* on page 95.

➤ **To change the default password:**

1. Sign in to the web user interface.
2. From the main menu, select **Router Settings > Router > Router Admin Password**.



3. Enter the **Current Admin Password**.
4. Enter the **New Admin Password**.
5. Enter the **New Admin Password** again.
6. Click **Apply**.

Note: Once the password has been changed, you will need to sign in again to make any other changes. If you have backed up the router settings previously, start a new backup to save the new password.

Change the Administrator Sign In Time-Out

For your security, access to the router configuration times out if it has not been used in a while.

➤ **To change the Administrator time-out period:**

1. Sign in to the web user interface.
2. From the main menu, select **Router Settings > Router > Router Admin Password**.
3. Enter a number in the **Administrator sign in times out after idle** field.

The suggested value is 60 minutes.

4. Click **Apply**.

Back Up or Restore Router Settings

Your router's configuration settings are stored in a file on the router. This file can be:

- *Backed up to your computer*
- *Restored*
- *Reverted to factory default settings*

Back Up the Configuration to a File

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

1. Sign in to the web user interface.

2. From the main menu, select **Router Settings > Router > Backup and Restore**.



3. Click **Back Up**.

A .cfg file is stored on a computer on your network.

Restore the Configuration from a File

➤ **To restore the configuration:**

1. Sign in to the web user interface.
2. From the main menu, select **Router Settings> Router > Backup and Restore**.



3. Click **Browse**.
4. Locate and select the .cfg file.
5. Click **Restore**.

The router resets the configuration settings.

Reset Default Settings

Use this feature to erase the router's configuration settings and restore the factory default settings.

➤ **To erase the configuration:**

1. Sign in to the web user interface.
2. From the main menu, select **Router Settings > Router > Backup and Restore**.



3. Click **Erase**.

The router restarts with the default settings.

After erasing, parameters are reset as:

Table 1.

Parameter	Setting
Router password	password
IP address	192.168.0.1
DHCP client status	On
Network name (SSID)	Reset to network name (SSID) on router label
Passphrase	Reset to passphrase on router label

See *Router Label* on page 9. For the factory default settings, see *Factory Defaults* on page 96.

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

Traffic Meter

Traffic metering lets you monitor the volume of Internet traffic passing through your router's Internet port. With it, you can:

- Set limits for traffic volume
- Set a monthly limit
- Get a live update of traffic usage
- Turn on separate traffic meters for the mobile broadband connection and the Ethernet connection.

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

1. Sign in to the web user interface.
2. From the main menu, select **Data Usage**.

The following screen appears:

The screenshot shows the 'Traffic Meter' configuration page. On the left is a navigation menu with 'Data Usage' selected. The main area has a red header with the Verizon logo and 'Sign Out' link. Below the header, there's a 'Traffic Meter' section with checkboxes for enabling the meter and options for traffic volume control (No limit, Monthly limit, Connection time control). A 'Traffic Counter' section allows restarting the counter at a specific time. A 'Traffic Control' section has options for warning messages and LED status. At the bottom, 'Connection Statistics' are shown for various periods (Today, Yesterday, This week, This month, Last month) with a table of upload/download/total traffic volume.

Period	Connection Time (h:mm)	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

3. Select **Enable Traffic Meter**.
4. (Optional) Control the volume of Internet traffic.

To control the volume of Internet traffic, use either the **Traffic Volume Control** feature or the **Connection Time Control** feature.

- Select **Traffic volume control by** and then select one of the following options:
 - **No Limit:** No restrictions occur when the traffic limit is reached.
 - **Download only:** Restrictions apply to incoming traffic only.
 - **Both Directions:** Restrictions apply to both incoming and outgoing traffic.
- 5. (Optional) If your Internet service provider charges for extra data volume when you make a new connection, enter it in MB in either the **Monthly limit** or the **Round up data volume for each connection** field.
- 6. Select **Connection time control** and enter the allowed hours in the Monthly limit field.
- 7. In **Traffic Counter**, set the traffic counter to begin on a certain time and date.
To start immediately, click **Restart Counter Now**.
- 8. In **Traffic Control**, specify if you will get a warning message before you have reached your monthly limit of MB or browsing hours.
By default, the value is 0 and no warning message is sent. Select an alert for when you have reached the limit:
 - The Internet LED blinks green or amber.
 - The Internet connection is disconnected and disabled.
- 9. Click **Apply**.
Click **Refresh** to update Traffic Statistics.
Click **Traffic Status** to show more information about the data traffic on your router.

Router Status

Use the **Router Status** screen to:

- See the status of the router
 - Show statistics
 - See the connection status
- **To see the router status:**
1. Sign in to the web user interface.
 2. From the main menu, select **About Router > Router Status**.

The following screen appears:

The screenshot displays the Verizon 4G LTE Broadband Router status page. The page has a red header with the Verizon logo and 'Verizon Wireless 4G LTE' signal strength indicator. A navigation bar includes 'Router Status', 'Diagnostics', 'Logs', and 'Support'. A left sidebar lists menu items: 'My Router Home', 'Data Usage', 'Connected Devices', 'Router Settings', 'Parental Controls', and 'About Router' (highlighted). The main content area is titled 'Router Status' and shows the following information:

- Active Connection:** 4G LTE Broadband
- Account Name:** MBR1515
- Firmware Version:** V3.2.2.20_LC
- Hardware Version:** V1.1
- WAN Broadband:**
 - MAC Address: 84:1B:5E:D3:F7:67
 - IP Address: 10.162.98.77
 - Network Type: DHCPClient
 - IP Subnet Mask: 255.255.255.252
 - Gateway IP Address: 10.162.98.78
 - Domain Name Server: 198.224.173.135
 - Modem Identity: MC7750
 - Modem SW version: 33_SW19000M_03.05.10.09ap r5700 oamld-en-10527 2013/03/12 10:37:48
 - Modem HW Version: "1.0"
 - Modem driver version: v1.7
 - IMSI: 311480001480490
 - MDN: +14086913467
 - UICC: 89148000000603891061
 - Access Number: *99***38
 - IMEI: 990000550400790
 - Operator: Verizon Wireless
 - Network mode: LTE
 - Network band: LTE
- LAN Port:**
 - MAC Address: 84:1B:5E:D3:F7:66
 - IP Address: 192.168.0.1
 - DHCP: ON
 - IP Subnet Mask: 255.255.255.0
- Wi-Fi Port:**
 - Name (SSID): Verizon-MBR1515-F700
 - Region: United States
 - Channel: Auto (11)
 - Wi-Fi AP: On
 - Broadcast Name: On

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

The following information is shown:

- **Active Connection:** The selected broadband connection (for example, 4G LTE broadband or WAN Ethernet).
- **Account Name:** The model of your router.
- **Firmware Version:** Your router's firmware version.
- **WAN broadband:** See *Configure Your Internet Settings* on page 15.
 - **MAC Address:** The MAC address used by your router's WAN port.
 - **IP Address:** The modem's IP address. If no address is shown, your router cannot connect to the Internet.
 - **Network Type:** DHCP Client.
 - **IP Subnet Mask:** The IP subnet mask used by your router's Internet port.

- **Gateway IP Address:** Your router's IP address.
- **Domain Name Server:** Your router's DNS server IP address. This address is found 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.
- **Port.** See *LAN Setup* on page 70.
 - **MAC Address:** The Ethernet MAC address used by your router's LAN port.
 - **IP Address:** The LAN port IP address. The default IP address is 192.168.0.1.
 - **DHCP:** If **Off**, IP addresses are not assigned to computers on the LAN. If **On**, IP addresses are assigned to computers on the LAN.
 - **IP Subnet Mask:** The LAN port IP subnet mask. The default IP is 255.255.255.0.
- **Wi-Fi Port.** See *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* on page 26.
 - **Network Name (SSID):** The service set ID, or Wi-Fi network name.
 - **Region:** The country where your router is set up for use.
 - **Channel:** The current channel, which determines the operating frequency.
 - **Wi-Fi AP:** Indicates if the Internet feature is disabled or not. If not enabled, the Wi-Fi LED on the front panel is off.
 - **Broadcast Name:** Indicates if your router lets other users know its network name.

3. To see your router usage statistics, click **Show 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 shown for each port:

- **Status:** The link status. Guest networks are 2, 3, and 4.
- **TxPkts:** The number of packets sent 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 how often your router polls these statistics.

4. For the status of the Internet connection, click **Connection Status**:

Mobile Broadband Status	
Connection Status	Negotiating
Received Signal Quality(in dbm)	-75
Bytes Transmitted	950
Bytes Received	29382
Tx B/s	0
Rx B/s	0
System Uptime	00:14:17

Connection Status	
Connection Time	00:00:00
Connecting to server	Off
Negotiation	--
Authentication	--
IP address	0.0.0.0
Network Mask	0.0.0.0

Poll Interval : (secs)

100% ▼

The following information is shown for each Internet connection mode:

- **Mobile broadband Status.**
 - **Connection Status:** The status of your Internet connection.
 - **No SIM card detected:** No SIM card has been detected in your router.
 - **Detecting Modem:** Your 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:** Your 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 sent 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 your router's last reboot.
- **Connection Status.**
 - **Connection Time:** How long the device has been connected to the network.
 - **Connecting to server:** Whether the device is connected to the server (On/Off).
 - **Negotiation:** The status of the network connection.
 - **Authentication:** The status of the network connection.
 - **IP address:** The unique public address provided to your router by the wireless mobile network.
 - **Network Mask:** The network mask address provided to your router by the wireless mobile network.

View Connected Devices

The **Attached Devices** screen shows all computers, smartphones and tablets that your router discovered on the local network.

➤ **To see the attached devices:**

1. Sign in to the web user interface.
2. From the main menu, select **Connected Devices > Connected Devices**.



For each device, the table shows the following:

- IP address
- Device name if available
- Ethernet MAC address

If your router is rebooted, this data is lost until the router rediscovers the devices. To force the router to look again for attached devices, click **Refresh**.

View Access Logs

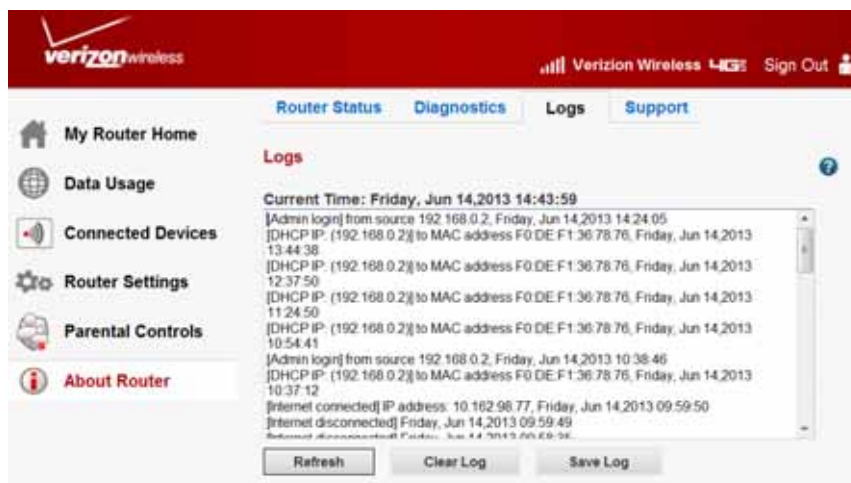
Your router logs security-related events such as:

- Denied incoming service requests
- Hacker probes
- Administrator sign ins

If you specify sites to block in the **Block Sites** screen, the **Logs** screen can show you when someone on your network tries to access a blocked site.

➤ To see, send, or clear the logs:

1. Sign in to the web user interface.
2. From the main menu, select **About Router > Logs**.



3. Click one of the following options:
 - **Refresh**: Updates the page with recent DHCP IP to MAC address activity.
 - **Clear Log**: Removes the messages from the page.
 - **Save Log**: Saves the log detail to a file.

Perform Diagnostics

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

➤ To use diagnostics:

1. Sign in to the web user interface.

2. From the main menu, select **About Router > Diagnostics**.

verizon wireless

Verizon Wireless 4G LTE Sign Out

Router Status Diagnostics Logs Support

My Router Home

Data Usage

Connected Devices

Router Settings

Parental Controls

About Router

Diagnostics

Ping an IP address

IP Address:

Perform a DNS Lookup

Internet Name:

IP Address:

DNS Server: 198.224.173.135
198.224.174.135

Display the Routing Table

Reboot the Router

Save Diagnostics File

Click the following options to perform diagnostic tests and actions:

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

Advanced Router Settings

5




WARNING:

Do not perform the following features without advanced network knowledge and experience.

This chapter describes how to configure the advanced features of your Verizon 4G LTE Broadband Router. You will find these tasks under Router settings > Advanced after signing in to the router.

- *Wi-Fi Repeating Function*
- *Port Forwarding/Port Triggering*
- *Miscellaneous WAN Settings*
- *LAN Setup*
- *Quality of Service Setup*
- *Dynamic DNS*
- *Static Routes*
- *Remote Management*
- *Universal Plug and Play*

See *The default Internet connection mode is 4G LTE broadband* on page 16 for information about broadband settings. See *WAN Ethernet Broadband Settings* on page 18 for information about WAN Ethernet broadband settings.

Note: For online help, click .

Wi-Fi Repeating Function



WARNING:

Your router is preset with the optimum settings. Verizon does not recommend changing these settings unless you are advised by Verizon support. An incorrect setting can disable your router.

The following security settings are not available when you enable the Wi-Fi repeating function. See *Configure WEP* on page 28:

- WPA-PSK (TKIP)
- WPA2-PSK (AES)
- WPA-PSK (TKIP) + WPA2-PSK (AES)
- The Wi-Fi repeating function cannot be used with Auto Channel. See *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 on page 26.*

➤ To configure the Wi-Fi repeating function:

1. Sign in to the web user interface.
2. From the main menu, select **Router Settings > Advanced > Wi-Fi Repeating Function**.

3. To use either bridge mode or repeater mode, select **Enable Wi-Fi Repeating Function**.

4. Select your preferred mode:
 - **Wi-Fi Repeater:** Your router communicates *only* with another base station–mode Wi-Fi device. You must enter the MAC address (physical address) of the other base station–mode Wi-Fi device. WEP or WPA-PSK (TKIP) should be used to protect this communication.
 - **Wi-Fi Base Station:** Select only if this router is the master for a group of repeater-mode Wi-Fi devices. The other repeater-mode Wi-Fi devices must be set to Wi-Fi Repeater-mode, using this router's MAC address. They then send all traffic to the master router. WEP security settings should be used to protect this traffic.
 - If selected, you will need to enter the MAC addresses of the other access points in the fields provided.
5. Click **Apply**.

Port Forwarding/Port Triggering

Your router is preset to block inbound traffic from the Internet to your computers, except for replies to your outbound traffic.

You can create exceptions to this rule:

- Allow remote computers on the Internet to access a server on your local network.
- Allow certain applications and games to work correctly if your router does not recognize their replies.

Your router provides two features for creating these exceptions:

- Port forwarding
- Port triggering

The next sections provide background information to help you understand these features.

Remote Computer Access Basics

When a computer on your network connects to a remote computer, smartphone or tablet through the Internet, your computer sends a message containing the source and destination address and process information to your router. Before forwarding your message to the remote computer, your router has to:

- Modify the source information
- Create and track the communication session so that replies can be routed back to your computer

Example: 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 enter a website address into the URL field, and your computer creates a web page request message with the following information to your router.

- **Source address:** Your computer's IP address.
 - **Source port number:** 5678, which is the browser session.
 - **Destination address:** The website's IP address.
 - **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. Before sending the web page request message, 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 the router chooses, 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.

4. The web server then composes a return message with the requested web page data to your router. The return message contains the following information:
- **Source address:** The website's IP address.
 - **Source port number:** 80, which is the standard port number for a web server process.
 - **Destination address:** Your router's public IP address 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. If yes, the router then modifies the message to restore the original address information that NAT replaced. Your router sends this reply message to your computer, which shows the web page. The message now contains the following information:
- **Source address:** The website's IP address.
 - **Source port number:** 80, which is the standard port number for a web server process.
 - **Destination address:** Your computer's IP address.
 - **Destination port number:** 5678, which is the browser session that made the initial request.
6. When you finish your browser session, your router eventually detects a period of inactivity in the communications. Your router then removes the session information from its session table and no longer accepts incoming traffic on port number 33333.

Port Triggering to Open Incoming Ports

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 your router to open more incoming ports when a particular outgoing port originates a session.

An example is Internet Relay Chat (IRC), outlined in the process below;

1. Your computer connects to an IRC server at destination port 6667.
2. The IRC server responds to your originating source port, and sends an “identify” message to your computer on port 113.
3. Using port triggering, 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.”

After you have defined a port triggering rule, the process for IRC expands:

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, and sends this request message to your router.
3. Your router then:
 - a. creates an entry in its internal session table describing this communication session between your computer and the IRC server;
 - b. stores the original information;
 - c. performs Network Address Translation (NAT) on the source address and port; and
 - d. 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 (for example, 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 NAT replaced 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 no longer accepts incoming traffic on ports 33333 or 113.

To configure port triggering, you need to know which inbound ports the application needs and the number of the outbound port triggering the opening of the inbound ports. You can usually get this information from 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

Normally, your router ignores any inbound traffic that is not a response to your own outbound traffic. Configure exceptions to this rule by using **Port Forwarding**.

A typical application of port forwarding can be shown by reversing the Port Triggering example's client-server relationship. In this case, a browser on a remote computer accesses a web server running on a computer in your local network. Using port forwarding, 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 effects of the port forwarding rule you have defined are outlined below:

1. The user of a remote computer opens a browser and requests a web page from www.example.com, which resolves to your router's public IP address. The remote computer composes a web page request message with the following destination information:
 - **Destination address:** The IP address of www.example.com (your router's address).
 - **Destination port number:** 80, which is the standard port number for a web server process.

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

2. Your router receives the request message and looks in its rules table for any rules regarding how to handle 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, which is sent to your router.
4. Your router performs Network Address Translation (NAT) on the source IP address, and sends this request message to the remote computer, which shows the web page from www.example.com.

To set up port forwarding, you need to know which inbound ports the application needs. Usually you can get this information from 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:

- Any computer on your network can use port triggering, 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. Sign in to the web user interface.
2. From the main menu, select **Router Settings > Advanced > Firewall > Port Forwarding/Port Triggering**.

By default, **Port Forwarding** is selected.



3. Select a service or create a custom service.
 - To select a service:
 - a. Select a service from the **Service Name** list.
 - b. Specify the computer's IP address.
 - c. Click **Add**.
 - To add a service that is not in the list:

- a. Click **Add Custom Application**.

- b. Configure the settings described in the following table.

Settings	Description
Service Name	A descriptive service name
Service Type	Select TCP/UDP .
Starting Port	The incoming starting port number of the range of ports that are opened when triggered.
Ending Port	The incoming ending port number of the range of ports that are opened when triggered.
Server IP Address	The local server's IP address.

- c. Click **Apply**.

The added service appears in the list.

Set Up Port Triggering

➤ To set up port triggering:

1. Sign in to the web user interface.
2. From the main menu, select **Router Settings > Advanced > Firewall > Port Forwarding/Port Triggering**.
3. Select **Port Triggering**.

The following screen appears:

The screenshot shows the Verizon Wireless router's web interface. The top navigation bar includes the Verizon logo, signal strength, 'Verizon Wireless 4G LTE', and a 'Sign Out' button. The left sidebar contains links to 'My Router Home', 'Data Usage', 'Connected Devices', 'Router Settings' (highlighted), 'Parental Controls', and 'About Router'. The main content area has tabs for 'Router', 'WiFi', and 'Advanced'. Under the 'Advanced' tab, there are sub-tabs for 'Wi-Fi Repeating Function', 'Firewall', 'LAN', 'Port Forwarding / Port Triggering' (selected), and 'Miscellaneous'. The 'Port Forwarding / Port Triggering' section includes a 'Please select the service type.' dropdown with 'Port Forwarding' and 'Port Triggering' (selected). Below this is a 'Disable Port Triggering' checkbox and a 'Port Triggering Time-out(in minutes)' field set to '20'. A 'Port Triggering Portmap Table' section contains a table with columns for '#', 'Enable', 'Service Name', 'Service Type', 'Inbound Connection', and 'Service User'. Below the table are buttons for 'Add Service', 'Edit Service', and 'Delete Service'. At the bottom are 'Apply' and 'Cancel' buttons.

4. Click **Add Service**.

The screenshot shows the 'Port Triggering - Services' configuration page. The top navigation bar and left sidebar are identical to the previous screenshot. The main content area has tabs for 'Router', 'WiFi', and 'Advanced'. Under the 'Advanced' tab, there are sub-tabs for 'Wi-Fi Repeating Function', 'Firewall', 'LAN', 'Port Forwarding / Port Triggering' (selected), and 'Miscellaneous'. The 'Port Triggering - Services' section includes a 'Service' section with fields for 'Service Name', 'Service User' (set to 'Any'), and 'Service Type' (set to 'TCP'). Below this is a 'Triggering Port' field set to '(1-65535)'. An 'Inbound Connection' section includes a 'Connection Type' dropdown set to 'TCP/UDP', and 'Starting Port' and 'Ending Port' fields both set to '(1-65535)'. At the bottom are 'Apply' and 'Cancel' buttons.

5. Configure the settings described in the following table.

Settings	Description
Service Name	A descriptive service name.
Service User	Select Any to allow any computer on the Internet to use this service. Select Single address and enter the IP address of one computer to only allow a trusted computer.
Service Type	Select TCP/UDP .
Triggering Port	Enter the outbound traffic port's number that opens the inbound ports.
Connection Type	Select: <ul style="list-style-type: none"> • TCP • UDP, • TCP/UDP (both) If you are not sure, select TCP/UDP .
Starting Port	The incoming starting port number of the range of ports that are opened when triggered.
Ending Port	The incoming ending port number of the range of ports that are opened when triggered.

6. Click **Apply**.

The added service appears in the list.

Miscellaneous WAN Settings

The **Miscellaneous** screen lets you:

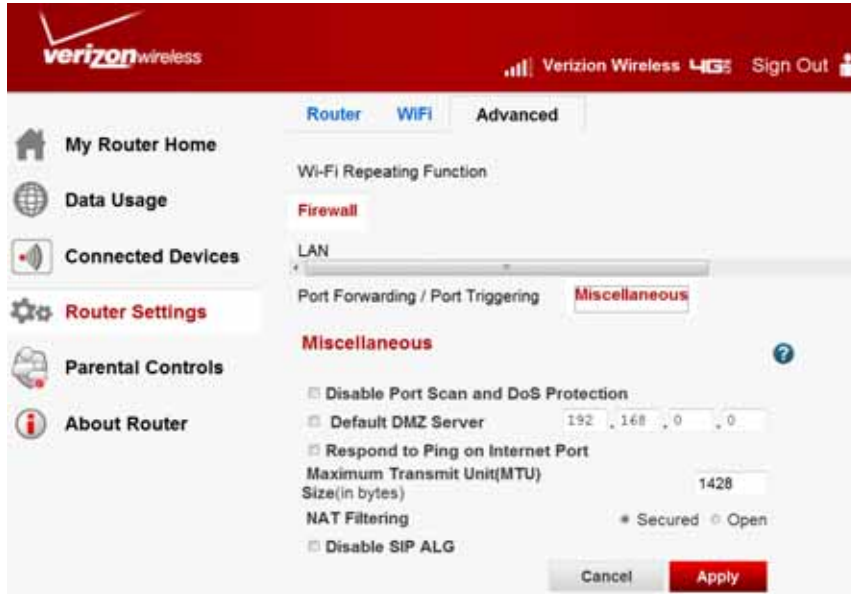
- Configure a DMZ (demilitarized zone) server.
- Change the maximum transmit unit (MTU) size.
- Enable the router to respond to a ping on the Wide Area Network (WAN) Internet port.

To change broadband Internet connection settings, use the **Broadband Settings** screen, as described in *Configure Your Internet Settings* on page 15.

➤ To see or to change the WAN setup:

1. Sign in to the web user interface.

2. From the main menu, select **Router Settings > Advanced > Firewall > Miscellaneous**.



3. Specify the following settings:

- **Disable Port Scans and DoS Protections:** This is cleared, letting the firewall protect your LAN against port scans and denial of service attacks. Select this check box only in special circumstances.
- **Default DMZ Server:** This feature is sometimes helpful when you are using some online games and videoconferencing. Using this feature makes the firewall security less effective. See *Set Up a Default DMZ Server* on page 69.
- **Respond to Ping on Internet:** Lets your router respond to a ping from the Internet. This feature should be used only as a diagnostic tool, because it lets your router be discovered.
- **MTU Size:** Maximum transmit unit (MTU) value. For most Ethernet networks, this setting is:
 - 1500 bytes;
 - 1492 bytes for PPPoE connections; or
 - 1436 bytes for PPTP connections.
- **NAT Filtering:** This parameter is set to **Secured** to provide a secure firewall, protecting computers on the LAN from attacks. The **Open** setting is less secure.
- **Disable SIP ALG:** Some Voice over IP (VoIP) applications do not work well with Session Initiation Protocol Application-level gateway (SIP ALG). Selecting this might help your VoIP devices create or accept a call through the router.

4. Click **Apply**.

Set Up a Default DMZ Server



WARNING:

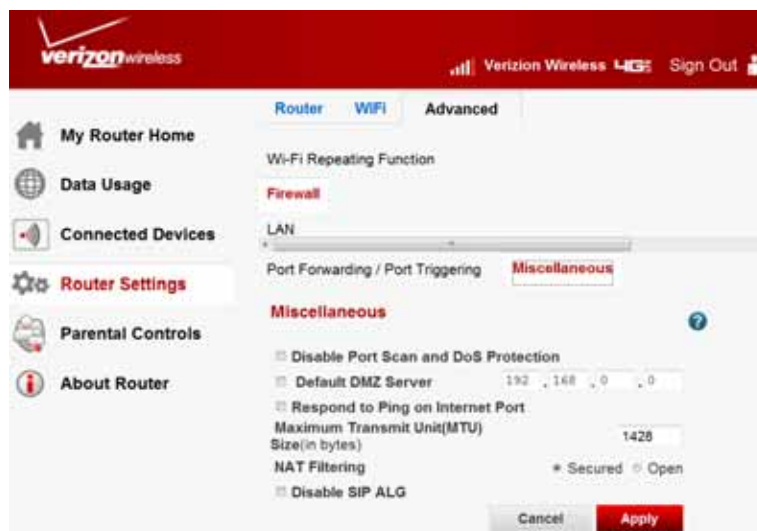
For security reasons, you should avoid using the default DMZ server feature. When a computer is designated as the default DMZ server, it loses much of the protection of the firewall and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

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

Your router normally discards incoming traffic from the Internet 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, forward it to one computer on your network dedicated as the default DMZ server.

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

1. Sign in to the web user interface.
2. From the main menu, select **Router Settings > Advanced > Firewall > Miscellaneous**.



3. Select **Default DMZ Server**.
4. Enter the IP address for that server.
5. Click **Apply**.

LAN Setup

The **Local Area Network (LAN) Setup** screen provides configuration of LAN IP services such as DHCP and Router Information Protocol (RIP).

Your router's default setup is to use private IP addresses on the LAN side, and to act as a DHCP server. The 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, make the changes in this screen.

Tip: If you change the LAN IP address of your router while connected through the browser, all users connected to the router will be disconnected. To reconnect, 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 see or change the LAN setup:**

1. Sign in to the web user interface.
2. From the main menu, select **Router Settings > Advanced > LAN**.

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

3. Specify the following settings:

- **Device Name:** Your router's name.
- **LAN TCP/IP Setup:**
 - **IP Address:** Your router's LAN IP address.
 - **IP Subnet Mask:** Your router's LAN subnet mask. Combined with the IP address, the IP subnet mask lets a computer, smartphone or tablet 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) lets a router exchange routing information with other routers. **RIP Direction** controls how your router sends and receives RIP packets. Your router is preset to **Both**.
 - 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 received.
 - **RIP Version:** This setting controls the format and the broadcasting method of the RIP packets that the router sends. Disabled is the default setting.
 - RIP-1 is universally supported. RIP-1 is adequate for most networks, unless you have an unusual network setup.
 - RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format.
 - RIP-2B uses subnet broadcasting.
 - RIP-2M uses multicasting.
- **DHCP Server.** For more information, see *DHCP Settings* on page 72.
 - **Use Router as a DHCP Server:** When selected, the router functions as a Dynamic Host Configuration Protocol (DHCP) server. See *DHCP Settings* on page 72.
 - **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 72.

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**.

DHCP Settings

Your router functions as a DHCP server, letting it assign the following to all computers connected to the router's LAN:

- IP address
- DNS server
- Default gateway address

The assigned default gateway address is your router's LAN address. 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 apply.

If another computer, smartphone or tablet on your network is the DHCP server, or if you manually configure the network settings of all of your computers, deselect **Use Router as DHCP Server** 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 subnetwork as the router's LAN IP address. Using the default addressing scheme, define a range between 192.168.0.2 and 192.168.0.254, saving part of the range for computers, smartphones or tablets with fixed addresses.

Your 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, your 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 lets your computers browse the network using the Network Neighborhood feature of Windows.

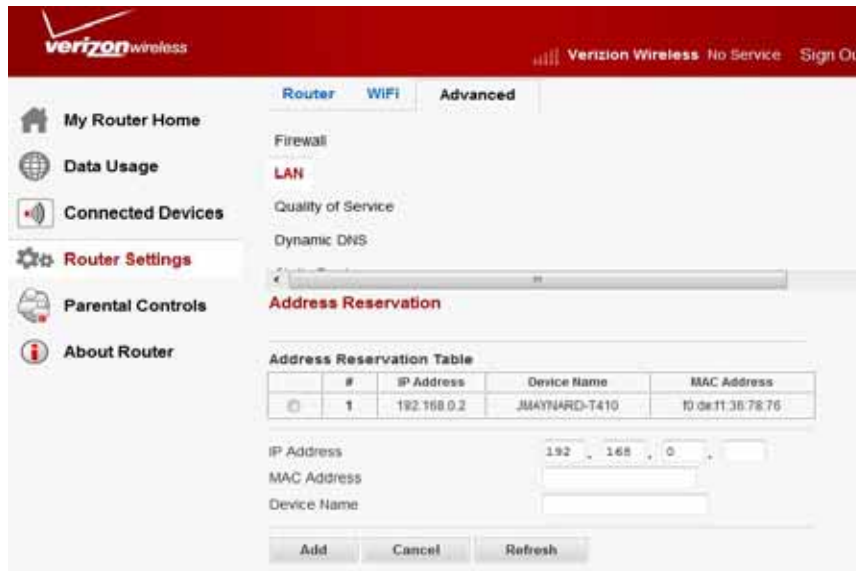
Reserved IP Addresses

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. Sign in to the web user interface.
2. From the main menu, select **Router Settings > Advanced > LAN**.
3. Under Address Reservation, click **Add**.

The following screen appears:



4. To assign to the computer or server, enter the IP address in the **IP Address** field. Choose an IP address from the router's LAN subnet, such as 192.168.0.x.
5. Enter 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. Selecting from the attached device list populates the fields automatically with the computer's MAC address and name.

6. Click **Apply**.

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

Quality of Service Setup

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

➤ **To set up QoS:**

1. Sign in to the web user interface.
2. From the main menu, select **Router Settings > Advanced > Quality of Service**.

The following screen appears.

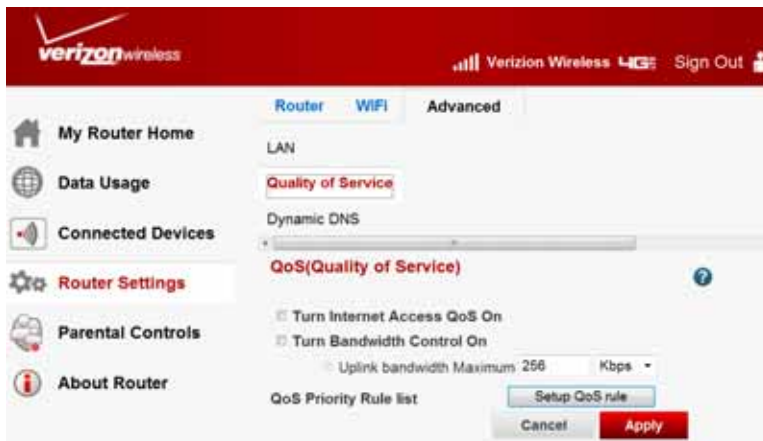


3. Specify the following settings:
 - **Turn Internet Access QoS On:** If you enable QoS, the QoS function works to prioritize Internet access traffic.
 - For information about setting up QoS rules, see *QoS Priority Rule List* on page 74.
 - **Turn Bandwidth Control On:** Select to set up the total maximum uplink bandwidth.
4. Click **Apply**.

QoS Priority Rule List

➤ **To set up a QoS priority rule:**

1. Sign in to the web user interface.
2. From the main menu, select **Router Settings > Advanced > Quality of Service**.



3. Click **Setup QoS rule**.

The following screen appears:

Quality of Service

Dynamic DNS

Static Routes

ID	Service	Priority	Application
8	Netgear EVA	Highest	Netgear EVA Applications
9	SSH	High	SSH Applications
10	Telnet	High	Telnet Applications
11	VPN	High	VPN Applications
12	FTP	Normal	FTP Applications
13	SMTP	Normal	SMTP Applications
14	WWW	Normal	WWW Applications
15	DNS	Normal	DNS Applications
16	ICMP	Normal	ICMP Applications
17	eMule / eDonkey	Low	eMule / eDonkey Applications
18	Kazaa	Low	Kazaa Applications
19	Gnutella	Low	Gnutella Applications
20	BT / Azureus	Low	BT / Azureus Applications
21	Counter Strike	High	Online Gaming Counter Strike
22	Ages of Empires	High	Online Gaming Age of Empires
23	Everquest	High	Online Gaming Everquest
24	Quake 2	High	Online Gaming Quake 2
25	Quake 3	High	Online Gaming Quake 3
26	Unreal Tournament	High	Online Gaming Unreal Tournament
27	Warcraft	High	Online Gaming Warcraft

Edit Delete Delete All

Add Priority Rule

Apply Cancel

4. To add a service to the **QoS Priority Rule** list, select the service you want.

5. To create a policy, click **Add Priority Rule**.

The priority categories described are available:

- *QoS for Applications and Online Gaming* on page 76
- *QoS For Ethernet LAN Ports* on page 79
- *QoS for a MAC Address* on page 79

6. Click **Apply**.

Set Up QoS for Internet Access

You can give prioritized Internet access to the following kinds of traffic:

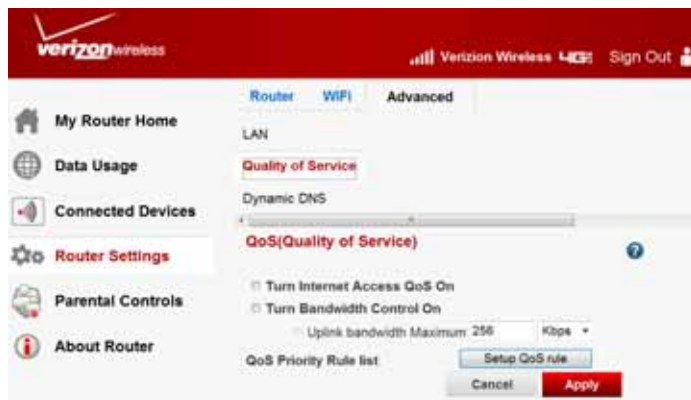
- Specific applications
- Specific online games
- Individual Ethernet LAN ports of the router
- A specific computer, smartphone or tablet by MAC address

To specify order of traffic importance, create a policy for the kind of traffic and add the policy to the **QoS Policy** table in the **QoS Setup** screen. For convenience, the **QoS Policy** table lists many common applications that can benefit from QoS handling.

QoS for Applications and Online Gaming

- To set up the priority rule for an application or online gaming:
 1. Sign in to the web user interface.
 2. Select **Router Settings > Advanced > Quality of Service**.

The following screen appears.



3. Click **Setup QoS rule**.

The following screen appears:

Quality of Service

Dynamic DNS

Static Routes

Priority	Application	Priority	Application
8	Netgear EVA	Highest	Netgear EVA Applications
9	SSH	High	SSH Applications
10	Telnet	High	Telnet Applications
11	VPN	High	VPN Applications
12	FTP	Normal	FTP Applications
13	SMTP	Normal	SMTP Applications
14	WWW	Normal	WWW Applications
15	DNS	Normal	DNS Applications
16	ICMP	Normal	ICMP Applications
17	eMule / eDonkey	Low	eMule / eDonkey Applications
18	Kazaa	Low	Kazaa Applications
19	Gnutella	Low	Gnutella Applications
20	BT / Azureus	Low	BT / Azureus Applications
21	Counter Strike	High	Online Gaming Counter Strike
22	Ages of Empires	High	Online Gaming Age of Empires
23	Everquest	High	Online Gaming Everquest
24	Quake 2	High	Online Gaming Quake 2
25	Quake 3	High	Online Gaming Quake 3
26	Unreal Tournament	High	Online Gaming Unreal Tournament
27	Warcraft	High	Online Gaming Warcraft

Edit Delete Delete All

Add Priority Rule

Apply Cancel

4. Click **Add Priority Rule**.

The following screen appears.

QoS - Priority Rules

Priority

QoS Policy for

Priority Category

Applications

Priority

Specified Port Range

Connection Type

Starting Port

Ending Port

Apply Cancel

5. From the **Priority Category** list, select **Applications** or **On-line Gaming**.

The screenshot shows the Verizon Wireless router's web interface. The left sidebar contains links: My Router Home, Data Usage, Connected Devices, Router Settings (highlighted), Parental Controls, and About Router. The main content area is titled 'QoS - Priority Rules'. It includes a 'Priority Policy for' field, a 'Priority Category' dropdown menu (set to 'Applications'), and a 'Priority' dropdown menu (set to 'Normal'). Below these is a 'Specified Port Range' section with a 'Connection Type' dropdown (set to 'TCP/UDP'), 'Starting Port' (1-65535), and 'Ending Port' (1-65535). At the bottom are 'Apply' and 'Cancel' buttons.

This screenshot is identical to the one above, but the 'Priority Category' dropdown menu is set to 'Online Gaming' instead of 'Applications'. The 'Add a new game' link is visible below the dropdown.

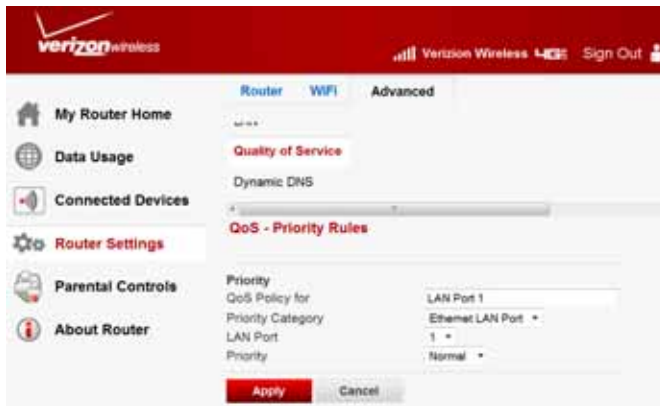
6. In the **QoS Policy** field, enter the name of the application or game.
7. In the **Priority Category** list, select either **Applications** or **Online Gaming**.
8. Scroll and select **Add a New Application**, or **Add a New Game**, as applicable.
9. If prompted, in the **Connection Type** list, select either **TCP**, **UDP**, or **TCP/UDP (both)**. Specify the port number or range of port numbers being used.
10. From the **Priority** list, select the priority for Internet access for this traffic relative to other applications and traffic. Click **Apply**.

The rule is saved in the **QoS Policy** list.

The **QoS Setup** screen appears.

QoS For Ethernet LAN Ports

- To create a QoS policy for a computer, smartphone or tablet connected to one of the router's LAN ports:
 1. Sign in to the web user interface.
 2. Select **Router Settings > Advanced > Quality of Service**.
 3. Select **Turn Internet Access QoS On**.
 4. Click **Setup QoS Rule**.
 5. Click **Add Priority Rule**.



6. From the **Priority Category** list, select **Ethernet LAN Port**.
7. From the **LAN Port** list, select the LAN port number.
8. From the **Priority** list, select the priority for Internet access for this port's traffic relative to other applications.
9. Click **Apply**.

The rule is saved in the **QoS Policy** list.

The **QoS Setup** screen appears.

QoS for a MAC Address

- To create a QoS policy for traffic from a specific MAC address:
 1. Sign in to the web user interface.
 2. Select **Router Settings > Advanced > Quality of Service**.
 3. Click **Setup QoS Rule**.
 4. Click **Add Priority Rule**.

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

verizon wireless Verizon Wireless 4G LTE Sign Out

Router WiFi Advanced

My Router Home

Data Usage

Connected Devices

Router Settings

Parental Controls

About Router

Quality of Service

Dynamic DNS

QoS - Priority Rules

Priority

QoS Policy for

Priority Category

MAC Address

MAC Device List

QoS Policy	Priority	Device Name	MAC Address
P1_MAC_367E76	Normal	JIMMYNARD-T410	F0:DE:F1:36:79:76

MAC Address

Device Name

Priority

Normal

Add Edit Delete Refresh

Apply Cancel

6. If the computer, smartphone or tablet to be prioritized appears in the **MAC Device** list, select it.

The information from the **MAC Device** list populates the following fields:

- Policy name
- MAC Address
- Device Name

If the computer, smartphone or tablet does not appear in the **MAC Device** list, click **Refresh**. If it still does not appear, fill in these fields.

7. From the **Priority** list, select the priority for Internet access for this device's traffic relative to other applications and traffic.
8. Click **Apply**.

This rule is saved in the **QoS Policy** list.

The **QoS Setup** screen appears.

9. Select **Turn Internet Access QoS On**.

10. Click **Apply**.

Edit or Delete an Existing QoS Policy

- To edit or delete a QoS policy:

1. Sign in to the web user interface.
2. Select **Router Settings > Advanced > Quality of Service**.
3. Click **Setup QoS Rule**.
4. Select the QoS policy that you want to edit or delete, and either:

- Click **Delete** to remove the QoS policy.
- Click **Edit** to edit the QoS policy and change the policy settings.

5. Click **Apply**.

Your changes are saved in the **QoS Setup** screen.

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, 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.

Your router contains a client that can connect to a Dynamic DNS service provider. To use this feature, select a service provider and set up 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.
- 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. The router IP address appears on the Router Status screen

For more information, see *Router Status* on page 50.

➤ **To configure Dynamic DNS:**

1. Sign in to the web user interface.

- From the main menu, select **Router Settings > Advanced > Dynamic DNS**.



- Go to the website of one of the Dynamic DNS service providers whose URLs appear in the **Service Provider** list, and register for an account.
- Select **Use a Dynamic DNS Service**.
- Select the URL of your Dynamic DNS service provider.
- Enter the **Host Name**, **User Name**, and **Password**.

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

Example: For dyndns.org, visit www.DynDNS.org.

- Click **Apply**.

Static Routes

Static routes provide more routing information to your router. Usually, your router has enough routing information after it has been configured for Internet access. You will need to configure static routes only for unusual cases such as multiple routers or multiple IP subnets on your network.

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

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

When you first configured your router, two implicit static routes were created:

- A default route, with your ISP as the router.
- A static route to your local network for all 192.168.0.x addresses.

With this configuration, if you attempt to access a computer, smartphone or tablet on the 134.177.0.0 network, your router forwards your request to the ISP, which forwards your request to the company where you are employed, where your company's firewall will likely deny the request.

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.
- The value in the **Metric** field represents the number of routers between your network and the destination.
- **Private** is selected only as a precautionary security measure in case RIP is activated.

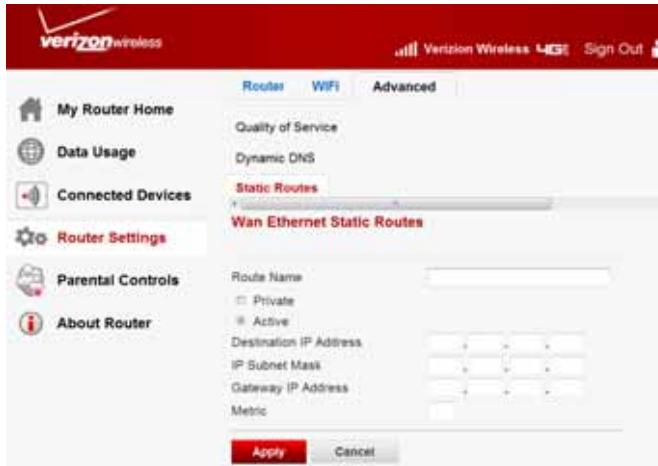
➤ **To configure static routes:**

1. Sign in to the web user interface.
2. From the main menu, select **Router Settings > Advanced > Static Routes**.



3. Select the static route you want to configure.
4. Click **Add**.

The following screen appears:



5. In the **Route Name** field, enter a name for this static route (for identification purposes only).
6. Select **Private** if you want to limit access to the LAN only.
If selected, the static route is not reported in RIP.

7. To make this route effective, select **Active**.
8. In the **Destination IP Address** field, enter the IP address of the final destination.
9. In the **IP Subnet Mask** field, enter the IP subnet mask for this destination. If the destination is a single host, type **255.255.255.255**.
10. In the **Gateway IP Address** field, enter the gateway IP address, which has to be on the same LAN segment as the router.
11. In the **Metric** field, enter a number from 1 through 15 as the metric value.

This value represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but for a direct connection, set it to 1.

12. Click **Apply**.

The static route is added.

➤ **To edit or delete a static route:**

1. Sign in to the web user interface.
2. Select **Router Settings > Advanced > Static Routes**.

The **Static Routes** screen appears.

3. In the table, select the route that you want to edit or delete.
4. Do one of the following:
 - Click **Edit**.

The **Static Routes** screen adjusts.

- a. Edit the route information.
- b. Click **Apply**.

- Click **Delete**.

The route is removed from the table.

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.



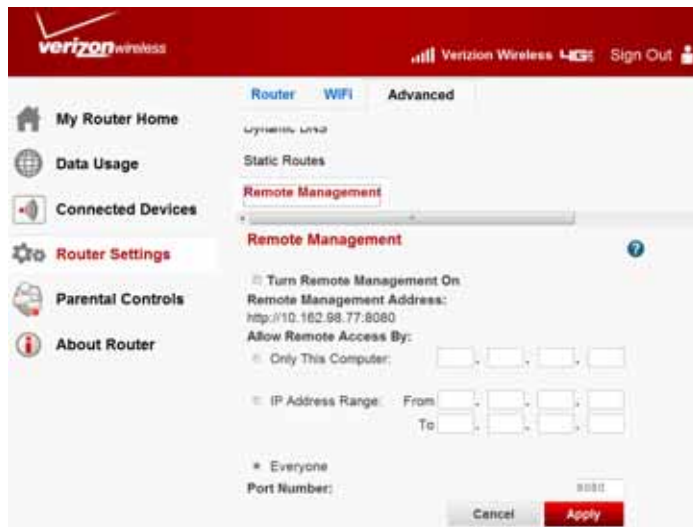
WARNING:

If your ISP assigns a private WAN IP address such as 192.168.x.x or 10.x.x.x, the Remote Management service does not work because private addresses are not routed on the Internet. The router IP address appears on the Router Status screen. For more information, see *Router Status* on page 50.

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, up to 30 characters. See *Set Password* on page 45.

➤ To configure remote management:

1. Sign in to the web user interface.
2. From the main menu, select **Router Settings > Advanced > Remote Management**.



3. Select **Turn Remote Management On**.
4. Specify the external IP addresses with connection to your router's remote management.

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

Under **Allow Remote Access By**, select one of the following:

- For a single IP address on the Internet, select **Only This Computer**. Enter the IP address.
- For a range of IP addresses on the Internet, select **IP Address Range**. Enter a beginning and ending IP address to define the allowed range.
- For connection from any IP address on the Internet, select **Everyone**.

5. Specify the port number for accessing the web management interface.

Normal web browser access uses the standard HTTP service port 80. For greater security, enter a custom port number for the remote web management interface. Choose a number from 1024 to 65535, but do not use the number of any common service port. The default port number is 8080, which is a common alternate for HTTP.

6. Click **Apply**.
7. When you access your router from the Internet, enter your router's WAN IP address into your browser's address or location field followed by a colon (:) and the custom port number.

Example: If your external address is 134.177.0.123 and you use port number 8080, enter **http://134.177.0.123:8080** in your browser.

Universal Plug and Play

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

If you use applications such as multiplayer gaming, peer-to-peer connections, or real-time communications, you should enable UPnP.

➤ To turn on Universal Plug and Play:

1. Sign in to the web user interface.

- From the main menu, select **Router Settings > Advanced > UPnP**.



- Select **Turn UPnP On**.

This check box is selected as a default setting. UPnP for automatic computer, smartphone tablet or console configuration can be enabled or disabled. If the **Turn UPnP On** check box is cleared, the router does not let any electronics automatically control the resources, such as port forwarding (mapping), of the router.

- Enter an amount in the **Advertisement Period** field (in minutes).

The advertisement period specifies how often the router broadcasts its UPnP information. This value can range from 1 to 1440 minutes, with a default period of 30 minutes.

- Shorter durations ensure that control points have the current status at the expense of more network traffic.
- Longer durations can compromise the freshness of the status, but can significantly reduce network traffic.

- Enter an amount in the **Advertisement Time to Live** field (in hops).

The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. Hops are the steps a packet takes between routers, ranging from 1 to 255, with a default value of four hops. If you notice that some computers, smartphones, tablets or consoles are not being updated or reached correctly, it might be necessary to increase this value.

- Click **Apply**.

The UPnP Portmap table shows the IP address of each UPnP device that is accessing the router and which ports (internal and external) it has opened. The UPnP Portmap table also shows what kind of port is open and whether that port is still active for each IP address.


- (Optional) To refresh the information in the UPnP Portmap table, click **Refresh**.

Troubleshooting

6

This chapter gives information about troubleshooting your 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?
See *Basic Functioning* on page 89.
- Have I connected the router correctly?
See *Basic Functioning* on page 89.
- I cannot access the router's configuration with my browser.
See *Troubleshoot Access to the Router Main Menu* on page 91.
- I have configured the router but I cannot access the Internet.
See *Troubleshoot Your Connection* on page 92.
- I cannot connect to a specific IP address.
See *Troubleshoot a TCP/IP Network Using the Ping Utility* on page 94.
- The router shows the wrong the date and time.
See *Problems with Date and Time* on page 95.
- I want to clear the configuration and start over again.
See *Restore the Default Configuration and Password* on page 95.

Note: For online help, click  .


Basic Functioning

After you turn on your router, the following should occur:







1. When power is first applied, make sure that the Power LED is lit.
2. After approximately 10 seconds, look for the following:
 - a. The Power LED is still solid green. An amber LED indicates that the router has failed its power-on self-test (POST).
 - b. The Internet Port LED is lit.
 - c. The Wi-Fi LED is lit.
 - d. The Ethernet LAN Port LED is lit when any local ports are connected.
 If a local area network (LAN) port's LED is lit, a link has been established to the connected computer. If a LAN port is connected to 100-Mbps equipment, the port's LED is green. If the equipment is 10 Mbps, the LED is amber.
 - e. The Ethernet wide area network (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 poor coverage.

If any of these conditions do not occur, see the following table.

Table 1. LED indicators

LED		Action
Power 	Power LED is off.	<ul style="list-style-type: none"> Make sure that the power cord is correctly connected to your router, and that the power supply adapter is correctly plugged into a working power outlet. Check that you are using the power adapter supplied for this product. If the error persists, you might have a hardware problem and should contact technical support.
	Power LED is amber.	POST (power-on self-test) is in progress. Wait for this test to complete.

Verizon 4G LTE Broadband Router

LED (continued)		Action (continued)
Internet Port 	Internet Port LED is off.	Be sure the SIM card that you received is in the router. SIM cards from other electronics do not function in the router, and this SIM card does not function in other electronics.
	Internet Port LED is amber.	The router cannot connect to the Internet. Check the Internet connection being used. <ul style="list-style-type: none"> • For a mobile broadband connection, check the Signal Quality LED. • For an Ethernet connection, check the WAN Port LED.
	Internet Port LED is blinking amber and green.	The traffic meter feature is enabled, and the limit set has been reached.
Wi-Fi 	Wi-Fi LED is off.	The Wi-Fi radio is off. For a Wi-Fi connection with the router, press the Wi-Fi 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 connection and check your router's Wi-Fi settings.
Ports 	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"> • The Ethernet cable connections are secure at both ends. • The power is turned on to the connected hub or workstation.
WAN Port 	WAN Port LED is off.	If using an Ethernet connection, check the following: <ul style="list-style-type: none"> • The Ethernet cable connections are secure at both ends. • The power is turned on to the modem.
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 a mobile broadband connection is used, check the following: <ul style="list-style-type: none"> • Ensure that good coverage exists in the area by checking with your Internet service provider. • Ensure that your mobile broadband account is active. • Ensure that the SIM card is inserted correctly into the router. • Move the router near a window or other area of the building. Log in to the router menu and check the Internet configuration. Check that the user name, password, and network name are set correctly. If you use a PIN to connect to the Internet, check that it is entered correctly.

Troubleshoot Access to the Router Main Menu

If you can't 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 connection between the computer and the router.
- Make sure your computer's IP address is on the same subnetwork as the router. Your computer's IP 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 in the range of 169.254.x.x when the computer cannot reach a DHCP server. 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 default settings and set your router's IP address to 192.168.0.1. See *Restore the Default Configuration and Password* on page 95.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click the **Refresh** button to be sure that the Java applet is loaded.
- Close the browser and open it again.
- Make sure that you are using the correct sign in information. The factory default sign in 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 your changes, check the following:

- When entering configuration settings, click **Apply** before moving to another screen or tab, or your changes are lost.
- Click **Refresh** or **Reload** in the browser. Your changes may have occurred, but the browser might not have updated yet.

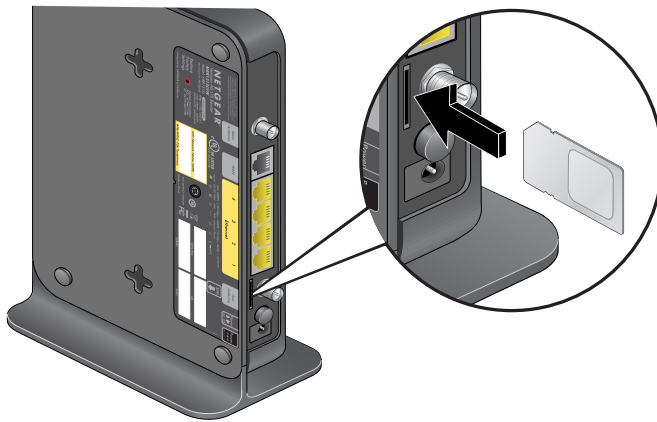
Troubleshoot Your Connection

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

Connecting to the Internet

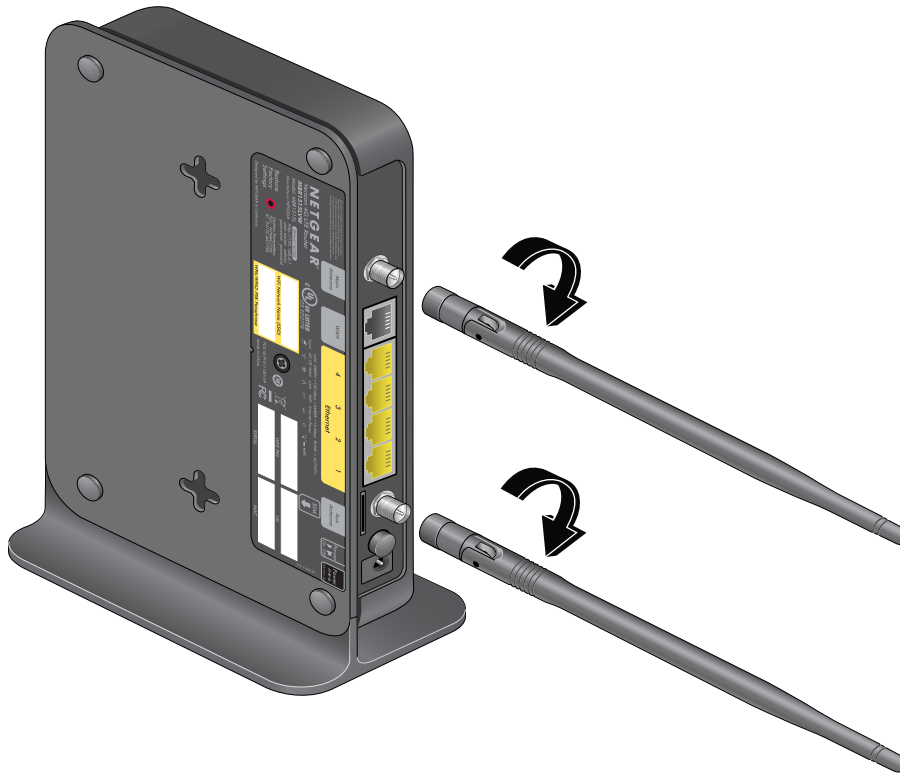
If unable to connect to Internet, check the following:

1. The Internet account is active.
2. The 4G LTE SIM card has been inserted into the SIM card slot on the back of the router.



3. Wireless broadband coverage is available where the router is located.
4. The router's broadband settings are correct. Check with your ISP if you are unsure.
5. Check the location of your router:
 - a. Move the router closer to a window for a better signal.
 - A blue Signal Quality LED indicates excellent coverage.
 - A green Signal Quality LED indicates good coverage.
 - An amber Signal Quality LED indicates poor coverage.
 - A Signal Quality LED that is off indicates no coverage.
 - b. Move the router away from any appliances causing interference (see *Interference Reduction Table* on page 100).

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



External antennas are shipped with the router and have to be installed. See *Insert the SIM Card* on page 10.

Troubleshoot Internet Browsing

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

- The traffic meter is on and the limit has been reached.
By changing the traffic meter not to block your connection when the limit is reached, you can resume Internet access. Your ISP may charge you for any overages.
- Your computer may not recognize any Domain Name System (DNS) server addresses.
A DNS server is a host that translates Internet names (such as www addresses) to numeric IP addresses. If you entered a DNS address during the router's configuration, reboot your computer and verify the DNS address. Or, setup your computer manually with DNS addresses.
- Your computer may not have the router configured as its Transmission Control Protocol (TCP)/IP router.

If your computer gets its information from the router by Dynamic Host Configuration Protocol (DHCP), reboot the computer, and verify the router address.

Troubleshoot a TCP/IP Network Using the Ping Utility

Most TCP/IP terminal routers contain a ping utility that sends an echo request packet to the designated computer, smartphone or tablet, which responds with an echo reply.

Test the LAN Path to Your Router

To verify that the path to your router is set up correctly, ping the router from your computer.

➤ **To ping your router from a computer running Windows 95 or later:**

1. From the Windows toolbar, click **Start**, and select **Run**.
2. Enter **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
 - Check if the LAN Port LED is lit. If the LED is off, follow the instructions in *Connecting to the Internet* on page 92.
 - Check that the corresponding link LEDs are lit for your network interface card and for the hub ports (if any).
- 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 subnetwork.

Test the Path from Your Computer to a Remote Device

If the path works correctly, test the path from your computer to a remote computer.

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

```
ping -n 10 IP address
```

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

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

- Check that your computer has the IP address of your router listed as the default router. If DHCP assigned the IP configuration of your computer, this information is not visible.
- 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 equipment.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your computer, enter it 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. If so, you will need to configure your router to clone or spoof the MAC address from the authorized computer. See the *Verizon Get to Know Your Device*.

Problems with Date and Time

The email screen shows the current date and time of day. The router uses the Network Time Protocol (NTP) to get the current time from the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000.
Cause: The router has not yet successfully reached a network time server. Check that your Internet access settings are correct, wait at least five minutes, then check the date and time again.
- Time is off by one hour.
Cause: The router does not automatically sense daylight saving time. On the Schedule screen, select **Automatically adjust for Daylight Savings Time**.

Restore the Default Configuration and Password

You can erase the current configuration and restore the factory default settings, changing the router's admin password to **password** and the IP address to **192.168.0.1**, in two ways:

- Use the Erase feature (see *Reset Default Settings* on page 48).
- Press the **Restore Factory Settings** button on the side of the router for six seconds. For a list of the factory default settings, see *Factory Defaults* on page 96.

Factory Defaults

Verizon 4G LTE Broadband Router User GuideVerizon 4G LTE Broadband Router User Guide

You can return the router to its factory settings. Use the end of a paper clip or a similar object to press and hold the **Reset** button on the side of the router for at least six seconds. The router resets, and returns to the factory configuration settings shown in the following table.

Table 1. Factory default settings

Feature		Default behavior
Router sign in	User sign in URL	www.routerlogin.com or www.routerlogin.net
	User name (case-sensitive)	admin
	Sign in password (case-sensitive)	password
Internet connection	WAN MAC address	Use default hardware address
	WAN MTU size	1500
	Port speed	AutoSensing
Local network (LAN)	IP	192.168.1.1
	Subnet mask	255.255.255.0
	DHCP server	Enabled
	DHCP range	192.168.1.2 to 192.168.1.254
	DHCP starting IP address	192.168.1.2
	DHCP ending IP address	192.168.1.254
	DMZ	Disabled
	Time zone	Pacific Standard Time for North America
	Time zone adjusted for daylight savings time	Disabled
Firewall	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the HTTP port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled
Mobile Broadband	Internet service provider	Verizon

Table 1. Factory default settings (continued)

Feature		Default behavior
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 Wi-Fi devices allowed

Notification of Compliance



NETGEAR wireless routers, gateways, APs

Regulatory Compliance Information

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

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

Europe – EU Declaration of Conformity

Products bearing the  marking comply with the following EU directives:

- EMC Directive 2004/108/EC
- Low Voltage Directive 2006/95/EC

If this product has telecommunications functionality, it also complies with the requirements of the following EU Directive:

- R&TTE Directive 1999/5/EC

Compliance with these directives implies conformity to harmonized European standards that are noted in the EU Declaration of Conformity.

For indoor use only. Valid in all EU member states, EFTA states, and Switzerland.

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

FCC Requirements for Operation in the United States

FCC Information to User

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

FCC Guidelines for Human Exposure

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

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

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the Verizon 4G LTE Broadband Router 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 and Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
- Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.
- Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Verizon 4G LTE Broadband Router) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

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

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

Industry Canada

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

Caution:

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

IMPORTANT NOTE: Radiation Exposure Statement:

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

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

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

Interference Reduction Table

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

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

A 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

Index

A

access **46**
 restricting by MAC address **25, 35**
 router password **45**
accessing remote computer **60**
administrator login **46**
attached devices **55**

B

back panel **8**
blocking
 inbound traffic **60**
 keywords and sites **38**
 services **39**

C

compliance **98**
compliance, adapters **98**
configuration backup **46**
configuring
 QoS **73**
connection status **54**
control buttons **6**

D

date and time **95**
daylight savings time **42, 95**
default factory settings, list of **96**
Denial of Service (DoS) **37**
DHCP **14, 72**
diagnostics **56**
DMZ server **69**
DNS servers **60**
Dynamic DNS, configuring **81**

E

Ethernet broadband settings **18**

F

factory defaults **9, 48**
factory settings
 list of **96**
front panel **6**

I

inbound traffic, allowing or blocking **60**
interference **25**
Internet Port LED **6**
Internet Relay Chat (IRC) **62**
IP addresses
 attached devices **55**
 autogenerated **91**
 DMZ server **69**
 LAN setup **70**
 port forwarding **63**
 reserved **72**
 troubleshooting **93**
 trusted user, setting **39**

K

keywords, blocking **38**

L

label **9**
LAN setup **70**
LED descriptions **7**
logging in and out **13**
login not required **21**
login required **19**

M

MAC address **95**
 location of **37**
 restricting access **25**
MAC addresses
 QoS for **79**
manual configuration **15**
metric value **83**

mobile broadband settings [16](#)

N

NAT (Network Address Translation) [61](#)

network management [44](#)

Network Time Protocol (NTP) [41](#), [95](#)

P

password

 changing [45](#)

 restoring [95](#)

placement [24](#)

port forwarding [60](#), [63](#), [64](#)

port triggering [60](#), [61](#), [64](#)

ports, LAN and WAN [7](#)

Power LED [7](#)

preset security, about [25](#)

Q

Quality of Service (QoS) [73](#)

R

range [25](#)

remote management [85](#)

reserved IP addresses [71](#)

restoring factory defaults [9](#), [48](#)

restricted access [35](#)

S

security [25](#)

security PIN [31](#)

settings, default. See default factory settings [96](#)

showing statistics [53](#)

signal quality [8](#)

static routes [82](#)

status LEDs [6](#), [89](#)

T

TCP/IP network, troubleshooting [94](#)

technical support [1](#)

time of day [95](#)

time out, login [46](#)

time zone [42](#)

time-stamping [43](#)

trademarks [1](#)

traffic meter [49](#)

troubleshooting [88](#)

trusted host [39](#)

U

Universal Plug and Play (UPnP) [86](#)

W

WAN Port LED [7](#)

WAN setup [67](#)

websites, blocking [38](#)

WEP [25](#), [28](#)

Wi-Fi Protected Setup (WPS) [31](#), [32](#)

Wi-Fi, LED and button [7](#)

WINS [72](#)

wireless configuration [24](#)

wireless devices, adding to the network [31](#)

wireless repeat function [59](#)

WPA [25](#), [27](#)

WPA + WPA2 [27](#)

WPA2 [25](#), [27](#)

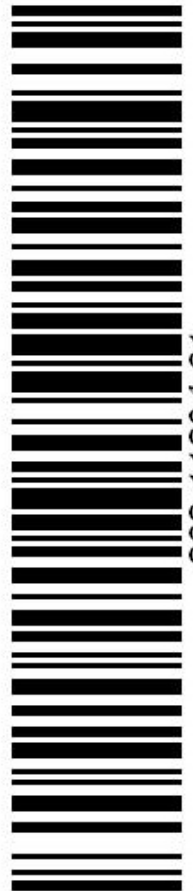
WPS [7](#)

 unsupported [32](#)



Guía del Usuario

Verizon 4G LTE
Broadband Router



202-11294-01