



Verizon Internet Gateway **USER GUIDE**



CONTENTS

01/

INTRODUCTION

1.0	Inside the box	5
1.1	Getting to Know Your Verizon Internet Gateway	5
1.2	Setting Up Your Verizon Internet Gateway	9

02/

CONFIGURING YOUR VERIZON INTERNET GATEWAY

2.0	Configure Your Verizon Internet Gateway	14
2.1	Expanding Wi-Fi Coverage	19
2.2	Computer Network Configuration	20
2.3	Main Screen	27

03/

WI-FI SETTINGS

3.0	Overview	33
3.1	Basic Settings	34
3.2	Advanced Settings	43

04/

CONNECTED DEVICES

4.0	Device Settings	51
4.1	Setting Parental Controls	56
4.2	Universal Plug & Play	60

05/

CONFIGURING ADVANCED SETTINGS

- 5.0 Security & Firewall 67
- 5.1 Network Settings 83
- 5.2 Diagnostics & Monitoring 130
- 5.3 System 136

06/

TROUBLESHOOTING

- 6.0 Troubleshooting Tips 153
- 6.1 Frequently Asked Questions 160

07/

SPECIFICATIONS

- 7.0 General Specifications 167
- 7.1 Connections 168

08/

NOTICES

- 8.0 Regulatory Compliance Notices 171

01/

INTRODUCTION

- 1.0** Inside the box
- 1.1** Getting to Know Your Verizon Internet Gateway
- 1.2** Setting Up Your Verizon Internet Gateway

INSIDE THE BOX

1.0/ INSIDE THE BOX

Inside the product package you should find the following items. Contact Verizon if any item is missing or damaged.

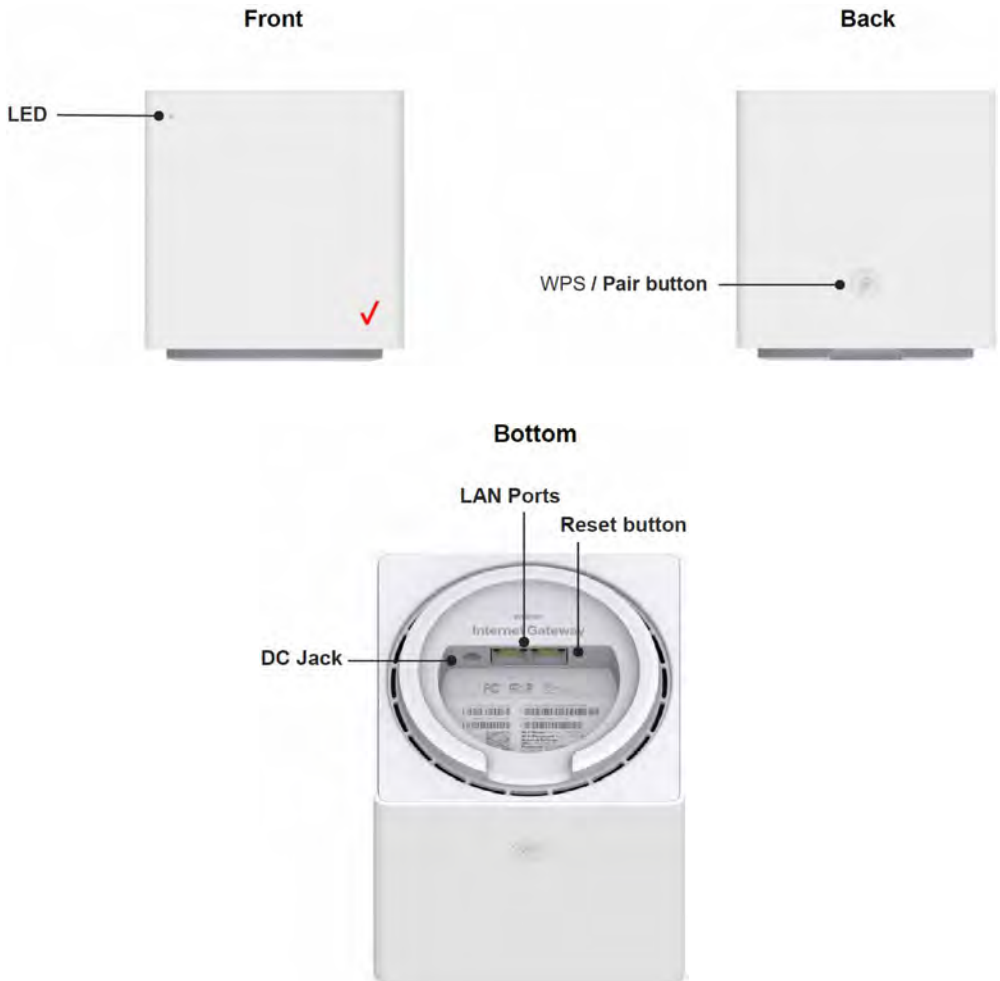
- Verizon Internet Gateway
- Power adapter
- Ethernet Cable



1.1/ GETTING TO KNOW YOUR VERIZON INTERNET GATEWAY

Your Verizon Internet Gateway provides fast dual-band Wi-Fi (with channel steering) for all your devices, and features built-in network security as well as parental controls, guest Wi-Fi and automatic software updates.

Take a moment to familiarize with your product:



GETTING TO KNOW YOUR VERIZON INTERNET GATEWAY

1.1a/ RESET BUTTON

If you experience difficulties with your router or you want to revert all settings that you have changed, the reset function allows you to reset the router back to its factory default state. To perform a factory reset and return the Verizon Internet Gateway to default settings, press and hold the reset button for 3+ seconds. The LED will flash yellow to indicate a reset has been triggered, followed by fading in/out (white) while the router restarts.

1.1b/ WPS

WPS is an easy way to add supported Wi-Fi devices to your network. Press the WPS button on the back of the Gateway to activate WPS. You will need to activate WPS on your Wi-Fi device too. Refer to “3.1d/ Wi-Fi Protected Setup (WPS)” on page 40.

1.1c/ LED

The LED indicates the system and connection status, and WPS activity.

Front LED Mode	Status	LED Pattern
Bootup	System Off	Off
	System Booting	Soft blink White
	Firmware update (FOTA)	Fast blink white

Front LED Mode	Status	LED Pattern
Cellular signal (or after single click pair button)	Passing signal	Solid White
	No Signal, Cold SIM	Solid Red
	No SIM Card	Hard blink red
Regular usage	Setup complete	50% bright White
	Wi-Fi disabled by user	Solid Green
Paring	WPS Paring	Hard blink Blue
Other	Factory Reset	Fast blink yellow
	FW Error	Soft blink red

Ethernet Port LED Mode	Status	Left LED	Right LED
Wired LAN connection * Threshold level can be decided based on port capability	Ethernet > 100M* Link	Off	Solid White
	Ethernet > 100M* Activity	Off	Blinking White
	Ethernet < 100M* Link	Solid Yellow	Off
	Ethernet < 100M* Activity	Blinking Yellow	Off
	No Ethernet connection	Off	Off

SETTING UP YOUR VERIZON INTERNET GATEWAY

1.2/ SETTING UP YOUR VERIZON INTERNET GATEWAY

Your Verizon Internet Gateway comes with a pre-installed SIM card and can be up and running in just a couple of minutes.

1.2a/ POSITIONING YOUR VERIZON INTERNET GATEWAY

For the best wireless signal transmission from the Gateway to your network devices:

- Place the Gateway in a central area near a window.
- Avoid keeping the device in the basement to get better signal.
- Avoid having obstacles near the device, clear any objects near the window that could interfere with getting a signal.
- Keep the Gateway away from metal obstructions and away from direct sunlight.
- Keep the Gateway away from 802.11g or 20MHz only Wi-Fi devices, 2.4GHz computer peripherals, Bluetooth devices, cordless phones, transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators, and other industrial equipment to prevent signal interference or loss.

1.2b/ SETUP REQUIREMENTS

To configure your wireless network via computer, you need a computer that meets the following system requirements:

- For Wired Connection: Ethernet RJ-45 (LAN) port (10Base-T/100Base-TX/1000Base-TX)
- For Wi-Fi Connection: IEEE 802.11a/b/g/n/ac/ax wireless capability
- An installed TCP/IP service
- Web browser such as Microsoft Edge, Firefox, Safari, or Google Chrome

1.2c/ SETTING UP

Before you begin, if you are replacing an existing router, disconnect it. Remove all old router components, including the power supply. They will not work with your new Verizon Internet Gateway.

1. Plug the Verizon Internet Gateway into a power outlet with the included power adapter.
2. Wait for a couple of minutes for the Gateway to power up and establish an LTE/5G connection. The LED should display on (white) after starting up.
3. That's it! You can connect your Internet devices to the Gateway's Wi-Fi networks named Verizon_<your network> (check your router's product label on the bottom side for your unique Wi-Fi network name and password). You can also connect Internet devices to your Gateway by connecting the device's LAN ports with an Ethernet cable.

SETTING UP YOUR VERIZON INTERNET GATEWAY



- Wi-Fi Network

The Verizon Internet Gateway has one Wi-Fi name supporting 2.4 GHz and 5 GHz signals. The Self-Organizing Network (SON) feature lets your devices move between the two signals automatically for an optimized Wi-Fi connection.

4. Go to 2.3/ Main Screen to login to your Gateway and configure settings such as Wi-Fi security.

02 /

CONFIGURING YOUR VERIZON INTERNET GATEWAY

- 2.0** Configure Your
Verizon Internet Gateway
- 2.1** Expanding Wi-Fi Coverage
- 2.2** Computer Network
Configuration
- 2.3** Main Screen

Connecting your Verizon Internet Gateway and accessing its web-based User Interface (UI) are both simple procedures.

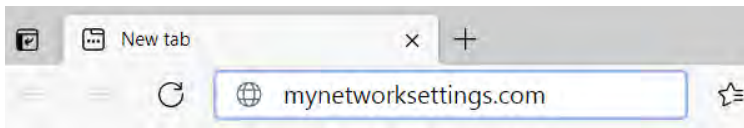
Accessing the UI may vary slightly, depending on your device's operating system and web browser.

CONFIGURE YOUR VERIZON INTERNET GATEWAY

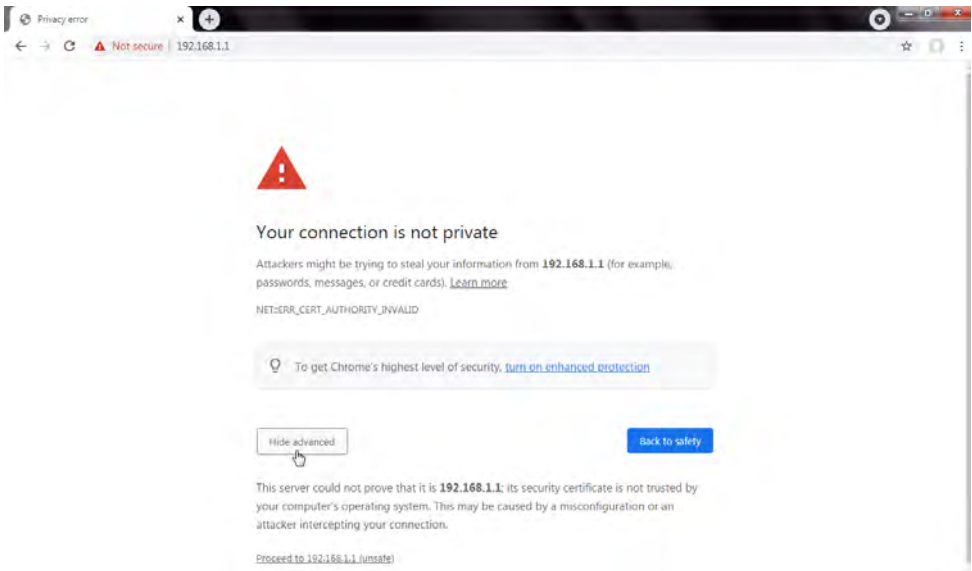
2.0/ CONFIGURE YOUR VERIZON INTERNET GATEWAY

1. Open a web browser on the device connected to your Verizon Internet Gateway network.
2. In the browser address field (URL), enter: mynetworksettings.com, then press the **Enter** key on your keyboard.

Alternately, you can enter: <https://192.168.1.1>



3. You may see a security message warning that **Your connection is not private** when you visit mynetworksettings.com (<https://192.168.1.1>) for GUI management. To get to the login screen, click the **ADVANCED** button, then on **Proceed to 192.168.1.1 (unsafe)** link.

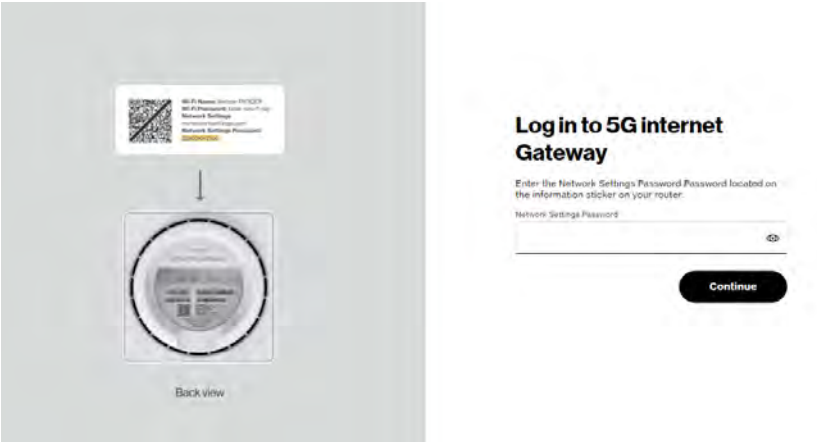


4. The login screen will appear.

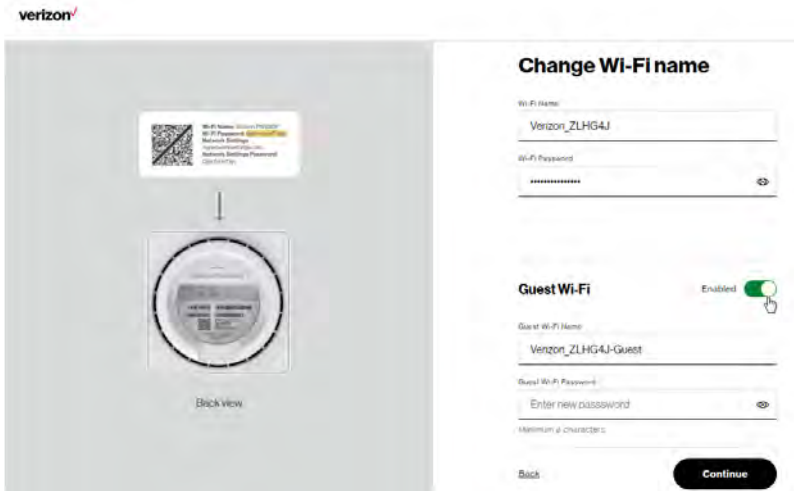
The first time you access your Verizon Internet Gateway, an Easy Setup Wizard displays to help step you through the setup process.

5. On the **Log in to 5G Internet Gateway** screen, enter the password that is printed next to the Password on the label on the bottom of your Gateway.

CONFIGURE YOUR VERIZON INTERNET GATEWAY



6. Click **Continue**. The **Change Wi-Fi name** screen displays. Move the selector to **on** for setting up your **Guest Wi-Fi** to personalize your Guest Wi-Fi Name and Password.



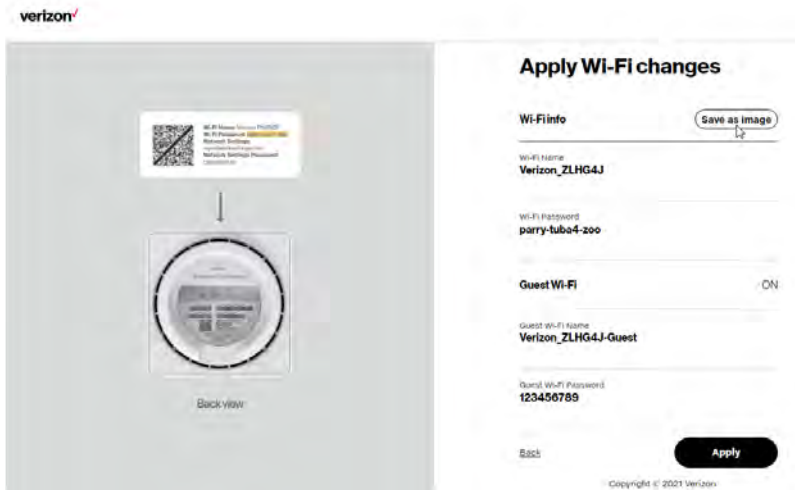
For your protection, your Verizon Internet Gateway is pre-set at the factory to use WPA2 (Wi-Fi Protected Access II) encryption for your Wi-Fi network. This is the best setting for most users and provides security.

7. Click **Continue**. The **Apply Wi-Fi changes** screen appears. You have an option of saving the Wi-Fi settings as an image on your device by clicking the **Save as image** button. After you click **Save as image** to save your Wi-Fi settings as an image, click **Apply** to save the Wi-Fi changes to your Verizon Internet Gateway.

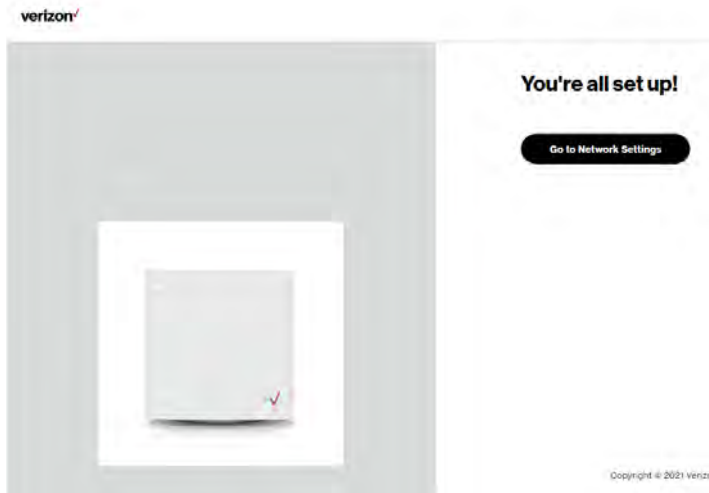
Note: If you select **Save as image**, the image file is saved to your web browser's download folder.

CONFIGURE YOUR VERIZON INTERNET GATEWAY

Important: *If you are on a Wi-Fi device when setting up your Verizon Internet Gateway, you will be disconnected from the Wi-Fi network when you change the Wi-Fi name or Wi-Fi password. When this occurs, your Verizon Internet Gateway will detect this situation and prompt you to reconnect using the new settings.*



The **You're all set up!** screen displays once your Gateway verifies the final settings and has successfully connected to the internet and is ready for use. You can click on **Go to Network Settings** to access the main screen of the Verizon Internet Gateway.



If your Verizon Internet Gateway is subsequently reset to the factory default settings, the settings printed on the label will again be in effect.

If your Verizon Internet Gateway fails to connect, follow the troubleshooting steps in the Troubleshooting section of this guide.

2.1/ EXPANDING WI-FI COVERAGE

Connecting one or more of Verizon's Extenders to the Verizon Internet Gateway allows you to extend Wi-Fi signal range and to eliminate Wi-Fi dead zones on your Wi-Fi network.

COMPUTER NETWORK CONFIGURATION

2.1a/ WI-FI INSTALLATION

1. Place the extender directly next to the Verizon Internet Gateway.
2. Connect the power cord to your extender then to an electrical outlet.
3. When the light on the extender is solid yellow, press and hold the buttons on your Gateway and extender for 2+ seconds until they slowly begin to blink blue.
4. The lights on the Gateway and extender should turn solid blue while the Wi-Fi connection is initiating and solid white when the connection is complete.
5. Once the Wi-Fi connection is complete, you can unplug and move the extender to an area between your Gateway and an area with spotty Wi-Fi coverage. Once plugged in again, the light should turn solid white again within a few minutes.

You're all set! Your devices will connect automatically with the same Wi-Fi network name and password as your Verizon Internet Gateway.

2.2/ COMPUTER NETWORK CONFIGURATION

Each network interface on your computer should either automatically obtain an IP address from the upstream Network DHCP server (default configuration) or be manually configured with a statically defined IP address and DNS address. We recommend leaving this setting as it is.

2.2a/ CONFIGURING DYNAMIC IP ADDRESSING

To configure a computer to use dynamic IP addressing:

WINDOWS 7/8

1. In the Control Panel, locate **Network and Internet**, then select **View Network Status and Tasks**.
2. In the **View your active networks – Connect or disconnect** section, click **Local Area Connection** in the **Connections** field. The Local Area Connection Status window displays.
3. Click **Properties**. The Local Area Connection Properties window displays.
4. Select **Internet Protocol Version 4 (TCP/IPv4)**, then click **Properties**. The Internet Protocol Version 4 (TCP/IPv4) Properties window displays.
5. Click the **Obtain an IP address automatically** radio button.
6. Click the **Obtain DNS server address automatically** radio button, then click **OK**.
7. In the Local Area Connection Properties window, click **OK** to save the settings.
8. To configure Internet Protocol Version 6 (TCP/IPv6) to use dynamic IP addressing, repeat steps 1 to 7. However for step 4, select **Internet Protocol Version 6 (TCP/IPv6)** in the **Properties** option (refer to IPv6 section for Verizon Internet Gateway configuration).

COMPUTER NETWORK CONFIGURATION

WINDOWS 10

1. On the Windows desktop, click on the **Start** icon. Select **Settings** and click **Network & Internet**.
2. In the Network & Internet, click **Ethernet**.
3. Select **Network and Sharing Center**. The **View your basic network information and set up connections** window displays.
4. In the **View your active networks**, click **Ethernet** in the **Connections** field. The **Ethernet Status** window displays.
5. Click **Properties**. The **Ethernet Properties** window displays.
6. Select **Internet Protocol Version 4 (TCP/IPv4)**, then click **Properties**. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window displays.
7. Click the **Obtain an IP address automatically** radio button.
8. Click the **Obtain DNS server address automatically** radio button, then click **OK**.
9. In the **Local Area Connection Properties** window, click **OK** to save the settings.
10. To configure Internet Protocol Version 6 (TCP/IPv6) to use dynamic IP addressing, repeat steps 1 to 9. However for step 6, select **Internet Protocol Version 6 (TCP/IPv6)** in the **Properties** option (refer to IPv6 section for Verizon Internet Gateway configuration).

MACINTOSH OS X

1. Click the **Apple** icon in the top left corner of the desktop. A menu displays.
2. Select **System Preferences**. The System Preferences window displays.
3. Click **Network**.
4. Verify that **Ethernet**, located in the list on the left, is highlighted and displays **Connected**.
5. Click **Assist Me**.
6. Follow the instructions in the Network Diagnostics Assistant.

2.2b/ CONNECTING OTHER COMPUTERS AND NETWORK DEVICES

You can connect your Verizon Internet Gateway to other computers or set top boxes using an Ethernet cable or Wi-Fi connection.

ETHERNET

1. Plug one end of an Ethernet cable into one of the Ethernet ports on the bottom of your Verizon Internet Gateway.
2. Plug the other end of the Ethernet cable into an Ethernet port on the computer.
3. Repeat these steps for each computer to be connected to your Verizon Internet Gateway using Ethernet.

COMPUTER NETWORK CONFIGURATION

CONNECTING A WI-FI DEVICE USING WPS

Wi-Fi Protected Setup (WPS) is an easier way for many devices to set up a secure Wi-Fi network connection. Instead of manually entering passwords or multiple keys on each Wi-Fi client, such as a laptop, printer, or external hard drive, your Verizon Internet Gateway creates a secure Wi-Fi network connection.

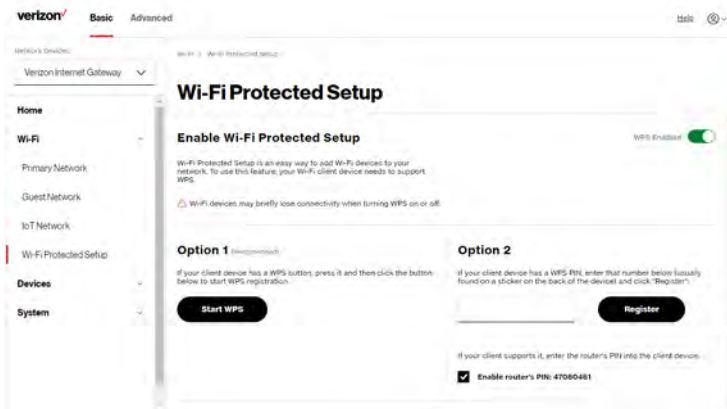
In most cases, this only requires the pressing of two buttons – one on your Verizon Internet Gateway and one on the Wi-Fi client. This could be either a built-in button or one on a compatible Wi-Fi adapter/card, or a virtual button in software. Once completed, this allows Wi-Fi clients to join your Wi-Fi network.

To initialize the WPS process, you can either press and hold the unified button located on the front of your Verizon Internet Gateway for more than two seconds or use the UI and press the on-screen button.

You can easily add Wi-Fi devices to your Wi-Fi network using the WPS option if your Wi-Fi device supports the WPS feature.

To access WPS using the user interface:

1. From the **Basic** menu, select **Wi-Fi** settings, then click **Wi-Fi Protected Setup**.



2. Enable the protected setup by moving the selector to **on**.
3. Use one of the following methods:
 - If your Wi-Fi client device has a WPS button, press the unified button on your Gateway for more than two seconds, then click the **Start WPS** button in the **Option 1** to start the WPS registration process.
 - If your client device has a WPS PIN, locate the PIN printed on the client's label or in the client documentation. Enter the PIN number in the **Option 2** on the user interface.
 - Click **Register**.
 - Alternatively, you can enter the Gateway's PIN shown on this screen into the WPS user interface of your device, if this PIN mode is supported by your Wi-Fi device.
4. After pressing the unified button (WPS) on your Gateway, you have two minutes to press the WPS button on the client device before the WPS session times out.

COMPUTER NETWORK CONFIGURATION

When the unified button (WPS) on your Gateway is pressed, the Status LED on the front of your Gateway begins flashing blue. The flashing continues until WPS pairing to the client device completes successfully. At this time, the Status LED turns solid blue.

If WPS fails to establish a connection to a Wi-Fi client device within two minutes, the Status LED on your Gateway flashes red for two minutes to indicate the WPS pairing process was unsuccessful. After flashing red, the light returns to solid white to indicate that Wi-Fi is on.

***Note:** Wi-Fi Protected Setup (WPS) cannot be used if WPA3 security is enabled or SSID broadcast is disabled or if MAC address authentication is enabled with an empty white list.*

CONNECTING A WI-FI DEVICE USING A PASSWORD

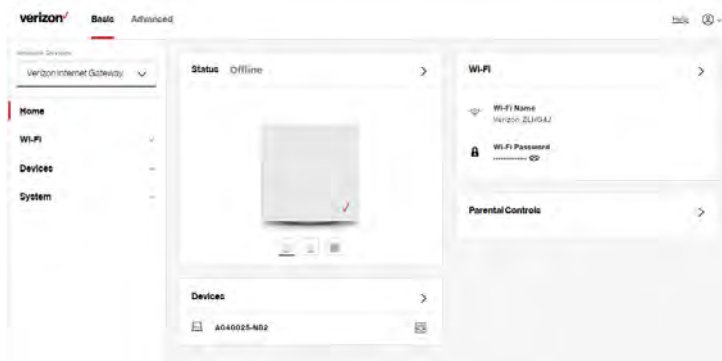
1. Verify each device that you are connecting with Wi-Fi has built-in Wi-Fi or an external Wi-Fi adapter.
2. Open the device's Wi-Fi settings application.
3. Select your Verizon Internet Gateway's Wi-Fi network name (SSID) from the device's list of discovered Wi-Fi networks.
4. When prompted, enter your Verizon Internet Gateway's Wi-Fi password (WPA2 or WPA3 key) into the device's Wi-Fi settings. Your Gateway's default Wi-Fi network name and password are located on the sticker on the bottom of your Verizon Internet Gateway.



5. Verify the changes were implemented by using the device's web browser to access a site on the internet.
6. Repeat these steps for every device that you are connecting with Wi-Fi to your Gateway.

2.3/ MAIN SCREEN

When you log into your Gateway, the dashboard main page displays the navigation menus of Basic and Advanced settings, Wi-Fi settings, Devices, Parental Controls, and connection status, and Basic quick links.



MAIN SCREEN

The configuration options available via the left-hand main menu are described in the following chapters:

- Basic Settings
 - System - this chapter
 - Wi-Fi - Chapter 3
 - Devices - Chapter 4
- Advanced Settings - Chapter 5

2.3a/ SYSTEM

SYSTEM STATUS

To view the status:

1. Access the dashboard **Home** page.
2. You can quickly view your Gateway's status by clicking **System\System Status** on the screen. This section displays the status of your Gateway's local network (LAN) and internet connection (WAN), firmware and hardware version numbers, MAC Address, IP settings of Verizon Internet Gateway and Wi-Fi extender(s) (if connected).

verizon

BasicAdvanced

Help

Network Devices

Verizon Internet Gateway

Home

Wi-Fi

Devices

System

System Status

Open Source Software

System > System Status

System Status

Auto-refresh

Refresh

Broadband IPv4

Status: Disabled

IPv4 address is from: STATIC

IPv4 address:

Current mask:

IPv4 default gateway:

IPv4 DNS Address 1:

IPv4 DNS Address 2:

WiFi Supported Band / Mode: 0 / 30000

Broadband IPv6

Status: Disabled

IPv6 address is from: DHCPv6-PD

Unpaired prefix:

IPv6 address:

Link-local Address:

IPv6 Default Gateway:

IPv6 DNS Address 1:

IPv6 DNS Address 2:

verizon

BasicAdvanced

Help

Network Devices

Verizon Internet Gateway

Home

Wi-Fi

Devices

System

System Status

Open Source Software

System > System Status

System Status

Auto-refresh

Refresh

Modem

Firmware Version: MOLVNR15.R3.MD700.MPV3B.P7.2

Mobile Number:

IMEI: 358998610004393

ICCID: 89148000007717343061

Sim Status: Ready

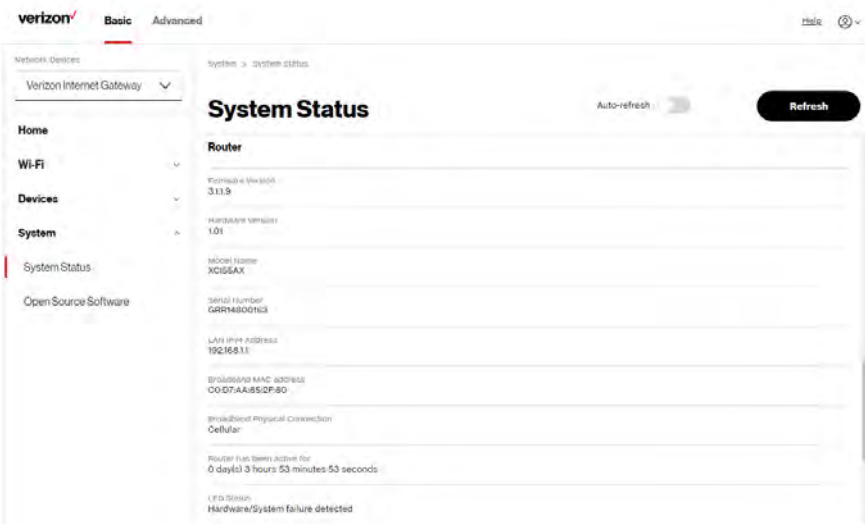
Receiving Status:

4G LTE Signal Strength:

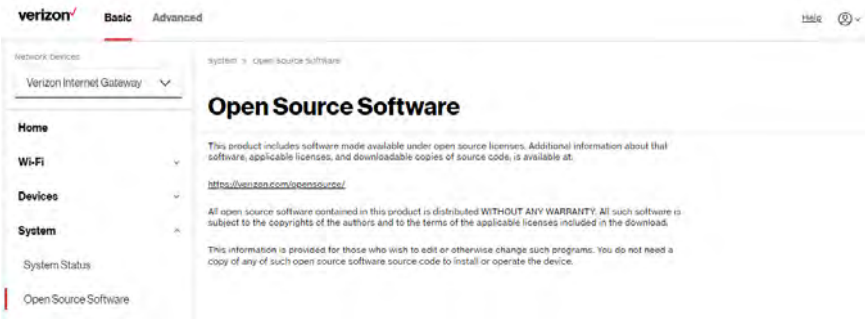
5G Signal Strength:

<http://support.verizon.com/router> | ©2022 Verizon. All Rights Reserved

MAIN SCREEN



OPEN SOURCE SOFTWARE



To view: From the **Basic** menu, select **System** from the left pane and then click **Open Source Software**.

03 /

WI-FI SETTINGS

3.0 Overview

3.1 Basic Settings

3.2 Advanced Settings

Wi-Fi networking enables you to free yourself from wires, making your devices more accessible and easier to use.

You can create a Wi-Fi network, including accessing and configuring Wi-Fi security options.

OVERVIEW

3.0/ OVERVIEW

Your Verizon Internet Gateway provides you with Wi-Fi connectivity using the 802.11a, b, g, n, ac or ax standards. These are the most common Wi-Fi standards.

802.11b has a maximum data rate of 11 Mbps, 802.11a and 802.11g have a maximum data rate of 54 Mbps, 802.11n has a maximum data rate of 450 Mbps, 802.11ac has a maximum data rate of 3.12 Gbps, and 802.11ax has a maximum data rate of 4.8 Gbps.

802.11b and g standards operate in the 2.4 GHz range. 802.11ac operates in the 5 GHz range. 802.11n and ax operate in both the 2.4 GHz and 5 GHz ranges.

***Note:** 802.11a, 802.11b, and 802.11g are legacy modes and are not recommended. Even one such device connected to the network will slow your entire Wi-Fi network.*

The Wi-Fi service and Wi-Fi security are activated by default. The level of security is preset to WPA2 encryption using a unique default WPA2 key (also referred to as a passphrase or password) pre-configured at the factory. This information is displayed on a sticker located on the bottom of your Verizon Internet Gateway.

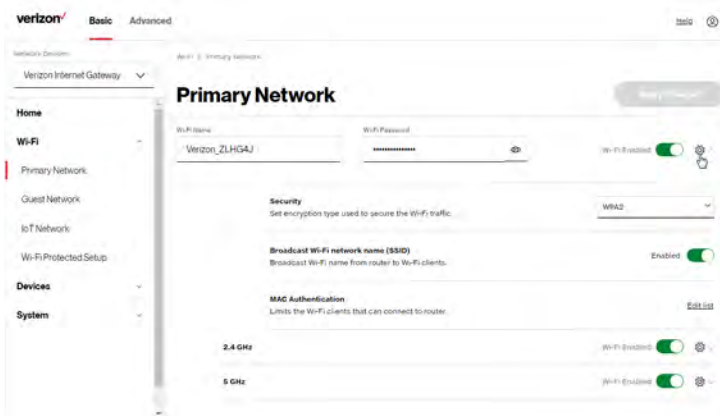
Your Gateway integrates multiple layers of security. These include Wi-Fi Protected Access, and firewall.



3.1/ BASIC SETTINGS

3.1a/ PRIMARY NETWORK

You can configure the basic security settings for either 2.4 GHz or 5 GHz of your Wi-Fi network.



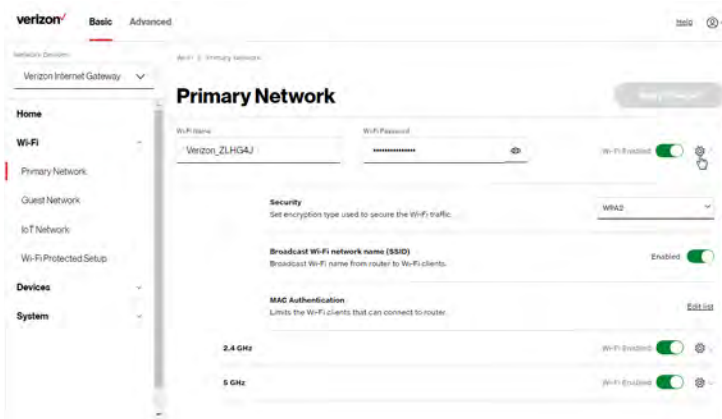
To configure the basic security radio, SSID and security settings:

1. From the **Basic** menu, select **Wi-Fi** from the left pane and then click **Primary Network**.
2. To activate the Wi-Fi radio, move the selector to **on**. If the radio is not enabled, no Wi-Fi devices will be able to connect to the home network.
3. If desired, enter a new name and password for the Wi-Fi network or leave the default name and password that displays automatically.

Note: The SSID is the network name. All devices must use the same SSID.

BASIC SETTINGS

4. To configure the Wi-Fi **Security**, click the setup ⚙ button and select **WPA2** or **WPA3**.



Caution: These settings should only be configured by experienced network technicians. Changing the settings could adversely affect the operation of your Gateway and your local network.

- **Broadcast Wi-Fi network name (SSID)**

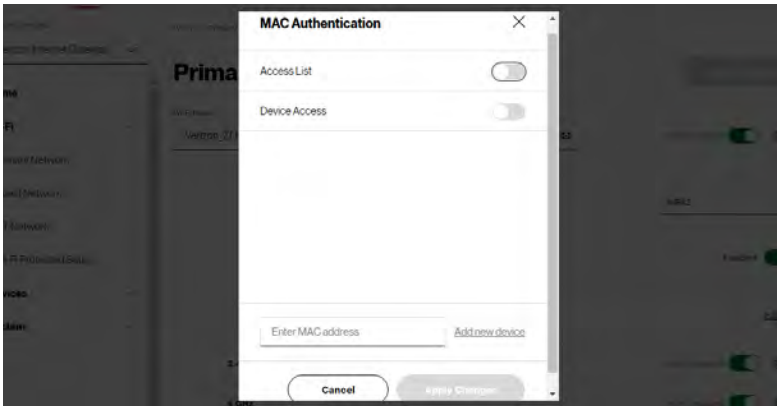
You can configure the Verizon Internet Gateway's SSID broadcast capabilities to allow or disallow Wi-Fi devices from automatically using a broadcast SSID name to detect your gateway Wi-Fi network.

- To enable SSID broadcasting, move the selector to **on**. SSID broadcast is enabled by default. The SSID of the Wi-Fi network will be broadcast to all Wi-Fi devices.

- To disable SSID broadcasting, move the selector to **off**. The public SSID broadcast will be hidden from all Wi-Fi devices. You will need to manually configure additional Wi-Fi devices to join the Wi-Fi network.

- **MAC Authentication**

You can configure your Gateway to limit access to your Wi-Fi network to only those devices with specific MAC addresses.



To set Wi-Fi MAC authentication:

1. To setup access control, click on the **Edit List**.
2. Select either:
 - **Access List** – allows the listed devices to access the Wi-Fi network.

Warning: *This will block Wi-Fi network access for all devices not in the list. Only devices in the list will be able to connect to the Wi-Fi network.*

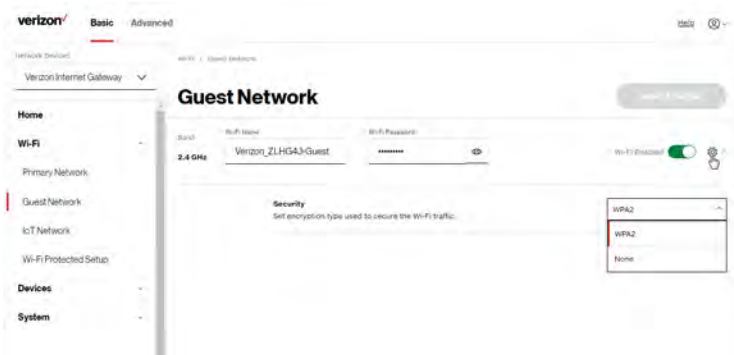
BASIC SETTINGS

- **Device Access** – Wi-Fi devices will be able to access the Wi-Fi network if they use the correct Wi-Fi password.
3. Enter the MAC address of a device and click **Add new device**.
 4. Repeat step 2 and step 3 to add additional devices, as needed.
 5. When all changes are complete, click **Apply Changes** to save the changes.

3.1b/ GUEST NETWORK

The **Guest Network** is designed to provide internet connectivity to your guests but restricts access to your primary network and shared files. The primary network and the guest network are separated from each other through firewalls. You create one Guest Wi-Fi SSID and one password, and use it for all guests. The guest network SSID does not change when you make a change to your primary network SSID.

The Verizon Internet Gateway is shipped from the factory with Guest Wi-Fi turned off. The default SSID for Guest Wi-Fi is preconfigured at the factory to the default Wi-Fi network name (SSID) which is displayed on a sticker located on the bottom of the Gateway followed by hyphen guest (-Guest). For example – if the Gateway is shipped with a default SSID of “Verizon-ABCDE” then the default SSID for Guest Wi-Fi is “Verizon-ABCDE-Guest”.



To configure the security settings for your guest network:

1. From the **Basic** menu, select **Wi-Fi** and then click **Guest Network**.
2. Move the selector to **on**.
3. If desired, enter a new name and password for the Wi-Fi network or leave the default name and password that displays automatically.
4. Press **Apply Changes** to save the changes.

Important: *It is not recommended to create a guest network without a password.*

BASIC SETTINGS

3.1c/ IOT NETWORK

The Gateway supports connection of multiple IoT devices on a separate Wi-Fi SSID. The IoT Network is designed to provide an easier setup experience for your Internet of Things (IoT) devices which benefit from connecting to the 2.4 GHz band while keeping your Primary Network settings unchanged. IoT devices and Primary devices can communicate with no firewall restrictions separating them.

The Verizon Internet Gateway is shipped from the factory with IoT Wi-Fi turned off. The default SSID for IoT Wi-Fi is preconfigured at the factory to the default Wi-Fi network name (SSID) which is displayed on a sticker located on the bottom of the Gateway followed by hyphen IoT (-IoT). For example – if the Gateway is shipped with a default SSID of “Verizon-ABCDE” then the default SSID for IoT Wi-Fi is “Verizon-ABCDE-IoT”.



To enable IoT Wi-Fi link:

1. From the **Basic** menu, select **Wi-Fi** and then click **IoT Network**.
2. Move the selector to **on**.
3. If desired, enter a new name and password for the Wi-Fi network or leave the default name and password that displays automatically.
4. Press **Apply Changes** to save the changes.

3.1d/ WI-FI PROTECTED SETUP (WPS)

Wi-Fi Protected Setup (WPS) is an easier way for many devices to set up a secure Wi-Fi network connection. Instead of manually entering passwords or multiple keys on each Wi-Fi client, such as a laptop, printer, or external hard drive, your Verizon Internet Gateway creates a secure Wi-Fi network connection.

In most cases, this only requires the pressing of two buttons – one on your Verizon Internet Gateway and one on the Wi-Fi client. This could be either a built-in button or one on a compatible Wi-Fi adapter/card, or a virtual button in software. Once completed, this allows Wi-Fi clients to join your Wi-Fi network.

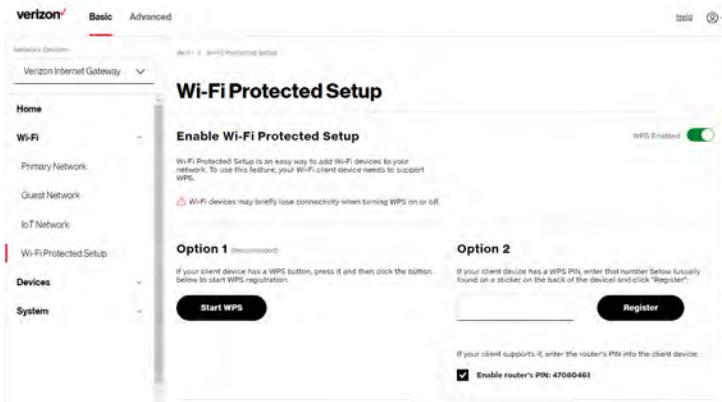
To initialize the WPS process, you can either press and hold the unified button located on the rear of your Verizon Internet Gateway for more than two seconds or use the UI and press the on-screen button.

BASIC SETTINGS

You can easily add Wi-Fi devices to your Wi-Fi network using the WPS option if your Wi-Fi device supports the WPS feature.

To access WPS using the user interface:

1. From the **Basic** menu, select **Wi-Fi** and then click **Wi-Fi Protected Setup (WPS)**.



2. Enable the protected setup by moving the selector to **on**.
3. Use one of the following methods:
 - If your Wi-Fi client device has a WPS button, press the WPS button on your Gateway for more than two seconds, then click the **start WPS** button in the **Option 1** to start the WPS registration process.
 - If your client device has a WPS PIN, locate the PIN printed on the client's label or in the client documentation. Enter the PIN number in the **Option 2** on the user interface.
 - Click **Register**.

- Alternatively, you can enter the Gateway's PIN shown on this screen into the WPS user interface of your device, if this PIN mode is supported by your Wi-Fi device.

4. After pressing the WPS button on your Gateway, you have two minutes to press the WPS button on the client device before the WPS session times out.

When the WPS button on your Gateway is pressed, the Status LED on the front of your Gateway begins flashing blue. The flashing continues until WPS pairing to the client device completes successfully. At this time, the Status LED turns solid blue.

If WPS fails to establish a connection to a Wi-Fi client device within two minutes, the Status LED on your Gateway flashes red for two minutes to indicate the WPS pairing process was unsuccessful. After flashing red, the light returns to solid white to indicate that Wi-Fi is on.

Note: *Wi-Fi Protected Setup (WPS) cannot be used if WPA3 security is enabled or SSID broadcast is disabled or if MAC address authentication is enabled with an empty white list.*

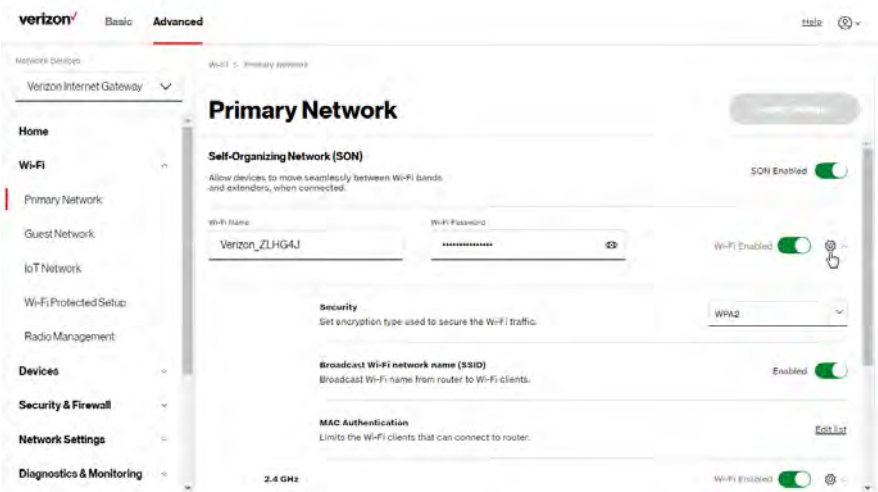
ADVANCED SETTINGS

3.2/ ADVANCED SETTINGS

3.2a/ PRIMARY NETWORK

Self-Organizing Network (SON)

The Verizon Internet Gateway supports 2.4 GHz and 5 GHz signals. The Self-Organizing Network (SON) feature lets your devices move between the two signals automatically for an optimized Wi-Fi connection.



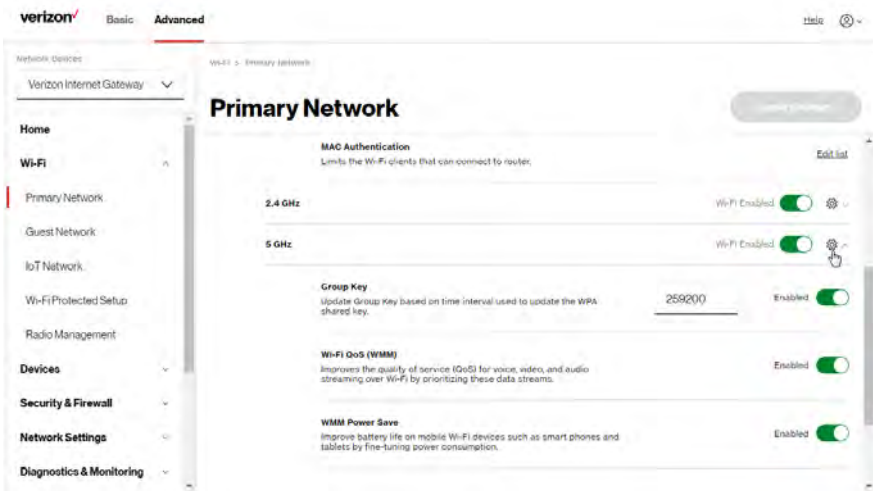
To configure SON, Wi-Fi radio, SSID and security settings:

1. From the **Advanced** menu, select **Wi-Fi** from the left pane and then click **Primary Network**.
2. To enable SON, move the selector to **on**.

3. To activate the Wi-Fi radio, move the selector to **on**. If the radio is not enabled, no Wi-Fi devices will be able to connect to the primary network.
4. If desired, enter a new name and password for the Wi-Fi network or leave the default name and password that displays automatically.

Note: The SSID is the network name. All devices must use the same SSID.

5. To configure the Wi-Fi security, click the setup ⚙ button.



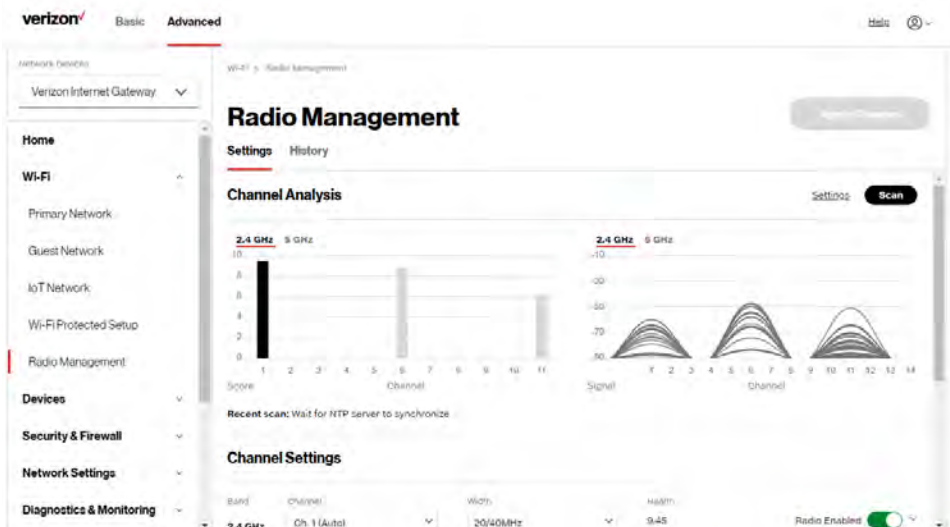
Caution: These settings should only be configured by experienced network technicians. Changing the settings could adversely affect the operation of your Gateway and your local network.

ADVANCED SETTINGS

- **Group key** - to update the WPA shared key, move the selector to on.
- **Wi-Fi QoS (WMM)** - improves the quality of service (QoS) for voice, video, and audio streaming over Wi-Fi by prioritizing these data streams.
- **WMM Power Save** - improves battery life on mobile Wi-Fi devices such as smart phones and tablets by fine-tuning power consumption.

3.2b/ RADIO MANAGEMENT

You can configure the channel settings for the 2.4 GHz and 5 GHz band(s) of your Wi-Fi network.



To view and configure the channel settings:

1. From the **Advanced** menu, select **Wi-Fi** and then click **Radio Management**.
2. Click on **Settings** on the top right-hand side of the **Radio Management** page to configure the channel scan settings:



- Select the **Keep my channel selection during power cycle** check box to save your channel selection when your Verizon Internet Gateway is rebooted.
- **Enable DFS channels during channel scan:** DFS channels are enabled by default during channel scans.

***Note:** DFS channels are a subset of the 5 GHz network that is shared with radar systems. Some consumer devices do not support these channels and cannot connect to gateways using them. Examples include some media streaming devices. Disabling this feature will allow the Gateway to select the best available channel to broadcast on and allow these devices to connect.*

- Press **Apply Changes** to save the changes.

ADVANCED SETTINGS

3. Click **Scan** to perform channel availability scan for the Verizon Internet Gateway accommodating the best radio channel and providing the best Wi-Fi performance.
4. On the **Channel Settings** page for either 2.4 GHz or 5 GHz, the following information displays and can be configured:
 - **Channel Analysis** - scans and displays channel bandwidth and signal strength of available APs. **Channel Score** displays a network congestion score of one to ten in each Wi-Fi channel. It can be used to determine which channels to use or to avoid. Higher score indicates less congestion in a channel.
 - **Channel Settings** - this is the radio channel used by the Wi-Fi router and its clients to communicate with each other. The channel must be the same on the Gateway and all of its Wi-Fi clients. Select the channel you want the Wi-Fi radio to use to communicate, or accept the default (**Auto**) channel selection. Then the Gateway will automatically assign itself a radio channel.
 - **Width** - displays the Wi-Fi channel currently in use on each band. Users can select from available channels.
 - **802.11 Mode**

You can limit the Wi-Fi access to your network by selecting the 2.4 GHz and 5 GHz Wi-Fi communication standard best suited for the devices you allow to access your Wi-Fi network.

Select the Wi-Fi mode as follows:

- **Compatibility** – This is the default mode setting on 5 GHz, providing a good balance of performance and

interoperability with existing Wi-Fi devices. 802.11a,n,ac and ax devices can connect.

- **Legacy** – This is the default mode setting on 2.4 GHz, providing broad connection support for old and new Wi-Fi devices. 802.11a,b,g,n and ac devices can connect.

Notes:

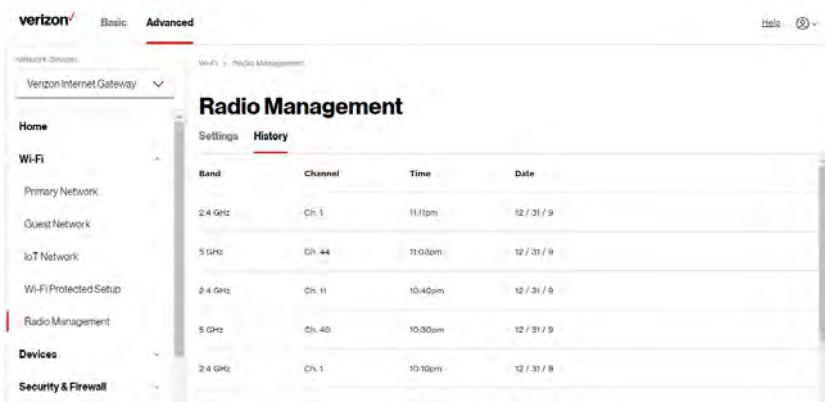
802.11n is available on both 2.4 GHz and 5 GHz frequencies.

Connecting 802.11a, b or g devices will cause your Wi-Fi network to slow on that radio and is not recommended.

- **Transmit Power** – adjusts the power of the Wi-Fi signal.

To view the channel settings history:

1. From the **Advanced** menu, select **Wi-Fi** and then click **Radio Management**.
2. Click on **History** to display the channel settings history.



04 /

CONNECTED DEVICES

- 4.0** Device Settings
- 4.1** Setting Parental Controls
- 4.2** Universal Plug & Play

You can view the settings of the network devices connected to your Verizon Internet Gateway's network.

The abundance of harmful information on the internet poses a serious challenge for employers and parents alike as they ask “How can I regulate what my employee or child does on the internet?”

With that question in mind, your Verizon Internet Gateway's Parental Controls were designed to allow control of internet access on all locally networked devices.

DEVICE SETTINGS

4.0/ DEVICE SETTINGS

To view and manage the connected devices on your network:

1. From the **Basic** menu, select **Devices** from the left pane.
2. The screen displays information about connected devices including **Device Name** and identifiers, **Parental Controls**, the type of network connection, and settings that you can view and configure.



3. To easily add a new device to the network:
 - i. Click **Add Device** button on the screen.
 - ii. Select the preferred **Network Type** from the dropdown list (**Primary**, **Guest** or **IoT**).
 - iii. Scan the provided QR code with the new device's camera.
 - iv. Tap the push notification to connect the device to your network.



v. You can add the new device to your Wi-Fi network using the WPS option if your Wi-Fi device supports the WPS feature. Refer to “3.1d/ Wi-Fi Protected Setup (WPS)” on page 40 for detailed information.

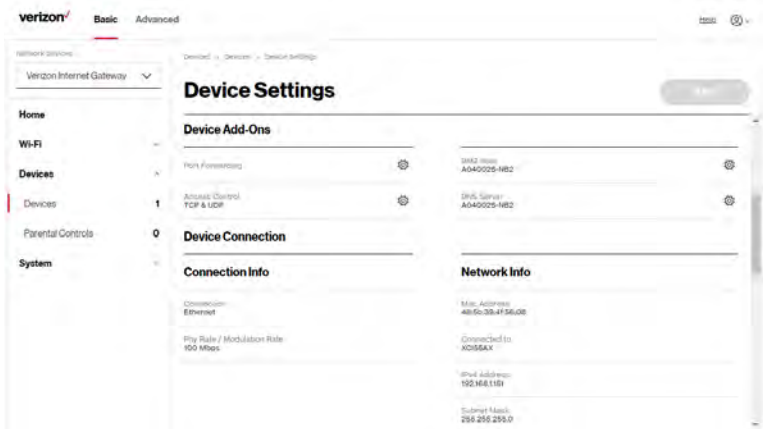
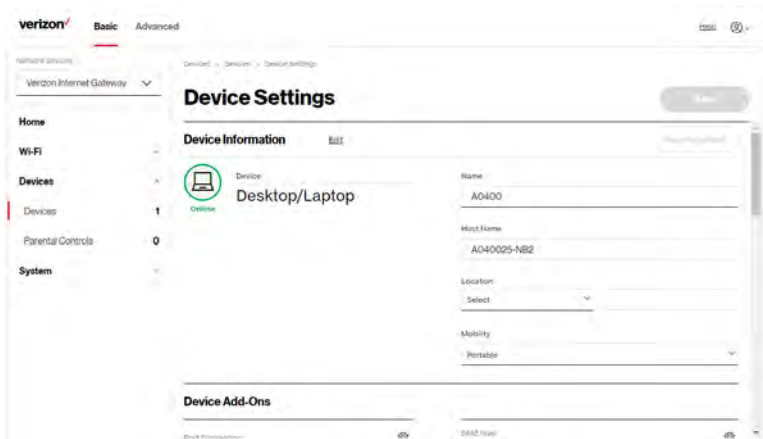
vi. Click **Done** to save the changes.

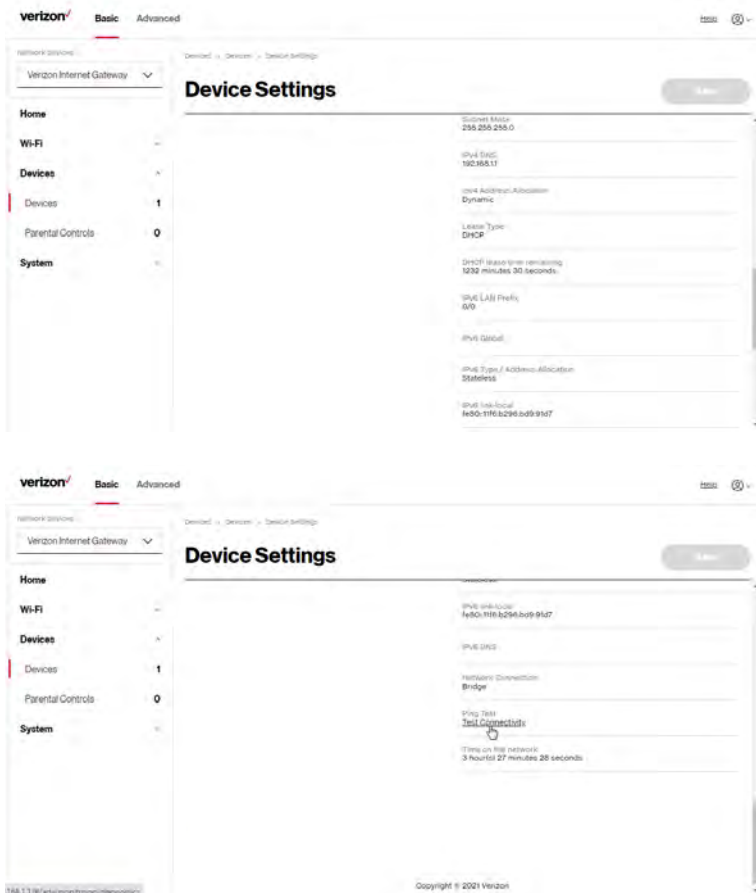
4. Click the **Block/Allow** option to quickly disable/enable a device from having internet access.

For additional information about blocking websites, refer to “Setting Parental Controls” on page 56.

5. Click the Settings icon to access the **Device Settings** page for that device:

DEVICE SETTINGS





– Device Information:

- **Device Type, Name/Host Name, Location, and Mobility** - Displays the current known information of the device. These can be updated or corrected as needed. Click **Edit** and **Save** to apply any changes.

DEVICE SETTINGS

- This section also provides the device MAC Address, Access Point information the device is connected to as well as the IPv4 Address of the device.

– Device Add-Ons

Port Forwarding - Port Forwarding allows your network to be exposed to the internet in specific limited and controlled ways. For example, you could allow specific applications, such as gaming, voice, and chat, to access servers in the local network. To access the Port Forwarding page, click the setup button.

For additional information, refer to the Port Forwarding section in Chapter 5 Configuring Advanced Settings.

Access Control - Access Control restricts access from the local network to the internet. To access the Access Control page, click the setup button.

For additional information, refer to the Access Control section in Chapter 5 Configuring Advanced Settings.

DMZ host - DMZ host allows a single device on your primary network to be fully exposed to the internet for special purposes such as internet gaming. To access the DMZ host page, click the setup button.

For additional information, refer to the section in Chapter 5 Configuring Advanced Settings.

DNS Server - DNS Server manages the DNS server host name and IP address. To access the DNS Server page, click the setup button.

For additional information, refer to the section in Chapter 5 Configuring Advanced Settings.

– Device Connection

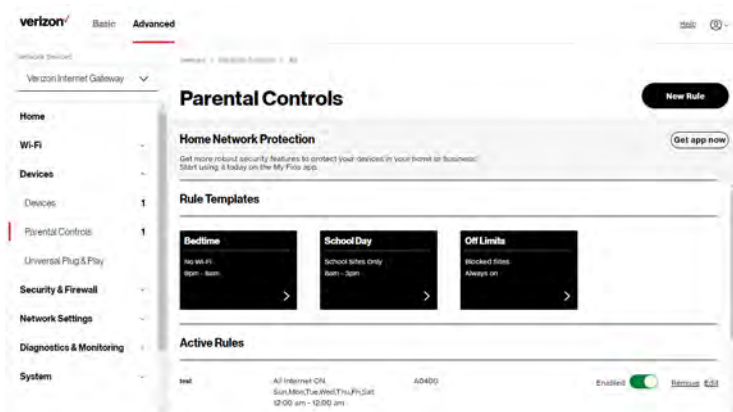
This section displays Connection information of how and how well the device is connected to the Access Point. It also displays the Network related information, including IPv6 addresses and a **Ping Test** option.

4.1/ SETTING PARENTAL CONTROLS

4.1a/ ACTIVATING PARENTAL CONTROLS

You can create a basic access policy or using the provided **Rule Templates** for any computer or device on your Verizon Internet Gateway network. Parental controls limit internet access to specific websites based on a schedule that you create.

Access can be limited on specific websites or keywords embedded in a website. For example, you can block access to the 'www.anysite.com' as well as block any website that has the word 'any' in its site name.



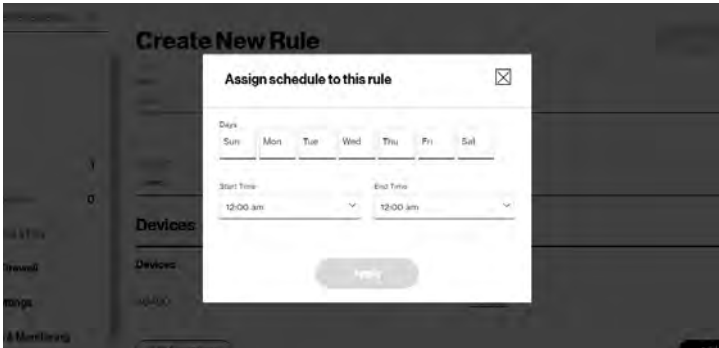
SETTING PARENTAL CONTROLS

To limit device access:

1. From the **Basic** menu, select **Devices** from the left pane and then click **Parental Controls**.
2. To use the default **Rule Templates**, select one of the pre-defined rules as shown on screen to quickly setup access policy for devices on your network.
3. To create a new access policy, click on the **New Rule** and the configuration page displays.

The screenshot shows the Verizon FiOS Router web interface. On the left is a navigation menu with options: Home, Wi-Fi, Devices (selected), Parental Controls, Universal Plug & Play, Security & Firewall, and Network Settings. Under 'Devices', there are counts for 'Devices' (2) and 'Parental Controls' (0). The 'Parental Controls' section is highlighted. The main content area is titled 'Create New Rule'. It has a 'Name' field with 'test' entered. The 'Schedule' dropdown is set to 'Always'. The 'Condition' dropdown is open, showing options: 'Select', 'Internet is always off', and 'Internet is always on'. The 'Devices' dropdown is set to 'User defined'. There is an 'Add Exceptions' button at the bottom left and an 'Add Devices' button at the bottom right. The top of the interface shows 'verizon' logo, 'Basic' and 'Advanced' tabs, and a 'title' field.

4. Create a rule name.
5. Create a **Schedule** by selecting **User defined** from the dropdown list.

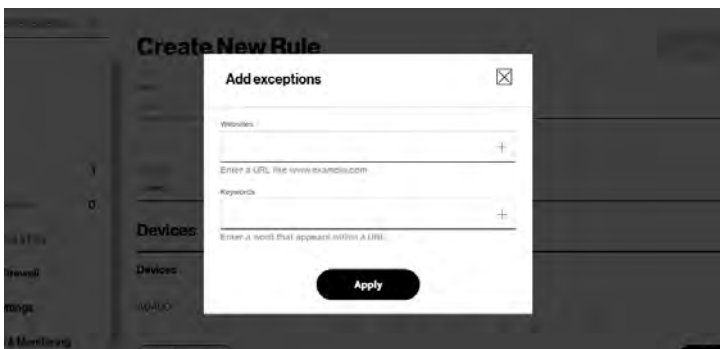


6. Select the days of the week when the rule will be active or inactive.
7. Set the time when the rule will be active or inactive, then specify the start time and end time.
8. Click **Apply** to save changes.
9. Select the **Condition** rule of **Internet is always off/Internet is always on** to block/allow the access to all internet websites.
10. Create the **Devices** rule by selecting **User defined** from the dropdown list and select the computers or clicking **Add Devices** to add a device where you are limiting access.

SETTING PARENTAL CONTROLS



11. Click **Apply** to save changes.
12. To remove a device from the list, click **Remove** to the assigned device.
13. Click **Add Exceptions** for the following exception options:
 - Enter the name of the website or keywords within a URL to block/allow the specified websites and websites with names containing the specified keyword.

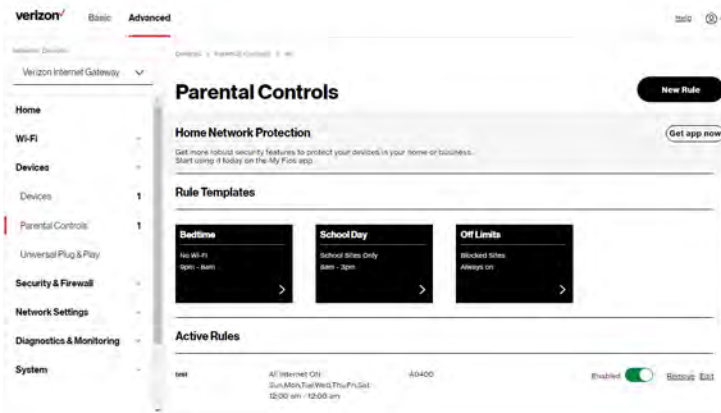


14. Click **Apply** to save changes.

NEW! The Verizon app provides robust security to protect your home and business networks. Click the **Get app now** link to download the app for using Verizon app on the iOS or Android OS.

4.1b/ ACTIVE RULES

You can view the rules created for your Verizon Internet Gateway shown on the **Parental Controls** page.



4.2/ UNIVERSAL PLUG & PLAY

You can use Universal Plug and Play (UPnP) to support new devices without configuring or rebooting your Verizon Internet Gateway.

In addition, you can enable the automatic cleanup of invalid rules. When enabled, this functionality verifies the validity of all UPnP

UNIVERSAL PLUG & PLAY

services and rules every five minutes. Old and unused UPnP defined services are removed, unless a user-defined rule depends on it.

UPnP services are not deleted when disconnecting a computer without proper shutdown of the UPnP applications, such as messenger. Services may often not be deleted and eventually this leads to the exhaustion of rules and services. No new services can be defined. The cleanup feature locates the invalid services and removes them, preventing services exhaustion.

To access this setting:

1. From the **Advanced** menu, select **Devices** from the left pane and then click **Universal Plug & Play**.



2. To enable UPnP and allow UPnP services to be defined on any network hosts, select the **UPnP Enabled** check box.
3. To enable automatic cleanup of invalid rules, select **Enable Automatic Cleanup of Old Unused UPnP Services** check box.
4. Click **Apply changes** to save changes.

05 /

CONFIGURING ADVANCED SETTINGS

- 5.0** Security & Firewall
- 5.1** Network Settings
- 5.2** Diagnostics & Monitoring
- 5.3** System

Advanced settings cover a wide range of sophisticated configurations for your Verizon Internet Gateway's firmware, security setup and network.

Verizon Internet Gateway's security suite includes comprehensive and robust security services, such as stateful packet inspection, firewall security, user authentication protocols, and password protection mechanisms.

These and other features help protect your computers from security threats on the internet.

This chapter covers the following advanced features:

Security & Firewall

- General Firewall - select the security level for the firewall.
- Access Control - restrict access from the local network to the internet.
- DMZ Host - allows a single device on your primary network to be fully exposed to the internet for special purposes such as internet gaming.
- IPv6 Pinholes - provide access tunnel to a service on a host for a particular application.
- Port Forwarding - enable access from the internet to specified services provided by computers on the local network.
- Port Forwarding Rules – displays port forwarding rules.
- Port Triggering - define port triggering entries to dynamically open the firewall for some protocols or ports.
- Scheduler Rules Settings – limits the activation of firewall rules to specific time periods.
- SIP ALG - supports the Application Layer Gateway for Session Initiation Protocol.

Network Settings

- ARP Table – displays active devices with their IP and MAC addresses.
- DNS Server - manages the DNS server host name and IP address.
- Dynamic DNS - allows a static domain name to be mapped to the dynamic IP address.
- IPv4/IPv6 Address Distribution - adds computers configured as DHCP clients to the network.
- IPv6 – enables IPv6 support.
- MAC Cloning – clones the MAC address.
- NDP (Neighbor Discovery Protocol) Table – displays active devices with their IPv6 and MAC addresses of DHCP connection.
- Network Connections – displays and manages the details of a specific network connection.
- Network Objects – defines a group, such as a group of computers.
- Port Configuration – sets up the Ethernet ports as either full- or half-duplex ports, at either 10 Mbps, 100 Mbps, or 1000 Mbps.
- Routing – manages the routing and IP address distribution rules.
- Static NAT - allow multiple static NAT IP addresses to be designated to devices on the network.

Diagnostics & Monitoring - performs diagnostic tests and displays the details and status of:

- Bandwidth Monitoring
- System Logging
- Full Status/System wide Monitoring of Connections/Traffic Monitoring
- Backhaul Logging

Advanced System Settings

- Date & Time Settings – sets the time zone and enables automatic time updates.
- Factory Reset – resets your Verizon Internet Gateway to its default settings.
- LED Brightness - controls the Status LED light to either dim or brighten.
- Reboot Router – restarts your Verizon Internet Gateway.
- Remote Administration – enable remote configuration of your Verizon Internet Gateway from any internet-accessible computer.
- System Settings - sets up various system and management parameters.

5.0/ SECURITY & FIREWALL

The firewall is the cornerstone of the security suite for your Verizon Internet Gateway. It has been exclusively tailored to the needs of the residential or office user and is pre-configured to provide optimum security.

The firewall provides both the security and flexibility that home and office users seek. It provides a managed, professional level of network security while enabling the safe use of interactive applications, such as internet gaming and video conferencing.

Additional features, including surfing restrictions and access control, can also be configured locally through the user interface or remotely by a service provider.

The firewall regulates the flow of data between the local network and the internet. Both incoming and outgoing data are inspected, then either accepted and allowed to pass through your Verizon Internet Gateway or rejected and barred from passing through your Verizon Internet Gateway, according to a flexible and configurable set of rules. These rules are designed to prevent unwanted intrusions from the outside, while allowing local network users access to internet services.

The firewall rules specify the type of services on the internet that are accessible from the local network and types of services in the local network that are accessible from the internet.

SECURITY & FIREWALL

Each request for a service that the firewall receives is checked against the firewall rules to determine whether the request should be allowed to pass through the firewall. If the request is permitted to pass, all subsequent data associated with this request or session is also allowed to pass, regardless of its direction.

For example, when accessing a website on the internet, a request is sent to the internet for this site. When the request reaches your Verizon Internet Gateway, the firewall identifies the request type and origin, such as HTTP and a specific computer in the local network. Unless your Verizon Internet Gateway is configured to block requests of this type from this computer, the firewall allows this type of request to pass to the internet.

When the website is returned from the web server, the firewall associates the website with this session and allows it to pass; regardless HTTP access from the internet to the local network is blocked or permitted. It is the origin of the request, not subsequent responses to this request, which determines whether a session can be established.

5.0a/ SETTING FIREWALL CONFIGURATION

You can select a normal, high, or low security level to limit, block, or permit all traffic. The following table shows request access for each security level.

Security Level	Internet Requests Incoming Traffic	Local Network Requests Outgoing Traffic
High	Blocked	Limited
Normal	Blocked	Unrestricted
Low	Unrestricted	Unrestricted

The request access is defined as:

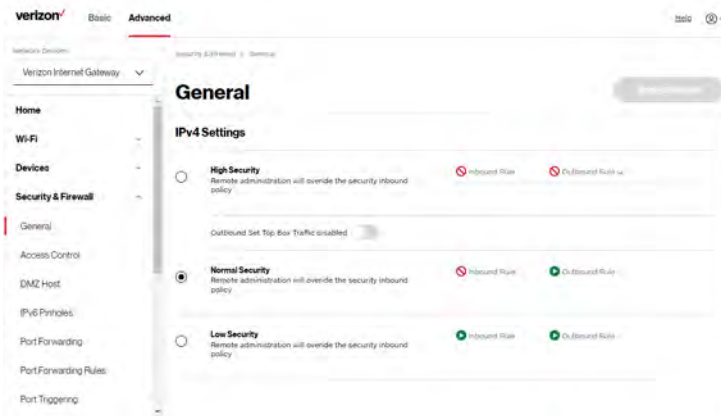
- Blocked traffic - no access allowed, except as configured in Port Forwarding and Remote Access
- Limited - permits only commonly used services, such as email and web browsing
- Unrestricted - permits full access of incoming traffic from the internet and allows all outgoing traffic, except as configured in Access Control

SPECIFYING GENERAL SETTINGS FOR IPV4 OR IPV6

To set your firewall configuration:

1. From the **Security & Firewall General** settings page, click on desired **IPv4 settings/IPv6 settings** option to configure IPv4/IPv6 security.

SECURITY & FIREWALL



2. Select a security level by clicking one of the radio buttons. Using the **Low Security** setting may expose the local network to significant security risks, and should only be used for short periods of time to allow temporary network access.
3. Click **Apply Changes** to save changes.

5.0b/ ACCESS CONTROL

You can block individual computers on your local network from accessing specific services on the internet. For example, you could block one computer from accessing the internet, then block a second computer from transferring files using FTP as well as prohibit the computer from receiving incoming email.

Access control incorporates a list of preset services, such as applications and common port settings.

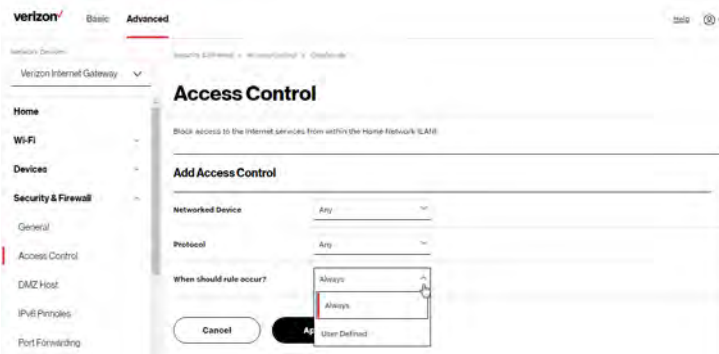
ALLOW OR RESTRICT SERVICES

To allow or restrict services:

1. From the **Advanced** menu, select **Security & Firewall** from the left pane and then click **Access Control**. The **Access Control** page opens with the allowed and blocked status displayed. The allowed section only displays when the firewall is set to maximum security.



2. To block a service, click **Add**. The **Add Access Control** page displays.



SECURITY & FIREWALL

3. To apply the rule to:
 - Networked Computer/Device - select **Any**.
 - Specific devices only - select **User Defined**.
4. In the **Protocol** field, select the internet protocol to be allowed or blocked. If the service is not included in the list, select **User Defined**. The **Edit Service** page displays. Define the service, then click **Apply**. The service is automatically added to the **Add Access Control** section.
5. Specify when the rule is active as **Always** or **User Defined**.

The screenshot shows the Verizon Internet Gateway interface. On the left is a navigation menu with options: Home, Wi-Fi, Devices, Security & Firewall (selected), General, Access Control (highlighted), DMZ Host, IPv6 Pinholes, Port Forwarding, Port Forwarding Rules, and Port Triggering. The main content area is titled 'Access Control' and contains a sub-section 'Set Rule Schedule'. Below this, there is a 'Rule name:' field, a 'Rule days:' row with buttons for Sun, Mon, Tue, Wed, Thu, Fri, and Sat, and a 'Rule time:' section with 'Start Time' (9:00 p.m.) and 'End Time' (12:00 a.m.) dropdowns. Two radio buttons are present: 'Rule will be active during scheduled time' (which is selected) and 'Rule will be inactive during scheduled time'. At the bottom of the form are 'Cancel' and 'Apply' buttons.

6. Enter the rule name, specify days of the week, and set the start time and end time when the rule will be active or inactive.
7. Click **Apply** to save changes.
8. The **Access Control** page displays a summary of the new access control rule.

DISABLE ACCESS CONTROL

You can disable an access control and enable access to the service without removing the service from the Access Control table. This can make the service available temporarily and allow you to easily reinstate the restriction later.

- To disable an access control, clear the check box next to the service name.
- To reinstate the restriction, select the check box next to the service name.
- To remove an access restriction, select the service and click **Remove**. The service is removed from the Access Control table.

5.0c/ DMZ HOST

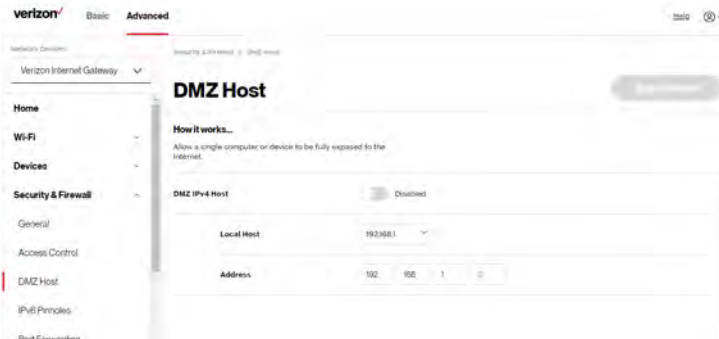
DMZ Host allows a single device on your primary network to be fully exposed to the internet for special purposes like internet gaming.

***Warning:** Enabling DMZ Host is a security risk. When a device on your network is a DMZ Host, it is directly exposed to the internet and loses much of the protection of the firewall. If it is compromised, it can also be used to attack other devices on your primary network.*

SECURITY & FIREWALL

Follow these steps to designate a device on your primary network as a DMZ Host:

1. From the **Advanced** menu, select **Security & Firewall** and then click **DMZ Host**.
2. Select **Enable** for the DMZ Host.
3. Enter the IP address or select the MAC address of the device you want to designate as the DMZ Host.



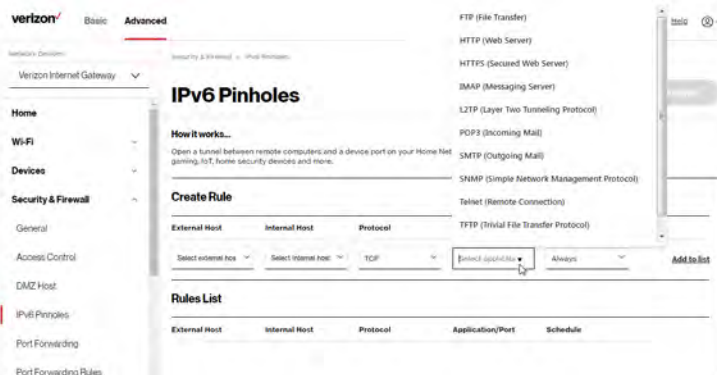
4. Click **Apply Changes** to save changes.

5.0d/ IPV6 PINHOLES

The IPv6 Pinhole feature of the Verizon Internet Gateway allows an application to send incoming packets for a certain port number to the destination computer by setting up the rule of authorization.

To configure the rules:

1. From the **Advanced** menu, select **Security & Firewall** and then click **IPv6 Pinhole**.



2. Select external and internal host, protocol and the application port type.
3. To schedule the rule, select either **Always** or **User Defined** in the **Schedule** list box.
4. Click **Add to list**. The screen displays opened pinhole port and its status. It shows the IP addresses of remote device and connected device on your network.
5. Click **Apply Changes** to save changes.

5.0e/ PORT FORWARDING

You can activate port forwarding to expose the network to the internet in a limited and controlled manner. For example, enabling applications, such as gaming and voice, to work from the local network as well as allowing internet access to servers within the local network.

SECURITY & FIREWALL

To create port forwarding rules:

1. From the **Advanced** menu, select **Security & Firewall** from the left pane and then click **Port Forwarding**. The **Port Forwarding** page opens with the current rules displayed.

The screenshot shows the Verizon Internet Gateway interface. The left sidebar has a menu with 'Security & Firewall' selected. The main content area is titled 'Port Forwarding' and includes a 'Create Rule' form. The form has the following fields: 'Application' (text input), 'Original Port' (text input with '0000'), 'Protocol' (dropdown menu with 'Select1'), 'Forward to Address' (dropdown menu with 'Select'), 'Forward to Port' (text input with '0000'), and 'Schedule' (dropdown menu with 'Select1'). An 'Add to list' button is located below the form. Below the form is a 'Rules List' table with the following data:

Application	Original Port	Protocol	Forward to Address	Forward to Port	Schedule
4967		TCP	127.0.0.1	4967	Always
4577		TCP	127.0.0.1	4577	Always

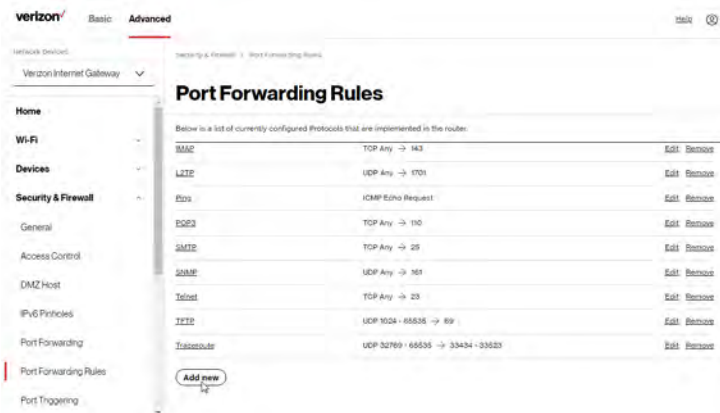
2. To create a new rule, enter the application name, configure its inbound and outbound port numbers, forwarding destination address, then select the protocol.
3. To schedule the rule, select either **Always** or **User Defined** in the **Schedule** list box.
4. Click **Add to list**. The rule displays in the **Rules List** section.
5. Click **Apply Changes** to save changes.

5.0f/ PORT FORWARDING RULES

You can view, modify, and delete port forwarding rules.

To access the rules:

1. Select **Port Forwarding Rules** in the **Security & Firewall** section.

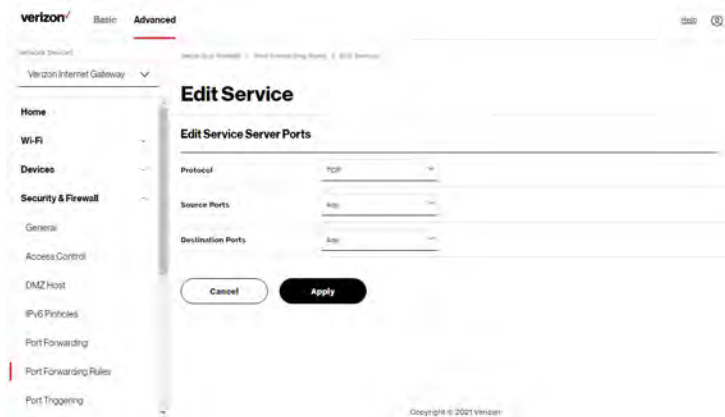


2. To create or edit a protocol rule, click the **Add new** or **Edit** icon in the action column. The **Edit Service** page displays.



SECURITY & FIREWALL

3. Modify the **Service Name** and **Service Description**, as needed.
4. To add server ports, click **Add**.
5. To modify the current protocol, click the **Edit** icon in the action column. The **Edit Service Server Ports** page displays.



6. Enter the **Protocol**, **Source Ports** and **Destination Ports**, as needed.
7. Click **Apply** to save changes.

5.0g/ PORT TRIGGERING

Port triggering can be described as dynamic port forwarding. By setting port triggering rules, inbound traffic arrives at a specific network host using ports that are different than those used for outbound traffic. The outbound traffic triggers the ports where the inbound traffic is directed.

For example, a gaming server is accessed using UDP protocol on port 2222. The gaming server then responds by connecting the user using UDP on port 3333, when a gaming session is initiated.

In this case, port triggering must be used since it conflicts with the following default firewall settings:

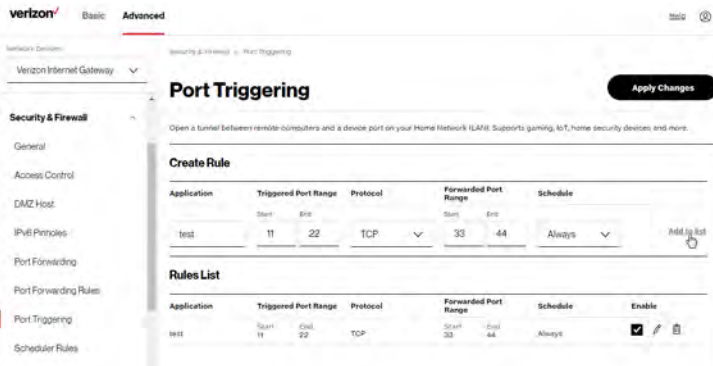
- Firewall blocks inbound traffic by default.
- Server replies to your Verizon Internet Gateway IP, and the connection is not sent back to the host since it is not part of a session.

To resolve the conflict, a port triggering entry must be defined, which allows inbound traffic on UDP port 3333 only after a network host generated traffic to UDP port 2222. This results in your Verizon Internet Gateway accepting the inbound traffic from the gaming server and sending it back to the network host which originated the outgoing traffic to UDP port 2222.

To configure port triggering:

1. From the **Advanced** menu, select **Security & Firewall** and then click **Port Triggering**.

SECURITY & FIREWALL



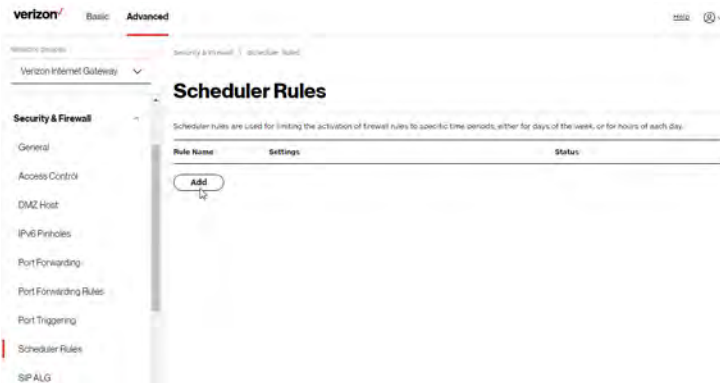
2. To add a service as an active protocol, enter the application name, configure its inbound and outbound (triggered/forwarded) port range, then select the protocol.
3. To schedule the rule, select either **Always** or **User Defined** in the **Schedule** list box.
4. Click **Add to list**. The rule displays in the **Rules List** section.
5. Click **Apply Changes** to save changes.

5.0h/ SCHEDULER RULES

Scheduler Rules are used for limiting the activation of firewall rules to specific time periods. The time periods are either for days of the week or for hours of each day based on activity or inactivity.

To define a rule:

1. Verify that the date and time of your Verizon Internet Gateway is correct.
2. Select **Scheduler Rules** in the **Security & Firewall** section.



3. Click **Add**. The **Set Rule Schedule** page displays.



4. Enter the name of the rule, select the active or inactive days of the week and the start and end time range.
5. Specify if the rule is **active** at the scheduled time or **inactive** at the scheduled time.
6. Click **Apply changes** to save changes.

SECURITY & FIREWALL

5.0i/ SIP ALG

SIP ALG (Application Level Gateway) - supports various multiple application protocols by allowing dynamic ephemeral TCP/ UDP ports to communicate with the known ports which a particular client application (such as FTP, VoIP service, net meeting or streaming media) requires.

To enable the SIP ALG settings:

1. From the **Advanced** menu, select **Security & Firewall** and then click **SIP ALG**.
2. Select **Enabled** for the SIP ALG.



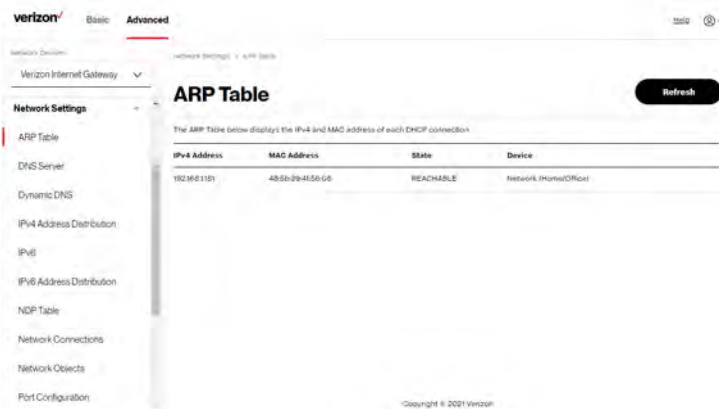
3. Click **Apply Changes** to save changes.

5.1/ NETWORK SETTINGS

5.1a/ ARP TABLE

You can view the IPv4 and MAC addresses of each DHCP connection.

To view the IPv4 and MAC addresses for each device: From the **Advanced** menu, select **Network Settings** and then click **ARP Table**.



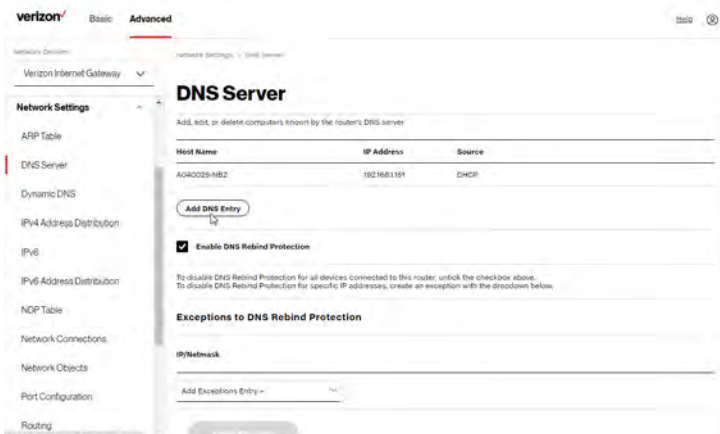
NETWORK SETTINGS

5.1b/ DNS SERVER

You can edit the host name and/or IP address, if the host was manually added to the DNS table. If not, you can only modify the host name.

To access the DNS server:

1. From the **Advanced** menu, select **Network Settings** and then click **DNS Server**.



2. To disable DNS rebind protection for all devices connected to the Gateway, untick the check box of **Enable DNS Rebind Protection**.

Warning: *Disabling this protection may create a risk of cybersecurity attack to devices connected to this Gateway.*

3. To add a computer stored in the **DNS** table, click **Add DNS Entry**. The **DNS Entry** page displays.



4. In the **Host Name** field, enter the name of the computer, then enter the **IP address** and click **Apply** to save changes.
5. Then the **DNS Server** page displays.
6. To add a new IP address entry, select the **Add Exceptions Entry** in the **Exceptions to DNS Rebind Protection** section. The **Add Exceptions List** page displays. Edit the IP address.
7. To remove a host from the DNS table, click the **Remove** icon on the screen.
8. Click **Apply changes** to save changes.

NETWORK SETTINGS

5.1c/ DYNAMIC DNS

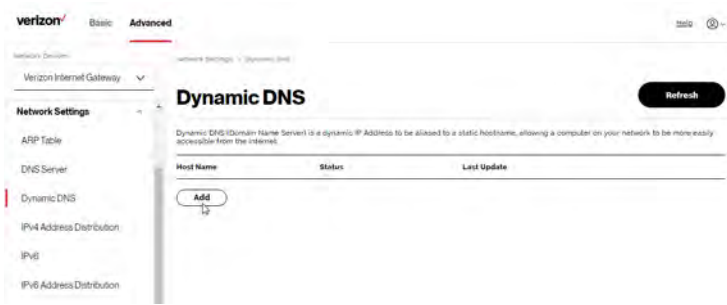
Typically, when connecting to the internet, your Gateway is assigned an unused public IP address from a pool, and this address changes periodically.

Dynamic DNS allows a static domain name to be mapped to the dynamic IP address, allowing a computer within your network to be more easily accessible from the internet.

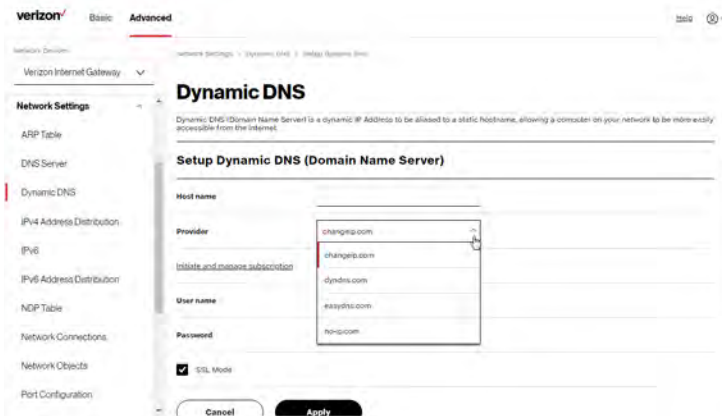
When using Dynamic DNS, each time the public IP address changes, the DNS database is automatically updated with the new IP address. In this way, even though the IP address changes often, the domain name remains constant and accessible.

To set up dynamic DNS:

1. Select **Dynamic DNS** in the **Network Settings** section.



2. To set up a new entry, click the **Add** button.



3. Configure the following parameters:
 - **Host Name** – enter the full domain name for your Dynamic DNS domain.
 - **Provider** – select the Dynamic DNS account provider from the menu.
 - **User Name** – enter your user name for your Dynamic DNS account.
 - **Password** – enter the password for your Dynamic DNS account.
 - **SSL Mode** – select if your Dynamic DNS service supports SSL.
4. Click **Apply** to save your changes.

NETWORK SETTINGS

5.1d/ IPV4 ADDRESS DISTRIBUTION

You can easily add computers configured as DHCP clients to the network. The DHCP server provides a mechanism for allocating IP addresses to these hosts and for delivering network configuration parameters to the hosts.

For example, a client (host) sends a broadcast message on the network requesting an IP address for itself. The DHCP server then checks its list of available addresses and leases a local IP address to the host for a specific period of time and simultaneously designates this IP address as taken. At this point, the host is configured with an IP address for the duration of the lease.

The host can renew an expiring lease or let it expire. If it renews a lease, the host receives current information about network services, as it did during the original lease, allowing it to update its network configurations to reflect any changes that occurred since the first connection to the network.

If the host wishes to terminate a lease before its expiration, it sends a release message to the DHCP server. This makes the IP address available for use by other hosts.

The DHCP server performs the following functions:

- Displays a list of all DHCP host devices connected to your Verizon Internet Gateway
- Defines the range of IP addresses that can be allocated in the network
- Defines the length of time the dynamic IP addresses are allocated

- Provides the above configurations for each network device and can be configured and enabled or disabled separately for each network device
- Assigns a static lease to a network computer to receive the same IP address each time it connects to the network, even if this IP address is within the range of addresses that the DHCP server may assign to other computer
- Provides the DNS server with the host name and IP address of each computer connected to the network

To view a summary of the services provided by the DHCP server:

1. Select **IPv4 Address Distribution** in the **Network Settings** section.



2. You can edit the DHCP server settings for a device. On the **IPv4 Address Distribution** page, click the **Edit** icon on the screen. The DHCP Settings page opens with the device information displayed.

NETWORK SETTINGS

3. To enable the DHCP server, select **DHCP Server** in the **IPv4 Address Distribution** field.
4. Once enabled, the DHCP server provides automatic IP assignments (IP leases) based on the preset IP range defined below.

The screenshot shows the Verizon Internet Gateway configuration page for DHCP Settings. The left sidebar lists various network settings, with 'IPv4 Address Distribution' highlighted. The main content area is titled 'DHCP Settings for Network (Home/Office)'. Under the 'Service' section, the 'IPv4 Address Distribution' dropdown menu is open, showing options: 'DHCP Server', 'Disabled', and 'DHCP Server'. The 'Start IP Address' field is set to 192.168.1.2, and the 'End IP Address' field is set to 192.168.1.254. The 'Lease Time in Minutes' field is set to 1440. Below these fields, there is a section for 'IPv4 Address Distribution According to DHCP Option 60 (Vendor Class Identifier)' with a table showing IP Address, MAC Address, and GUS.

Vendor Class Id	IP Address	MAC Address	GUS
MDPT 5.0	192.168.1.151	48:05:39:4F:56:06	

5. To configure the DHCP server, complete the following fields:
 - **Start IP Address** – enter the first IP address that your Verizon Internet Gateway will automatically begin assigning IP addresses from. Since your Verizon Internet Gateway’s default IP address is 192.168.1.1, the default start IP address should be 192.162.1.2.
 - **End IP Address** – enter the last IP address that your Verizon Internet Gateway will stop at for the IP address allocation. The maximum end IP address range that can be entered is 192.168.1.254.

- **WINS Server** – determines the IP address associated with a network device.
- **Lease Time in Minutes** – assigns the amount of time in minutes that each device is assigned an IP address by the DHCP server when it connects to the network.

When the lease expires, the server determines if the computer has disconnected from the network. If it has, the server may reassign this IP address to a newly connected computer.

6. Click **Apply** to save changes.

IPv4 Address Distribution According to DHCP option 60 (Vendor Class Identifier)

DHCP vendor class is related to DHCP option 60 configuration within the Gateway. User can add option 60 configurations such that particular vendor can get lease from a specified pool of address. The existing vendor class ID, IP address, MAC address and QoS are shown on the screen above.

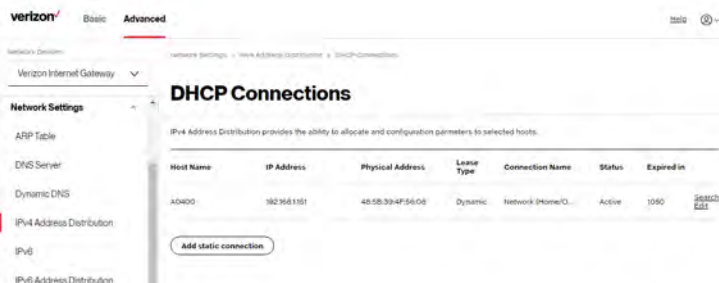
DHCP Connection List

You can view a list of the connections currently assigned and recognized by the DHCP server.

NETWORK SETTINGS

To view a list of computers:

1. On the **IPv4 Address Distribution** page, click **Connection List**.



2. To define a new static connection with a fixed IP address, click **Add static connection**.



3. Enter the host name.
4. Enter the fixed IP address to be assigned.
5. Enter the MAC address of the network interface of the computer used with this DHCP static connection.
6. Click **Apply** to save changes.

5.1e/ IPV6

Use the IPv6 feature settings to enable, disable, or configure an IPv6 Internet connection and IPv6 LAN settings.

1. To configure your network to use the IPv6 Internet connection type, select **IPv6** in the **Network Settings** section to display the IPv6 service options:

The screenshot shows the Verizon router's web interface for IPv6 Configuration Controls. The page is titled "IPv6 Configuration Controls" and has an "Apply Changes" button. The left sidebar shows "Network Settings" with "IPv6" highlighted. The main content area is divided into three sections:

- 1. Enable IPv6 Support**: A toggle switch labeled "Enabled" is turned on.
- 2. Specify the method to be used to obtain your WAN IPv6 Address**: A dropdown menu is open, showing options: "DHCPv6-PD", "None", "DHCPv6-PD", "Static (Auto-Configure)", and "Static (Manually Configure)". "DHCPv6-PD" is selected.
- 3. Specify the method to be used to assign LAN IPv6 addresses**: A dropdown menu is open, showing options: "Stateless" and "Stateful". "Stateless" is selected.

2. Select **Enabled** in the **Enable IPv6 Support** field. (Once IPv6 is enabled the default setting will be IPv6 WAN as DHCPv6 and IPv6 LAN as Stateless).
3. Select the appropriate IPv6 connection method from the dropdown list (DHCPv6 or Static) to specify the method to be used to obtain your WAN IPv6 Address.

NETWORK SETTINGS

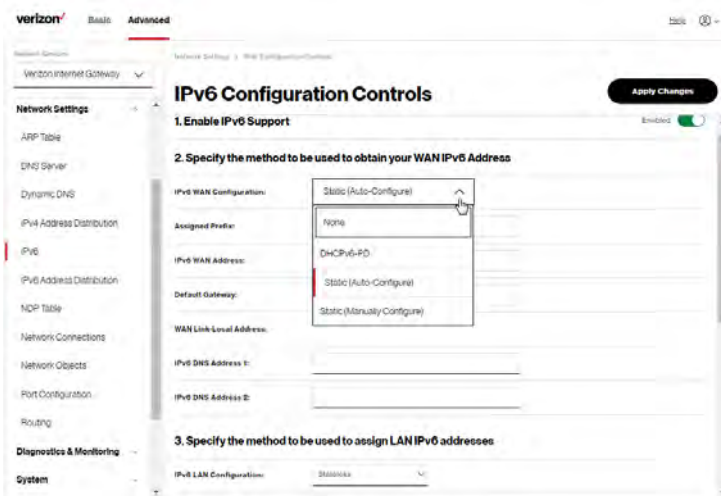
- 4. Click **Apply changes** to have changes take effect.
 - Note: The Internet IPv6 service is required for this feature to work over the internet.*
 - 5. To disable the IPv6 service, move the selector to **off** in the **Enable IPv6 Support** field.
 - 6. Click **Apply changes** to have changes take effect.
- Once configured using valid IPv6 WAN and LAN configurations, you should not see any errors when you click on the **Apply changes** button and the **Basic/System/System Status** page will reflect the Gateway's new IPv6 address.
- You should also see the IPv6 address for all IPv6 supported devices on your local network displayed on the **Basic/Devices/Devices** page by selecting the Settings icon to access the **Device Settings** page for that device.



Static - WAN IPv6 Address Connection

The IPv6 WAN Static configurations are IPv6 settings that you enter manually. These specific IPv6 addresses and settings are not expected to change frequently.

1. To configure IPv6 WAN Static mode, select the **Static** option on the **IPv6 Configuration Controls** page as shown below:



2. Specify the **Static** method to be used to obtain your WAN IPv6 Address by entering:
 - **IPv6 WAN Configuration** (select Static)
 - **Assigned Prefix** (A numeric value between 16 and 128)
 - **IPv6 WAN Address**
 - **Default Gateway:** Verizon Internet Gateway
 - **IPv6 (Primary) DNS Address 1**
 - **IPv6 (Secondary) DNS Address 2**
3. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

NETWORK SETTINGS

Static WAN with LAN IPv6 Stateful Settings

1. To configure IPv6 LAN Stateful mode with **Static** WAN, select the **Stateful (DHCPv6)** option on the **IPv6 Configuration Controls** page as shown below:

The screenshot displays the 'IPv6 Configuration Controls' page in the Verizon Network Settings interface. The left sidebar shows a navigation menu with 'IPv6' highlighted. The main content area is titled 'IPv6 Configuration Controls' and includes an 'Apply Changes' button. The configuration is divided into sections: '3. Specify the method to be used to assign LAN IPv6 addresses', 'IPv6 LAN Configuration' (a dropdown menu with 'Stateful (DHCPv6)' selected), 'LAN Prefix', 'DHCPv6 Client Address Range' (with start and end address fields), 'LAN Link Local Address', 'Subnet ID' (with a value of 00), 'Router Advertisement Lifetime' (with a value of 15), and 'IPv6 Address Lifetime' (with a value of 90). An 'Option' section at the bottom contains a checkbox for 'Allow ICMPv6 Echo Requests for LAN devices using their Global IPv6 Address from WAN side'.

2. Specify the **Stateful (DHCPv6)** settings to be used to assign LAN IPv6 addresses by entering the following details:
 - **IPv6 LAN Configuration** (select **Stateful** from the dropdown list)
 - **LAN Prefix** (automatically populated)
 - **DHCPv6 Client Address Range** (start and end)
 - **LAN Link Local Address** (automatically populated)
 - **Subnet ID** - set the site topology for your internal site

- **Router Advertisement Lifetime** (minutes between 0-150)
 - **IPv6 Address Lifetime** (minutes between 3-150)
 - **Option: Allow ICMPv6 Echo Request for LAN devices** using their **Global IPv6 Address** from **WAN** side - requesting an IPv6 address from any available DHCPv6 servers available on the ISP
3. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

Static WAN with LAN IPv6 Stateless Settings

1. To configure IPv6 LAN Stateless mode with **Static WAN**, select the **Stateless** option on the **IPv6 Configuration Controls** page as shown below:

The screenshot shows the Verizon router's web interface. The left sidebar lists various settings categories: Network Settings, Network Connections, Network Objects, Port Configuration, Routing, Diagnostics & Monitoring, and System. The 'IPv6' option under Network Settings is highlighted. The main content area is titled 'IPv6 Configuration Controls' and includes an 'Apply Changes' button. The settings are organized into sections: 'Obtain IPv6 DNS Server address automatically' (radio buttons for 'Obtain IPv6 DNS Server address automatically' and 'Use the following IPv6 DNS Server addresses'), '3. Specify the method to be used to assign LAN IPv6 addresses' (a dropdown menu for 'IPv6 LAN Configuration' with 'Stateless' selected), 'LAN Prefix', 'LAN Link-Local Address', 'Subnet ID', 'Router Advertisement Lifetime', and an 'Option' section with a checkbox for 'Allow ICMPv6 Echo Request for LAN devices using their Global IPv6 Address from WAN side'.

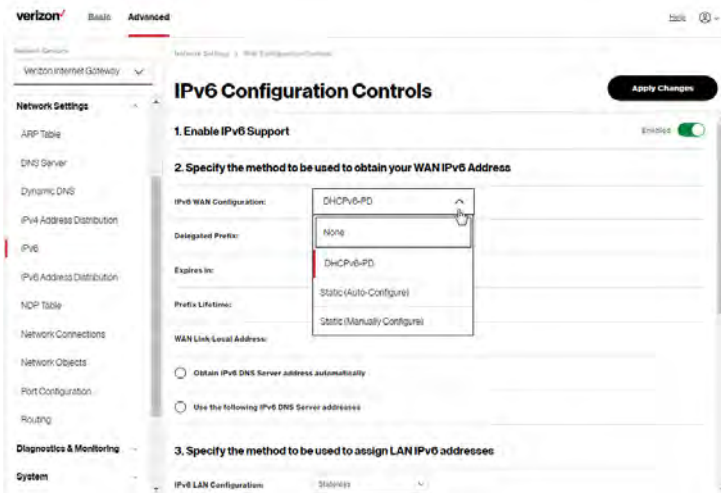
NETWORK SETTINGS

2. Specify the settings to be used to assign LAN IPv6 addresses by entering the following details:
 - **IPv6 LAN Configuration** (select **Stateless** from the dropdown list)
 - **LAN Prefix** (automatically populated)
 - **LAN Link Local Address** (automatically populated)
 - **Subnet ID** - set the site topology for your internal site
 - **Router Advertisement Lifetime** (minutes between 0-150)
 - **Option: Allow ICMPv6 Echo Request for LAN devices using their Global IPv6 Address from WAN side** - requesting an IPv6 address from any available DHCPv6 servers available on the ISP
3. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

DHCPv6 PD - WAN IPv6 Address Connection

The IPv6 WAN DHCPv6 configurations are IPv6 settings that you enter that will allow your IPv6 connection to be updated by the ISP as needed.

1. To configure IPv6 WAN Stateful (DHCPv6) mode, select the **DHCPv6-PD** option on the **IPv6 Configuration Controls** page as shown below:



2. Check to either **Obtain IPv6 DNS Server address automatically**, or **Use the following IPv6 DNS Server addresses**
3. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

DHCPv6 WAN with LAN IPv6 Stateful (DHCPv6) Settings

1. To configure IPv6 WAN Stateful (DHCPv6) mode, select the **Stateful (DHCPv6)** option on the **IPv6 Configuration Controls** page as shown below:

NETWORK SETTINGS

verizon Basic Advanced

Network Settings

IPv6 Configuration Controls

Apply Changes

3. Specify the method to be used to assign LAN IPv6 addresses

IPv6 LAN Configuration: Stateful (DHCPv6)

LAN Prefix: [empty]

DHCPv6 Client Address Range: [empty] - [empty]

LAN Link Local Address: [empty]

Subnet ID: 00

Router Advertisement Lifetime: 15 (minutes) (0-150)

IPv6 Address Lifetime: 90 (minutes) (3-150)

Option

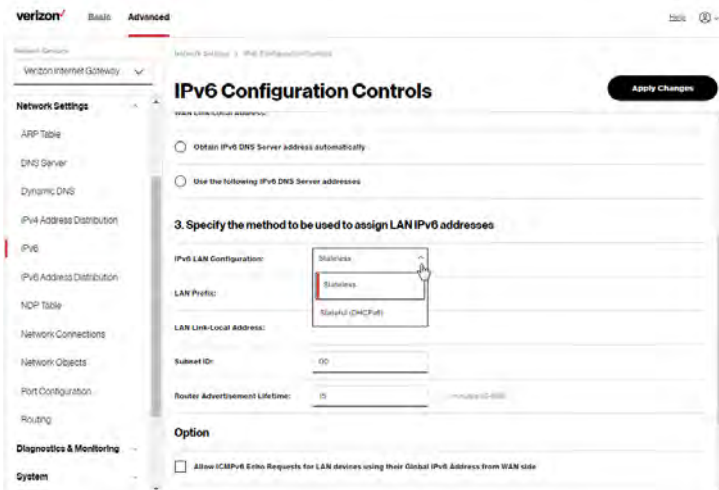
☐ Allow ICMPv6 Echo Requests for LAN devices using their Global IPv6 Address from WAN side

2. Specify the **Stateful (DHCPv6)** settings to be used to assign LAN IPv6 addresses by entering the following details:
 - **IPv6 LAN Configuration** (select **Stateful** from the dropdown list)
 - **LAN Prefix** (automatically populated)
 - **DHCPv6 Client Address Range** (start and end)
 - **LAN Link Local Address** (automatically populated)
 - **Subnet ID** - set the site topology for your internal site
 - **Router Advertisement Lifetime** (minutes between 0-150)
 - **IPv6 Address Lifetime** (minutes between 3-150)

- Option: Allow ICMPv6 Echo Request for LAN devices using their Global IPv6 Address from WAN side - requesting an IPv6 address from any available DHCPv6 servers available on the ISP
3. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

DHCPv6 WAN with LAN IPv6 Stateless Settings

1. To configure IPv6 LAN Stateless mode with DHCPv6 WAN, select the **Stateless** option on the **IPv6 Configuration Controls** page as shown below:

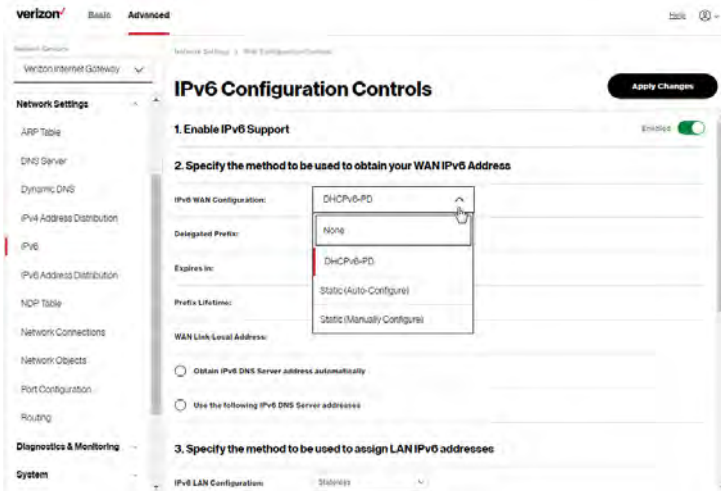


NETWORK SETTINGS

2. Specify the settings to be used to assign LAN IPv6 addresses by entering the following details:
 - **IPv6 LAN Configuration** (select **Stateless** from the dropdown list)
 - **LAN Prefix** (automatically populated)
 - **LAN Link Local Address** (automatically populated)
 - **Subnet ID** - set the site topology for your internal site
 - **Router Advertisement Lifetime** (minutes between 0-150)
 - **Option: Allow ICMPv6 Echo Request for LAN devices using their Global IPv6 Address from WAN side** - requesting an IPv6 address from any available DHCPv6 servers available on the ISP
3. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

LAN IPv6 Configuration without An IPv6 WAN Connection

1. To configure IPv6 to use either the IPv6 LAN Stateful or Stateless mode without using an IPv6 Internet WAN connection, select the **None** option on the **IPv6 Configuration Controls** page.



2. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

LAN IPv6 Stateful (DHCPv6) with No WAN Settings

1. To configure IPv6 LAN Stateful mode with no WAN connection, select the Stateful option on the **IPv6 Configuration Controls** page as shown below:

NETWORK SETTINGS

The screenshot shows the Verizon Network Settings interface. On the left is a sidebar with a menu: Network Settings (selected), ARP Table, DNS Server, Dynamic DNS, IPv4 Address Distribution, IPv6 (highlighted with a red bracket), IPv6 Address Distribution, NDP Table, Network Connections, Network Objects, Port Configuration, Routing, Diagnostics & Monitoring, and System. The main content area is titled 'IPv6 Configuration Controls' and has a sub-header '2. Specify the method to be used to obtain your WAN IPv6 Address'. Below this, 'IPv6 WAN Configuration' is set to 'None'. A section titled '3. Specify the method to be used to assign LAN IPv6 addresses' contains 'IPv6 LAN Configuration' set to 'Stateful (DHCPv6)', 'DHCPv6 Client Address Range' with start and end address fields, and 'LAN Link-Local Address' which is populated. Below these are 'Router Advertisement Lifetime' (15 minutes) and 'IPv6 Address Lifetime' (60 minutes). At the bottom, an 'Option' section has a checkbox for 'Allow ICMPv6 Echo Requests for LAN devices using their Global IPv6 Address from WAN side'.

2. Specify the **Stateful (DHCPv6)** settings to be used to assign LAN IPv6 addresses by entering the following details:
 - **IPv6 LAN Configuration** (select **Stateful** from the dropdown list)
 - **DHCPv6 Client Address Range** (start and end)
 - **LAN Link Local Address** (automatically populated)
 - **Router Advertisement Lifetime** (minutes between 0-150)
 - **IPv6 Address Lifetime** (minutes between 3-150)
 - **Option: Allow ICMPv6 Echo Request for LAN devices using their Global IPv6 Address from WAN side** - requesting an IPv6 address from any available DHCPv6 servers available on the ISP
3. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

LAN IPv6 Stateless with No WAN Settings

1. To configure IPv6 LAN Stateless mode with no WAN connection, select the **Stateless** option on the **IPv6 Configuration Controls** page as shown below:



2. Specify the settings to be used to assign LAN IPv6 addresses by entering the following details:
 - **IPv6 LAN Configuration** (select **Stateless** from the dropdown list)
 - **LAN Link Local Address** (automatically populated)
 - **Router Advertisement Lifetime** (minutes between 0-150)
 - **Option: Allow ICMPv6 Echo Request for LAN devices using their Global IPv6 Address from WAN side** - requesting an IPv6 address from any available DHCPv6 servers available on the ISP

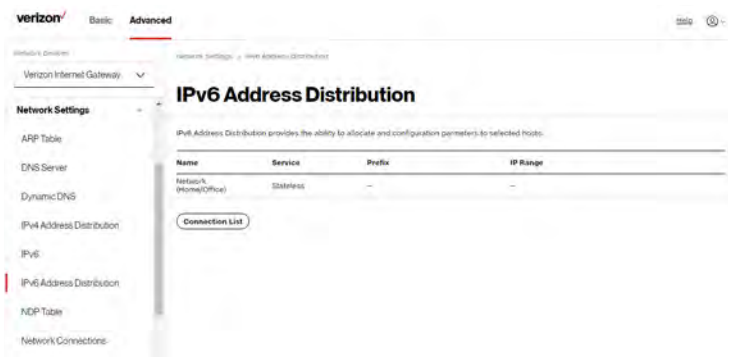
NETWORK SETTINGS

3. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

5.1f/ IPV6 ADDRESS DISTRIBUTION

To view a summary of the services provided by the DHCP server:

1. Select **IPv6 Address Distribution** in the **Network Settings** section.



2. You can edit the DHCP server settings for a device. On the **IPv6 Address Distribution** page, click the **Edit** icon on the screen column. The DHCP Settings page opens with the device information displayed.
3. To configure the DHCP server complete the following fields:
 - **Start IPv6 Address** – the starting IPv6 address in the consecutive list of addresses that makes up this LAN pool for the DHCPv6 server.

- **End IPv6 Address** – the ending IPv6 address in the consecutive list of addresses that makes up this LAN pool for the DHCPv6 server.
- **Lease Time in Minutes** – assigns the amount of time in minutes that each device is assigned an IP address by the DHCP server when it connects to the network.

When the lease expires, the server determines if the computer has disconnected from the network. If it has, the server may reassign this IP address to a newly connected computer.

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

DHCP Connection List

You can view a list of the connections currently assigned and recognized by the DHCP server.

To view a list of computers:

1. On the **IPv6 Address Distribution** page, click **Connection List**.
2. To define a new static connection with a fixed IP address, click **Add static connection**.
3. Enter the host name.
4. Enter the fixed IP address to be assigned.
5. Enter the MAC address of the network interface of the computer used with this DHCP static connection.
6. Click **Apply** to save changes.

NETWORK SETTINGS

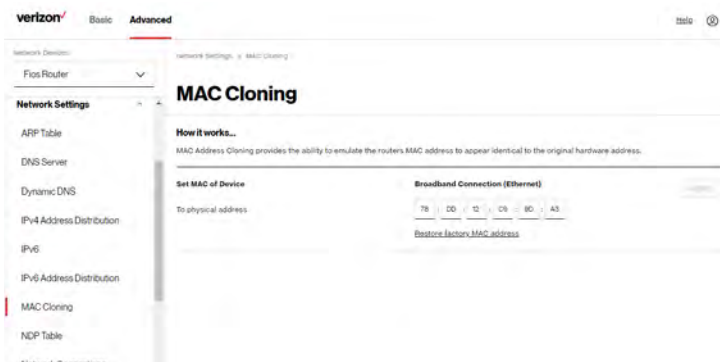
5.1g/ MAC CLONING

A MAC address is a hexadecimal code that identifies a device on a network. All networkable devices have a unique MAC address.

When replacing a network device on your Verizon Internet Gateway, you can simplify the installation process by copying the MAC address of the existing device to your Verizon Internet Gateway.

To copy the MAC address of the existing device:

1. Select **MAC Cloning** in the **Network Settings** section.



2. In the **To physical address** field, enter the MAC address of your new device.
3. To locate the MAC address, refer to the documentation from the device manufacturer.
4. Click **Apply** to save changes.

5.1h/ NDP TABLE

You can view the IPv6 and MAC addresses of each DHCP connection.

*To view the IPv6 and MAC addresses for each device: select **NDP** (Neighbor Discovery Protocol) **Table** in the **Network Settings** section.*



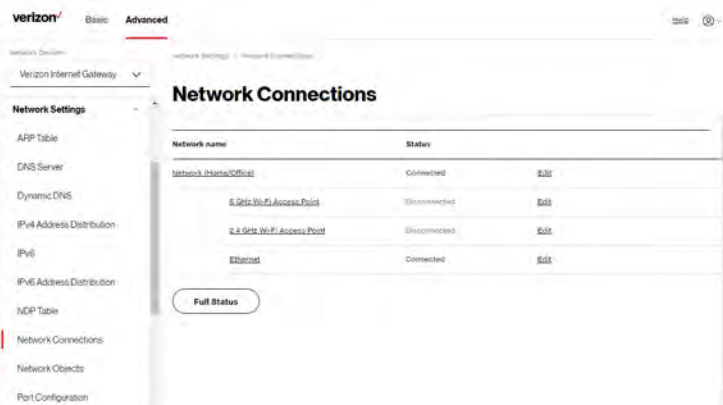
5.1i/ NETWORK CONNECTIONS

Caution: *The settings described in this chapter should only be configured by experienced network technicians. Changes could adversely affect the operation of your Gateway and your local network.*

To view the network connections:

1. From the **Advanced** menu, select **Network Settings** from the left pane and then click **Network Connections**.

NETWORK SETTINGS



2. To view and edit the details of a specific network connection, click the hyperlinked name or the action icon. The following sections detail the types of network connections that you can view.

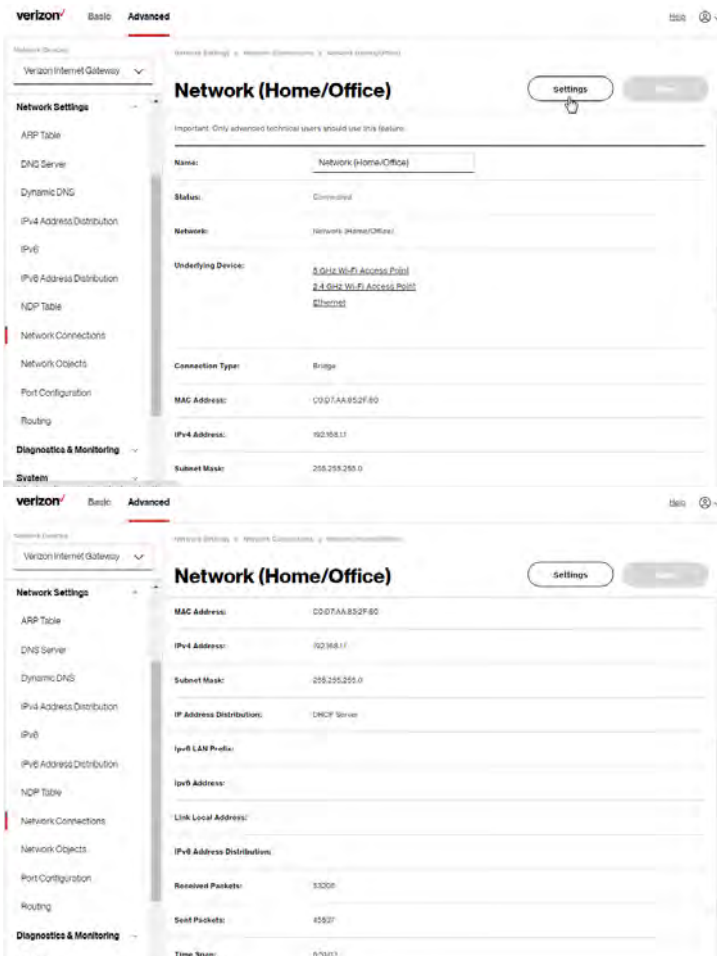
NETWORK (HOME/OFFICE) CONNECTION

You can view the properties of your local network. This connection is used to combine several network interfaces under one virtual network. For example, you can create a home/office network connection for Ethernet and other network devices.

Note: When a network connection is disabled, the underlying devices formerly connected to it will not be able to obtain a new DHCP address from that Verizon Internet Gateway network interface.

To view the connection:

1. On the **Network Connections** page, click the **Network (Home/Office)** connection link. The **Network (Home/ Office) Properties** page displays.



NETWORK SETTINGS

2. To rename a network connection, enter the new network name in the **Name** field.
3. Click **Save** to save the changes.

CONFIGURING THE HOME/OFFICE NETWORK

To configure the network connection:

1. In the **Network (Home/Office)** properties page, click **Settings**. The configuration page displays.

The screenshot shows the Verizon Network (Home/Office) configuration page. The left sidebar contains a navigation menu with categories: Network Settings, Network Connections, Network Objects, Port Configuration, Routing, Diagnostics & Monitoring, and System. The main content area is titled "Network (Home/Office)" and includes a "Settings" button. Below the title, there is a warning: "Important: Only advanced technical users should use this feature." The configuration is divided into sections: General, Bridge, and a table for connections. The General section includes fields for Status (Controlled), Connection Type (Network (Home/Office)), Physical Address (C0D7A652F80), MTU (Automatic, 1500), IP Address (192.168.1.1), and Subnet Mask (255.255.255.0). The Bridge section has a table with columns Name, VLAN, and Status. The connections table shows two entries: "Broadband Connection (Ethernet)" and "Ethernet", both with a status of "Disconnected".

Name	VLAN	Status
Broadband Connection (Ethernet)	Disabled	Disconnected
Ethernet	Disabled	Disconnected

verizon Basic Advanced

Network Settings

Network (Home/Office)

Bridge

Name	VLAN	Status	Action
☐ Broadband Connection (Ethernet)	Disable	Disconnected	Edit
☐ Broadband Connection (Ethernet)	Disable	Disconnected	Edit
☐ Broadband Connection (Ethernet)	Disable	Disconnected	Edit
☐ Broadband Connection (Ethernet)	Disable	Connected	Edit

IP Address Distribution: DHCP Server: [v]

Start IP Address: 192.168.1.2

End IP Address: 192.168.1.254

WINS Server: 0.0.0.0

Lease time in minutes: 1440

IP Address Distribution According to DHCP Option 80 (Vendor Class Identifier)

Vendor Class ID	IP Address	MAC Address	QoS
MSFT 5.0	192.168.1.101	48:50:39:4F:50:00	

Routing Table

Name	Destination	Gateway	Netmask	Metric	Status	Action
Add new route						

2. Configure the following sections, as needed.

NETWORK SETTINGS

General

In the **General** section, verify the following information:

- **Status** - displays the connection status of the network.
- **Connection Type** - displays the type of connection interface.
- **Physical Address** - displays the physical address of the network card used for the network.
- **MTU** - displays the Maximum Transmission Unit (MTU) indicating the largest packet size permitted for internet transmissions:
 - **Automatic**: sets the MTU (Maximum Transmission Unit) at 1500.
 - **Automatic by DHCP**: sets the MTU according to the DHCP connection.
 - **Manual**: allows you to manually set the MTU.
- **IP address and Subnet Mask**: the network connection uses a permanent or static **IP address** and **Subnet Mask** address, provided by Verizon or experienced network technician.
- **Bridge**

In the **Bridge** section of the **Network (Home/Office)** properties, you can configure the various LAN interfaces.

***Caution:** Do not change these settings unless specifically instructed to by Verizon. Changes could adversely affect*

the operation of your Verizon Internet Gateway and your local network.

Verify the following information:

- **Status** – displays the connection status of a specific network connection.
- **Action** – contains an **Edit** hyperlink that, when clicked, generates the next level configuration page for the specific network connection or network device.

- **IP Address Distribution**

The **IP Address Distribution** section is used to configure the Dynamic Host Configuration Protocol (DHCP) server parameters of your Verizon Internet Gateway.

Once enabled and configured, the DHCP server automatically assigns IP addresses to any network devices which are set to obtain their IP address dynamically.

If DHCP Server is enabled on your Verizon Internet Gateway, configure the network devices as DHCP Clients. There are 2 basic options in this section: **Disabled** and **DHCP Server**.

To set up the Verizon Internet Gateway's network bridge to function as a DHCP server:

1. In the **IP Address Distribution** section, select the **DHCP server**. Once enabled, the DHCP server

NETWORK SETTINGS

provides automatic IP assignments (also referred to as IP leases) based on the preset IP range defined below.

- **Start IP Address** – Enter the first IP address in the IP range that the Verizon Internet Gateway will automatically begin assigning IP addresses from. Since your Verizon Internet Gateway's IP address is 192.168.1.1, the default Start IP Address is 192.168.1.2.
 - **End IP Address** – Enter the last IP address in the IP range that the Verizon Internet Gateway will automatically stop the IP address allocation at. The maximum end IP address range that can be entered is 192.168.1.254.
2. If Windows Internet Naming Service (WINS) is being used, enter the **WINS Server** address.
 3. In the **Lease time in minutes** field, enter the amount of time a network device is allowed to connect to the Verizon Internet Gateway with its currently issued dynamic IP address.
- **IP Address Distribution According to DHCP option 60 (vendor class Identifier)**

DHCP vendor class is related to DHCP option 60 configuration within the Gateway. Adding option 60 configurations allows a particular vendor to get a lease from a specified pool of addresses.

Routing Table

You can configure your Verizon Internet Gateway to use static or dynamic routing.

- **Static routing** – specifies a fixed routing path to neighboring destinations based on predetermined metrics.
- **Dynamic routing** – automatically adjusts how packets travel on the network. The path determination is based on network/device reachability and the status of the network being traveled.

To configure routing:

1. In the **Routing Table** section, click **Add new route** button to display and modify the new route configuration page.



2. To save your changes click **Apply**.

NETWORK SETTINGS

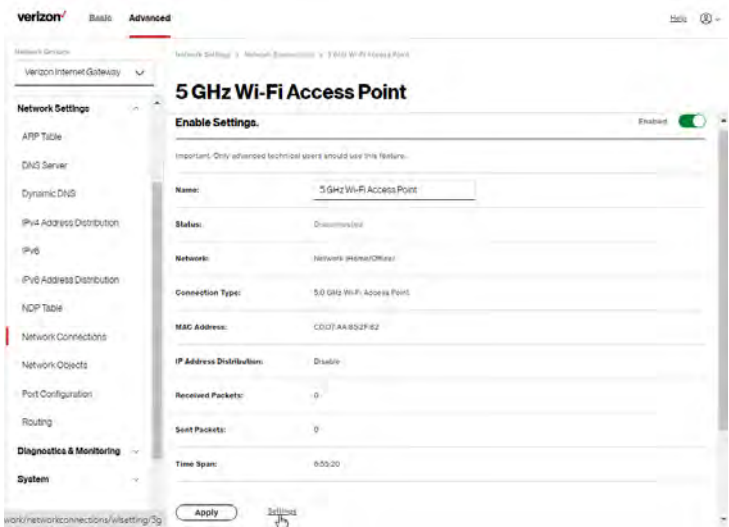
Wi-Fi ACCESS POINT CONNECTION

A Wi-Fi Access Point network connection allows Wi-Fi devices to connect to the local area network (LAN) using the 2.4 GHz or 5 GHz Wi-Fi network.

Note: Once disabled, all Wi-Fi devices connected to that Wi-Fi network will be disconnected from the LAN network and internet.

To view the connection settings:

1. From the **Advanced** menu, select **Network Settings** from the left pane and then click **Network Connections**.
2. To access the connection settings pages, click on the link of the Wi-Fi Access Point connections listed under **Network name** on the **Network Connections** page.



3. From the connection's **Enable Settings** page, to enable or disable the connection, move the selector to **on** or **off**.
4. To rename the connection, enter a name in the **Name** field.
5. Click **Apply** to save the changes.
6. Reboot your Verizon Internet Gateway.

CONFIGURING WI-FI ACCESS POINT PROPERTIES

To configure the connection:

1. On the bottom of the Access Point's specific **Enable Settings** page, click **Settings**. The configuration page displays.

The screenshot shows the Verizon Internet Gateway configuration interface. The top navigation bar includes the Verizon logo, 'Basic', and 'Advanced' tabs. The left sidebar lists various settings categories: Network Settings (selected), ARP Table, DNS Server, Dynamic DNS, IPv4 Address Distribution, IPv6, IPv6 Address Distribution, ICMP Table, Network Connections, Network Objects, Port Configuration, and Routers. The main content area is titled '5 GHz Wi-Fi Access Point' and contains a 'General' section. A warning message states: 'Important: Only advanced technical users should use this feature.' The configuration fields are as follows: 'Status' is set to 'On (recommended)'; 'Network' is 'Network (Home/Office)'; 'Connection Type' is '5.0 GHz Wi-Fi Access Point'; 'Physical Address' is 'C0:07:AA:B5:5F:82'; 'MTU' is set to 'Automatic' with a value of '1500' displayed. An 'Apply' button is located at the bottom of the configuration area.

2. Verify the following information:

NETWORK SETTINGS

General

- **Status** - displays the connection status of the network.
- **Network** – displays the type of network connection.
- **Connection Type** - displays the type of connection interface.
- **Physical Address** - displays the physical address of the network card used for the network.
- **MTU** - specifies the largest packet size permitted for internet transmissions:
 - **Automatic**: set the MTU (Maximum Transmission Unit) at 1500.
 - **Automatic by DHCP**: sets the MTU according to the DHCP connection.
 - **Manual**: allows you to manually set the MTU.

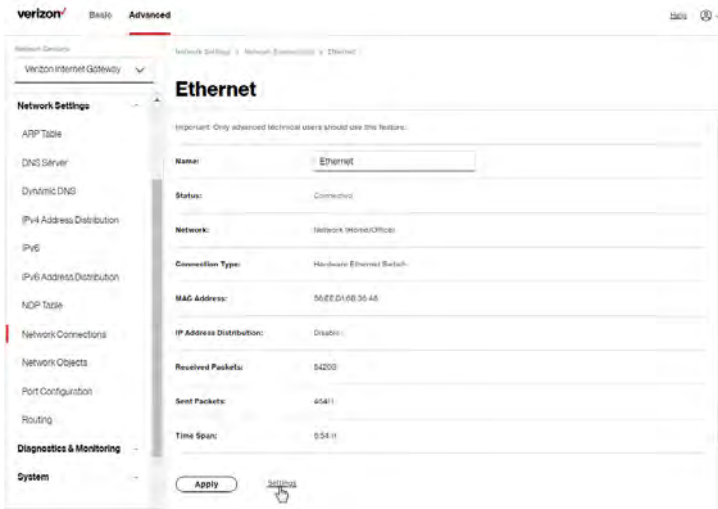
3. Click **Apply** to save changes.

ETHERNET CONNECTION

You can view the properties of your Ethernet LAN connection using an Ethernet cable inserted into one of your Verizon Internet Gateway's Ethernet LAN ports.

To view the connection settings:

1. To access the **Ethernet** properties page, click the **Ethernet** link listed under **Network name** on the **Network Connections** page.



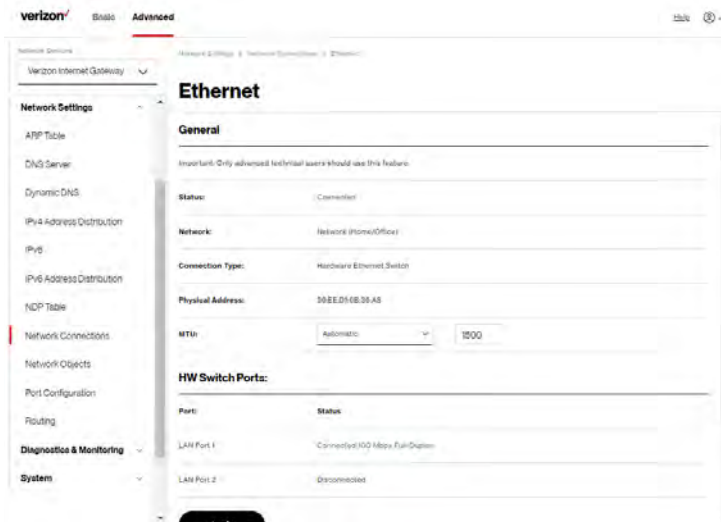
2. To rename the network connection, enter the new name in the **Name** field.
3. Click **Apply** to save changes.

CONFIGURING ETHERNET PROPERTIES

To configure the connection:

1. In the **Ethernet** page, click **Settings**. The configuration page displays.

NETWORK SETTINGS



2. Verify the following information:

General

- **Status** - displays the connection status of the network.
- **Network** – displays the type name of network connection.
- **Connection Type** - displays as **Hardware Ethernet Switch**.
- **Physical Address** - displays the physical address of the network card used for the network.
- **MTU** - specifies the largest packet size permitted for
 - **Automatic**: sets the MTU (Maximum Transmission Unit at 1500).

- **Automatic by DHCP:** sets the MTU according to the DHCP connection.
 - **Manual:** allows you to manually set the MTU.
 - **HW Switch Ports** - displays the status of each LAN port.
3. Click **Apply** to save the changes.

5.1j/ NETWORK OBJECTS

Network objects define a group, such as a group of computers, on your Verizon Internet Gateway network by MAC address, IP address, and/or host name. The defined group becomes a network object. You can apply settings, such as configuring system rules, to all devices defined in the network object.

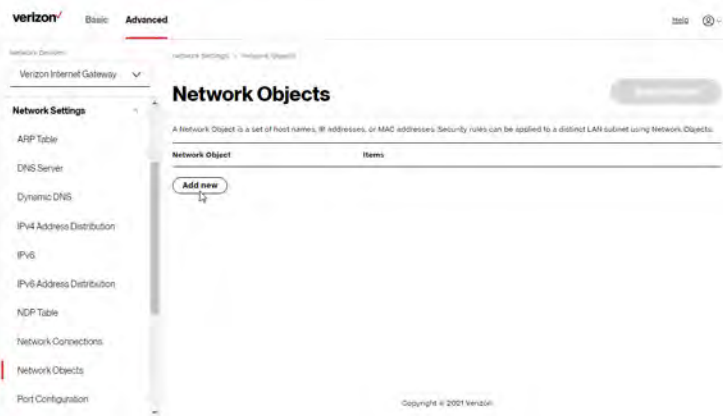
For example, instead of setting the same website filtering configuration individually to five computers one at a time, you can define the computers as a network object. Website filtering can then be simultaneously applied to all the computers.

You can use network objects to apply security rules based on host names, instead of IP addresses. This is useful since IP addresses change from time to time. In addition, you can define network objects according to MAC address to make the rule application more persistent against network configuration settings.

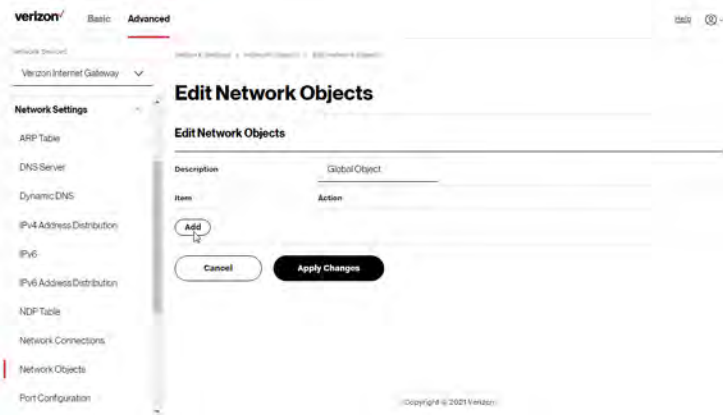
NETWORK SETTINGS

To define a network object:

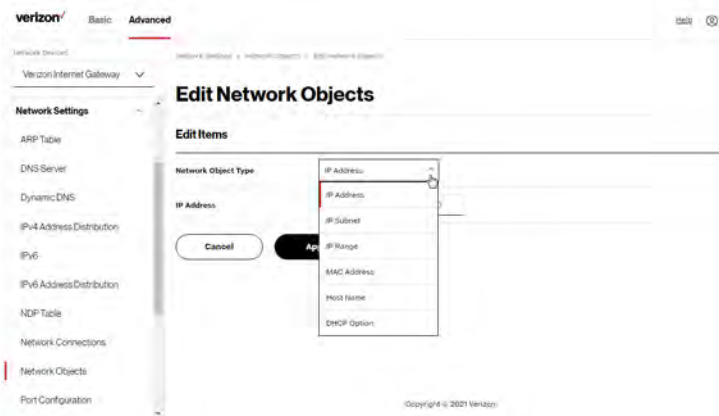
1. From the **Advanced** menu, select **Network Settings**.
2. Select **Network Objects** in the **Network Settings** section.



3. To define a network object, click **Add new**. The **Edit Network Objects** page displays.



4. In the **Description** field, enter a name for the network object.
5. Click **Add**. The **Edit Item** page displays.



6. Select and configure the type of network object as IP address, IP subnet, IP range, MAC address, host name, or DHCP option, and click **Apply** to save changes.
7. Repeat the above steps to create additional network objects.
8. When complete, click **Apply changes** to save changes.

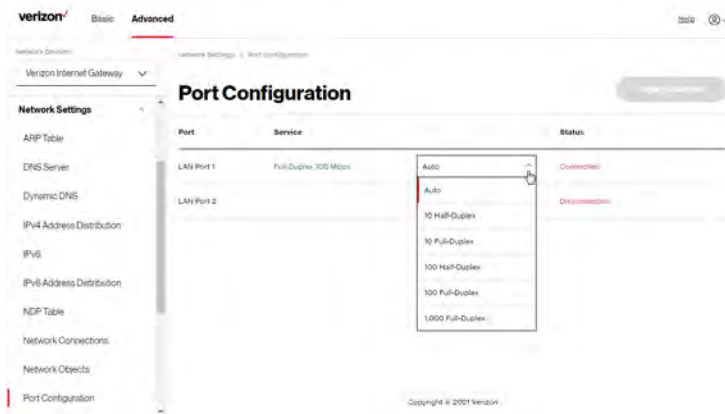
NETWORK SETTINGS

5.1k/ PORT CONFIGURATION

Ethernet port configuration allows you to set up the Ethernet ports as either full- or half-duplex ports, at either 10 Mbps, 100 Mbps, or 1000 Mbps.

To configure the ports:

1. Select **Port Configuration** in the **Network Settings** section.



2. To emulate the speed and duplex configuration of the port with which it's communicating, select **Auto** or select the port speed and duplicity.
3. Click **Apply changes** to save changes.

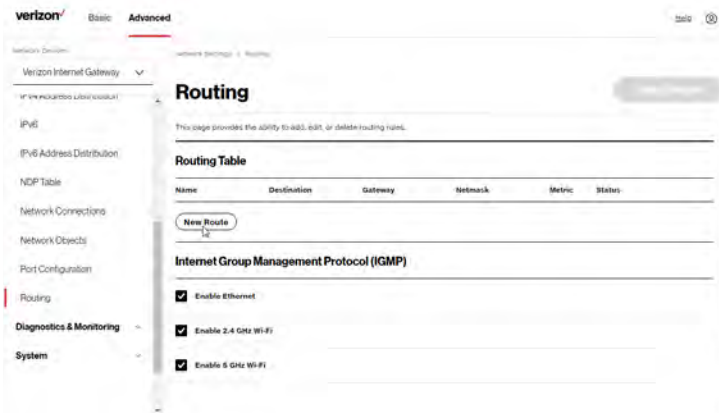
5.11/ ROUTING

You can view the routing and IP address distribution rules as well as add, edit, or delete the rules.

Routing Table

To view the rules:

1. Select **Routing** in the **Network Settings** section.



2. To add a new Route, click **New Route**.

NETWORK SETTINGS



3. Specify the following parameters:
- **Routing Entry** - select the IP address type.
 - **Name** – the network connection type.
 - **Destination** - enter the destination IP of the destination host, subnet address, network address, or default route. The destination for a default route is 0.0.0.0.
 - **Netmask** – enter the network mask. This is used in conjunction with the destination to determine when a route is used.
 - **Gateway** – enter the IP address of your Verizon Internet Gateway.

- **Metric** – enter a measurement preference of the route. Typically, the lowest metric is the most preferred route. If multiple routes exist to a specific destination network, the route with the lowest metric is used.
4. Click **Apply** and **Apply changes** to save changes.

Internet Group Management Protocol (IGMP)

IGMP allows for managing a single upstream interface and multiple downstream interfaces of the IGMP/MLD (Multicast Listener Discovery)-based forwarding. This function enables the system to send IGMP host messages on behalf of hosts that the system discovers through standard IGMP interfaces. Also, IGMP snooping allows an Ethernet switch to “listen in” on the IGMP conversation between hosts and routers, while IGMP querier will send out periodic IGMP queries.

To enable this function:

1. Choose the IGMP interfaces by clicking on the check boxes on the screen.
2. Click **Apply changes** to save changes.

DIAGNOSTICS & MONITORING

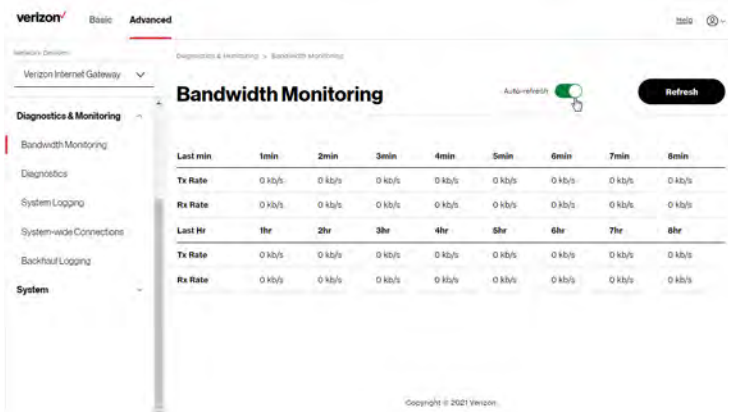
5.2/ DIAGNOSTICS & MONITORING

5.2a/ BANDWIDTH MONITORING

You can view and monitor the recorded bandwidth usage measured in Kbps.

To view the bandwidth:

1. From the **Advanced** menu, select **Diagnostics & Monitoring**.
2. In the **Diagnostics & Monitoring** section, select **Bandwidth Monitoring**.



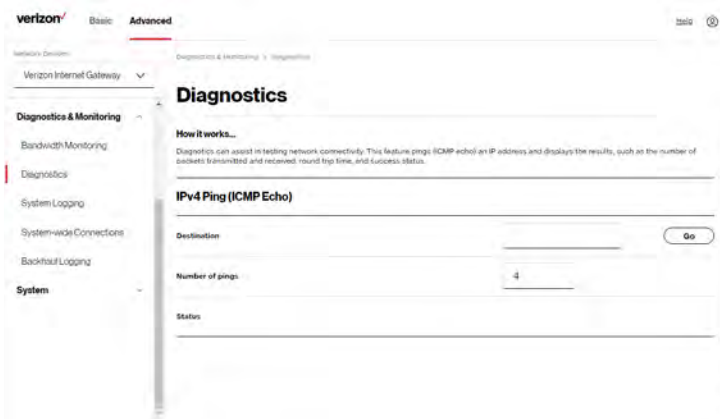
3. To refresh the page, click **Refresh**.
4. To continuously refresh the page, click **Auto-refresh on**.

5.2b/ DIAGNOSTICS

You can use diagnostics to test network connectivity.

To diagnose network connectivity:

1. Select **Diagnostics** in the **Diagnostics & Monitoring** section.
2. To ping an IP address, enter the IP address or domain name in the **Destination** field and click **Go**.



The diagnostics will display the number of pings, status, packets sent, and round trip time.

If no diagnostic status displays, click refresh in your web browser.

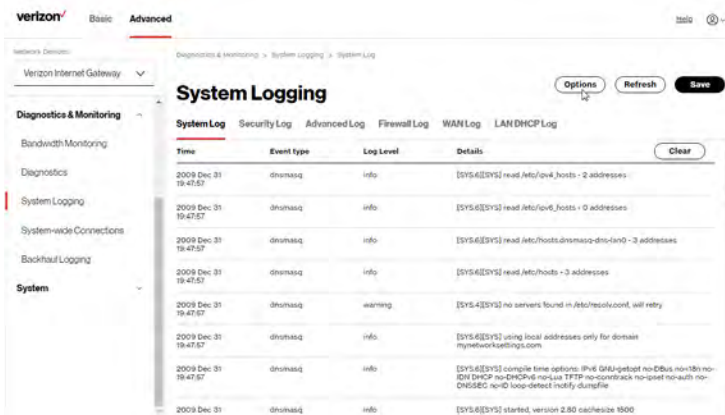
DIAGNOSTICS & MONITORING

5.2c/ SYSTEM LOGGING

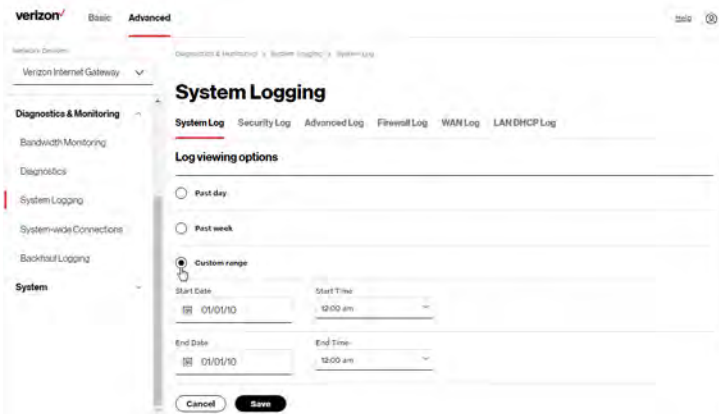
System logging provides a view of the most recent activity of your Verizon Internet Gateway. In addition, you can view additional logs, such as the security, advanced, firewall, WAN DHCP and LAN DHCP.

To view the system log:

1. Select **System Logging** in the **Diagnostics & Monitoring** section.



2. To view a specific time of log event, click on the **Options** button.



3. Select your preferred logging time.
4. Click **Save** to save changes.
5. To view a specific type of log event such as Security Log, WAN DHCP Log, etc., click the appropriate link in the menu on the top.
6. To update the data, click **Refresh**.

5.2d/ SYSTEM-WIDE CONNECTIONS

You can view a summary of the monitored data collected for your Verizon Internet Gateway.

To view your Verizon Internet Gateway's full system status and traffic monitoring data:

1. Select **System-wide Connections** in the **Diagnostics & Monitoring** section.

DIAGNOSTICS & MONITORING

verizon

Basic

Advanced

Networks & Monitoring

System-wide Wi-Fi Connections

Verizon Internet Gateway

System-wide Wi-Fi Connections

Devices

Security & Firewall

Network Settings

Diagnostics & Monitoring

Bandwidth Monitoring

Diagnostics

System Logging

System-wide Connections

Backhaul Logging

System

System-wide Connections

Auto-refresh

Name	Network (Home/Office)	5 GHz Wi-Fi Access Point	2.4 GHz Wi-Fi Access Point	Ethernet
Status	Connected	Disconnected	Disconnected	Connected
Underlying Device	Network (Home/Office)	Network (Home/Office)	Network (Home/Office)	Network (Home/Office)
Connection Type	5 GHz Wi-Fi Access Point	2.4 GHz Wi-Fi Access Point	2.4 GHz Wi-Fi Access Point	Ethernet
MAC Address	00:07:AA:BB:CC:DD	00:07:AA:BB:CC:DD	00:07:AA:BB:CC:DD	00:07:AA:BB:CC:DD
IPv4 Address	192.168.1.1	—	—	—
Subnet Mask	255.255.255.0	—	—	—

verizon

Basic

Advanced

Networks & Monitoring

System-wide Wi-Fi Connections

Verizon Internet Gateway

System-wide Wi-Fi Connections

Devices

Security & Firewall

Network Settings

Diagnostics & Monitoring

Bandwidth Monitoring

Diagnostics

System Logging

System-wide Connections

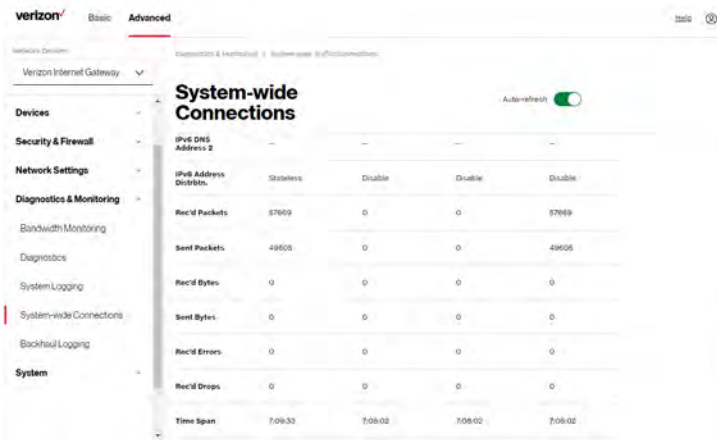
Backhaul Logging

System

System-wide Connections

Auto-refresh

IPv4 Default Gateway	192.168.1.1	—	—	—
IPv4 DNS Address 1	—	—	—	—
IPv4 DNS Address 2	—	—	—	—
IPv4 Address Discovery	DHCP Server	Disable	Disable	Disable
IPv6 Prefix	—	—	—	—
IPv6 Address	—	—	—	—
IPv6 Link-Local Address	—	—	—	—
IPv6 DNS Address 1	—	—	—	—
IPv6 DNS Address 2	—	—	—	—



2. To modify the connection properties, click the individual connection links.
3. To continuously refresh the page, click **Auto-refresh on**.

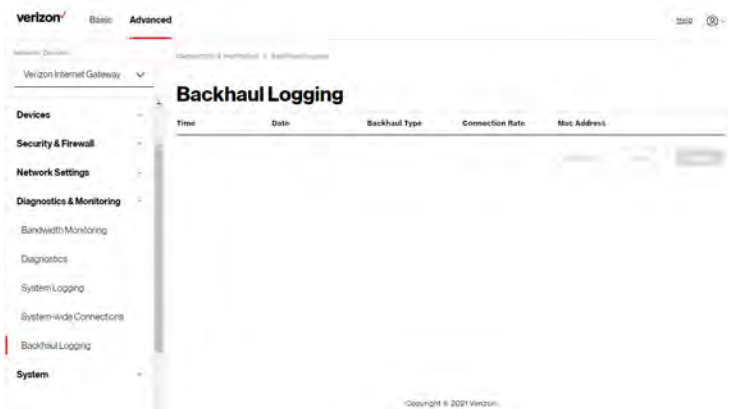
5.2e/ BACKHAUL LOGGING

You can view a summary of the BHM (backhaul modes: Ethernet and Wi-Fi) status of your network.

To view the backhaul modes log:

1. Select **Backhaul Logging** in the **Diagnostics & Monitoring** section.

SYSTEM



- 2. To refresh the page, click **Refresh**.
- 3. To delete the log information, click **Clear**.
- 4. To save the log information, click **Save**.

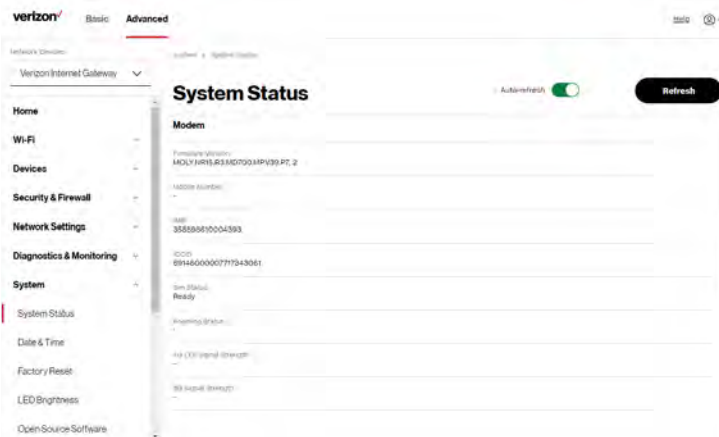
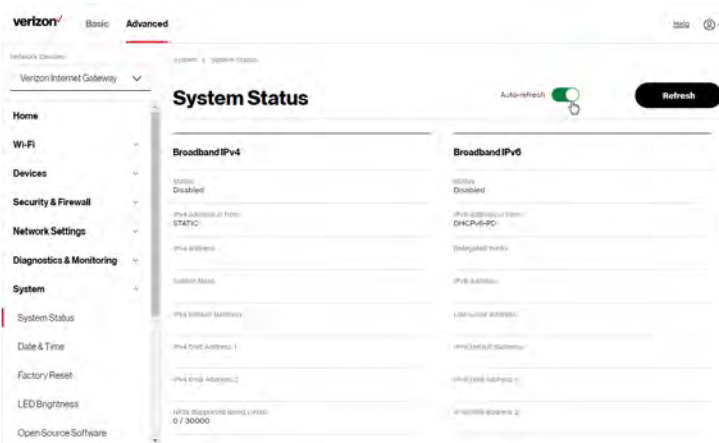
5.3/ SYSTEM

5.3a/ SYSTEM STATUS

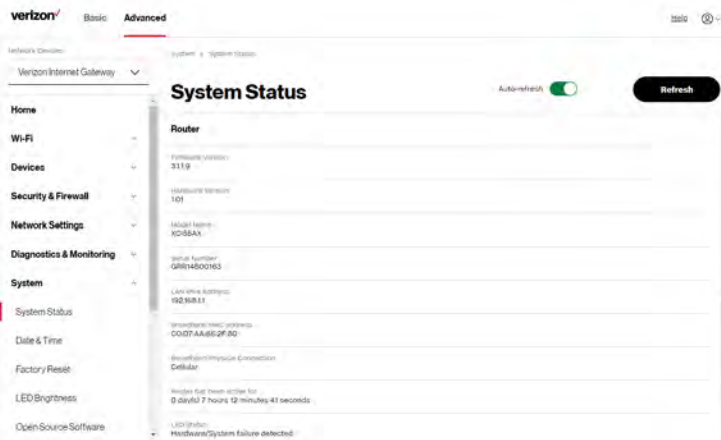
To view the status:

- 1. From the **Advanced** menu, select **System**.
- 2. You can quickly view your Gateway's status by selecting **System Status** in the **System** section.
- 3. To refresh the page, click **Refresh**.
- 4. To continuously refresh the page, click **Auto-refresh on**.

This section displays the status of your Gateway's local network (LAN) and internet connection (WAN), firmware and hardware version numbers, MAC Address, IP settings of Verizon Internet Gateway and extender(s) (if connected).



SYSTEM

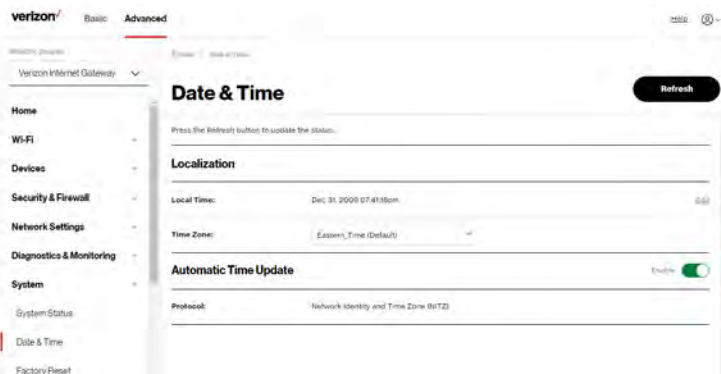


5.3b/ DATE & TIME SETTINGS

You can set the time zone and enable automatic time updates.

To configure the settings:

1. From the **Advanced** menu, select **System**.
2. Select **Date & Time** in the **System** section.



3. Select the local time zone. Your Verizon Internet Gateway automatically detects daylight saving times for selected time zone.
4. In the **Automatic Time Update** section, select the **Enable** check box to perform an automatic time update.
5. To refresh the page, click **Refresh**.

5.3c/ FACTORY RESET

You can use this functionality to save and load configuration files. These files are used to backup and restore the current configuration of your Verizon Internet Gateway.

Only configuration files saved on a specific Verizon Internet Gateway can be applied to that Verizon Internet Gateway. You cannot transfer configuration files between Verizon Internet Gateways.

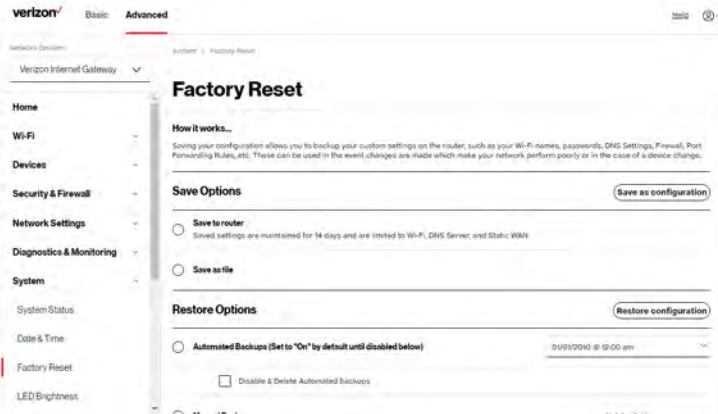
***Warning:** Manually editing a configuration file can cause your Verizon Internet Gateway to malfunction or become completely inoperable.*

Save Options

To save the configuration file:

1. From the **Advanced** menu, select **System**.
2. Select **Factory Reset** in the **System** section.

SYSTEM



3. Select **Save to router** or **Save as file** to save the current configuration, then click **Save as configuration**.
4. If you select **Save as file**, the configuration file is saved to your web browser's download folder.

Restore Options

You can restore your configuration settings to your Verizon Internet Gateway factory default settings. Restoring the default settings erases the current configuration, including user defined settings and network connections. All connected DHCP clients must request new IP addresses. Your Verizon Internet Gateway must restart.

Prior to restoring the factory defaults, you may want to save your current configuration to a file. This allows you to reapply your current settings and parameters to the default settings, as needed.

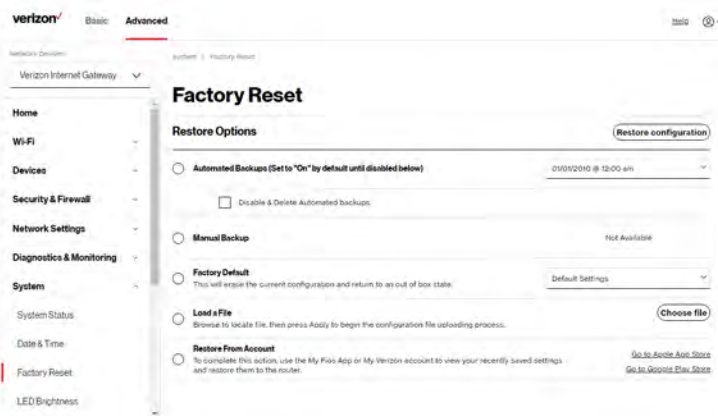
Note: When restoring defaults, the setting and parameters of your Verizon Internet Gateway are restored to their default values. This includes the administrator password. A user-specified password will no longer be valid.

To backup your Verizon Internet Gateway's settings:

1. Select **Factory Reset** in the **System** section.
2. To take a backup of the current settings, click **Automated Backups** or **Manual Backup**. You will be prompted to save a file with the extension “.enc”.
3. Click **Backup** to begin the configuration backup process.

To restore your Verizon Internet Gateway's factory default settings:

1. Select **Factory Reset** in the **System** section.
2. Click **Factory Default**.



SYSTEM

- **Default Settings** – will erase all router settings including user settings for SSID and Passwords.
 - **Default Settings except current user settings** – will erase all router settings but will retain the user settings for SSID and passwords.
3. Click **Restore configuration** button. The factory default settings are applied and your Verizon Internet Gateway restarts. Once complete, the Login page for the First Time Easy Setup Wizard displays.

To load the configuration file:

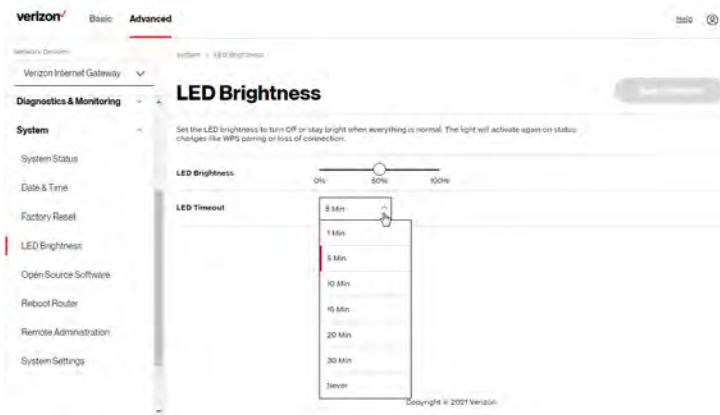
1. Select **Factory Reset** in the **System** section.
2. To load a previously saved configuration file, select **Load a File** then click **choose file**.
3. Browse to the location of the file, and click **Restore configuration** button to begin the configuration uploading process.
4. Accessing the **My Fios** app or the **My Verizon** account also allows you to restore the previously saved settings. Click **Restore From Account** and select **Go to Apple App Store/ Go to Google Play Store** to restore the saved settings to the Gateway.
5. Click **Restore configuration** button. Your Verizon Internet Gateway will automatically restart with that configuration.

5.3d/ LED BRIGHTNESS

The Verizon Internet Gateway allows you to set the LED brightness to turn Off (0%) or stay bright (50% or 100%) using the user interface.

To control the LED brightness:

1. Select **LED Brightness** in the **System** section.

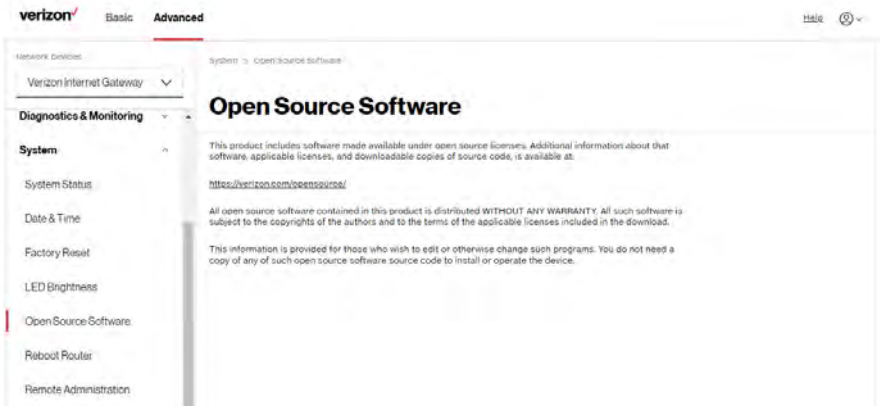


2. Slide the bar to adjust the brightness of the LED.
3. Select your preferred timeout period (in minutes) from the dropdown list for the LED dimming setting. The Status LED will automatically turn off after the timeout period.
4. Click **Apply changes** to save changes.

Note: *The light will activate again on status changes like WPS pairing or loss of connection.*

SYSTEM

5.3e/ OPEN SOURCE SOFTWARE



To view: From the **Advanced** menu, select **System** from the left pane and then click **Open Source Software**.

5.3f/ REBOOT VERIZON INTERNET GATEWAY

Warning: Only select *Reboot Router* if instructed to do so by Verizon support.

You can reboot your Verizon Internet Gateway using the Reboot Router Only feature. Refer to 1.1a/ Reset Button for power button options.

To reboot your Verizon Internet Gateway using the user interface:

1. Select **Reboot Router** in the **System** section.



2. To reboot, click **Reboot Device**. Your Gateway will reboot. This may take up to a minute.
3. To access your Verizon Internet Gateway user interface, refresh your web browser.
4. After the Status LED on the front panel turns solid white, you will automatically be sent to the web browser login page.

5.3g/ REMOTE ADMINISTRATION

Caution: *Enabling Remote Administration places your Verizon Internet Gateway network at risk from outside attacks.*

You can access and control your Verizon Internet Gateway not only from within the local network, but also from the internet using **Remote Administration**.

SYSTEM

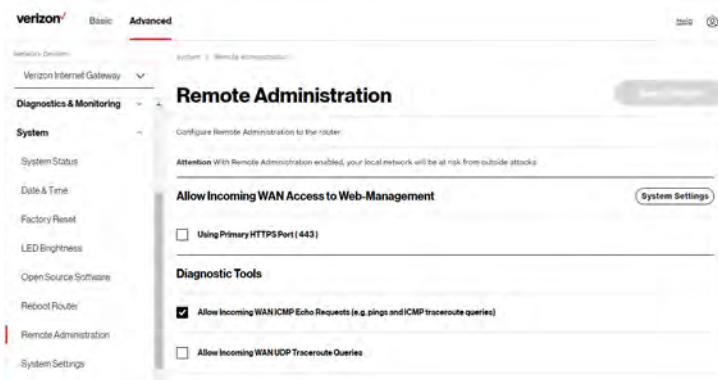
You can allow incoming access to the following:

- **Allow Incoming WAN Access to Web-Management** - used to obtain access to your Verizon Internet Gateway's UI and gain access to all settings and parameters through a web browser.
- **Diagnostic Tools** - used for troubleshooting and remote system management by a user or Verizon.

Web Management remote administration access may be used to modify or disable firewall settings. Web Management services should be activated only when absolutely necessary.

To enable remote administration:

1. Select **Remote Administration** in the **System** section.



2. To enable access, select the check box.
3. To remove access, clear the check box.
4. Click **Apply changes** to save changes.

5.3h/ SYSTEM SETTINGS

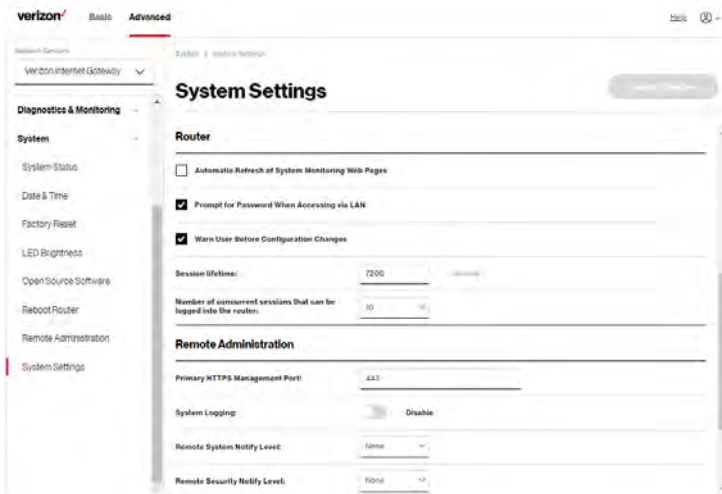
You can configure various system and management parameters.

To configure system settings:

1. Select **System Settings** in the **System** section.

The screenshot shows the Verizon Internet Gateway web interface. The top navigation bar includes the Verizon logo, 'Basic', and 'Advanced' tabs. The left sidebar lists various system settings under the 'System' section, with 'System Settings' highlighted. The main content area is titled 'System Settings' and contains three sections: 'Router Status' with fields for 'Router's Hostname' (NDSAX) and 'Local Domain' (myverizon.com); 'User Settings' with fields for 'User name' (Admin), 'Set new password', 'Refresh new password', and 'Unsuccessful Login Attempts' (10); and a 'Router' section with a checkbox for 'Automatic Refresh of System Monitoring Web Pages'.

SYSTEM



2. In the **Router Status** section, configure the following:
 - **Router's Hostname** – enter the host name of your Verizon Internet Gateway.
 - **Local Domain** – view the local domain of the network.
 - **Location** – select your current location of the Gateway from the dropdown list.
3. In the **User Settings** section, you can view the administration user that can currently access your Wi-Fi network. In addition, you can modify the login password and manage the number of unsuccessful login attempts the administration user can enter before your Verizon Internet Gateway temporarily denies all further login attempts by the user.

-
4. In the **Router** section, configure the following by selecting the check box:
 - **Automatic Refresh of System Monitoring Web Pages** – activates the automatic refresh of system monitoring web pages.
 - **Prompt for Password when Accessing via LAN** – causes your Verizon Internet Gateway to ask for a password when trying to connect to the network.
 - **Warn User Before Configuration Changes** – activates user warnings before network configuration changes take effect.
 - In the **Session Lifetime** field, specify the length of time required before re-entering the login password after your Verizon Internet Gateway has been inactive.
 - In the **Number of concurrent sessions that can be logged into the router** field, select the number of users that can access your Verizon Internet Gateway at the same time.
 5. In the **Remote Administration** section, configure the following:
 - Enter the **Primary HTTP Management Port**.
Refer to 5.3g Remote Administration for using this feature.
 - In the **System Logging** section move the selector to **on** to activate system logging.

SYSTEM

- **Remote System Notify Level** – specify the type of information, such as none, error, warning, and information, received for remote system logging.
- **Remote Security Notify Level** – specify the type of information, such as none, error, warning, and information, received for remote system logging.
- In the **DHCP Timeout** section, specify the DHCP timeout.

6. Click **Apply changes** to save changes.

06 /

TROUBLE SHOOTING

6.0 Troubleshooting Tips

6.1 Frequently Asked Questions

This chapter lists solutions for issues that may be encountered while using your Verizon Internet Gateway as well as frequently asked questions.

Although the majority of the Verizon Internet Gateway's internet connectivity is automatic and transparent, if an issue does occur accessing the internet (e.g. complete loss of connectivity, inability to access services, etc.), you may need to take additional steps to resolve the problem.

TROUBLESHOOTING TIPS

***Note:** The advanced settings should only be configured by experienced network technicians to avoid adversely affecting the operation of your Verizon Internet Gateway and your local network.*

6.0/ TROUBLESHOOTING TIPS

6.0a/ IF YOU ARE UNABLE TO CONNECT TO THE INTERNET:

- The first thing to check is whether your Verizon Internet Gateway is powered on and is connected to the internet. Check the Status LED on the front of the Verizon Internet Gateway. Be sure to refer to the “1.1c/ LED” on page 7 to determine status of the Verizon Internet Gateway. Check the WAN cable connecting your Verizon Internet Gateway to the internet to make sure it is properly connected on both ends.
- If the prior tips do not resolve your connection issue, try restarting (rebooting) the Gateway portion of the Verizon Internet Gateway by manually pressing the reset power button on the bottom panel of the Verizon Internet Gateway for 3+ seconds (the Status LED should go off) to begin rebooting your Verizon Internet Gateway. Your Verizon Internet Gateway will begin rebooting and will return to service in 3 - 5 minutes depending on your network connection. Check Status LED and if it is solid white, try again to access the internet.
- If rebooting your Gateway does not resolve your connection issue, try power cycling the Verizon Internet Gateway by unplugging the power cord from the power supply and wait 2 minutes. During the 2 min. wait period, also power cycle the

network device (e.g. the computer, tablet, etc.) and then plug the power cable back into the Verizon Internet Gateway. After 3-5 minutes, recheck the Status LED and try again to access the internet.

6.0b/ IF YOU ARE UNABLE TO CONNECT TO YOUR VERIZON INTERNET GATEWAY USING WI-FI:

- Be sure your Wi-Fi device is within range of your Verizon Internet Gateway; move it closer to see if your connection improves.
- Check your network device's Wi-Fi settings to be sure your device's Wi-Fi is on (enabled) and that you have the correct Wi-Fi network and password (if using a Wi-Fi password) as configured on your Verizon Internet Gateway.
- Be sure you are connecting to the correct Wi-Fi network; check to be sure you are using your Verizon Internet Gateway's SSID. In some cases, if using a Wi-Fi password, you may need to enter the Wi-Fi password into your network device again to be sure your device accepts the password.
- Check to be sure you are running the latest software for your network device.
- Try turning your network device's Wi-Fi off and on, and try to connect.

TROUBLESHOOTING TIPS

- If you have made any changes in your network settings and turning your network device's Wi-Fi off and on does not help, try to restart your network device.
- You may need to turn the Wi-Fi settings from on to off, and back to on again and apply the changes.
- If you are still unable to access your Verizon Internet Gateway, you may need to try connecting to the Verizon Internet Gateway using another network device. If the issue goes away with another network device, the issue is likely with that individual network device's configuration.

6.0c/ ACCESSING YOUR VERIZON INTERNET GATEWAY IF YOU ARE LOCKED OUT

- If your Verizon Internet Gateway connection is lost while making configuration changes, a setting that locks access to your Verizon Internet Gateway's UI may have inadvertently been activated.

The common ways to lock access to your Verizon Internet Gateway are:

- Scheduler - If a schedule has been created that applies to the computer over the connection being used, your Verizon Internet Gateway will not be accessible during the times set in the schedule.
- Access Control - If the access control setting for the computer is set to block the computer, access to your Verizon Internet Gateway is denied.

To gain access, restore the default settings to your Verizon Internet Gateway.

6.0d/ RESTORING YOUR VERIZON INTERNET GATEWAY'S DEFAULT SETTINGS

There are two ways to restore your Verizon Internet Gateway's default settings. It is important to note that after performing either procedure, all previously save settings on your Gateway will be lost.

For additional information regarding the Restore Defaults feature, refer to section 5.3c/ Factory Reset/Restore Options.

- Using the tip of a ballpoint pen or pencil, press and hold the Reset button on the bottom of your Verizon Internet Gateway for over three seconds.
- Access the UI and navigate to the Advanced Settings page. Select the 5.3c/ Factory Reset option. After saving your configuration, if desired, click the Factory Default radio button. For additional details, refer to the 5.3c/ Factory Reset/Restore Options section of this guide.

Note: *If you reset or reboot your Verizon Internet Gateway, you may also need to disconnect your Verizon Internet Gateway's power supply for a few minutes (3 or more) and then reconnect the power cable.*

TROUBLESHOOTING TIPS

6.0e/ LAN CONNECTION FAILURE

To troubleshoot a LAN connection failure:

- Verify your Verizon Internet Gateway is properly installed, LAN connections are correct, and that the Verizon Internet Gateway and communicating network devices are all powered on.
- Confirm that the computer and Verizon Internet Gateway are both on the same network segment.

If unsure, let the computer get the IP address automatically by initiating the DHCP function, then verify the computer is using an IP address within the default range of 192.168.1.2 through 192.168.1.254. If the computer is not using an IP address within the correct IP range, it will not connect to your Verizon Internet Gateway.

- Verify the subnet mask address is set to 255.255.255.0.

6.0f/ TIMEOUT ERROR OCCURS WHEN ENTERING THE URL OR IP ADDRESS

Verify the following:

- All computers are working properly.
- IP settings are correct.
- Verizon Internet Gateway is on and connected properly.
- Verizon Internet Gateway settings are the same as the computer.

For connections experiencing lag or a slow response:

- Check for other devices on the network utilizing large portions of the bandwidth and if possible temporarily stop their current utilization and recheck the connection.
- If lag still exists, clear the cache on the computer and if still needed, unplug the Ethernet cable or disable the Wi-Fi connection to the computer experiencing the slow connection and then reconnect or enable the Wi-Fi connection and try the connection again.

In rare cases you may also need to:

- Unplug the Ethernet cable to Verizon Internet Gateway and restart the Verizon Internet Gateway, wait 1-2 mins. and insert the Ethernet cable again.
- Under limited circumstances you may use a port forwarding configuration on the router, based on the application you are using (refer to the 5.0e/ Port Forwarding section or Verizon's support online help for more details).

TROUBLESHOOTING TIPS

6.0g/ FRONT LED AND WPS BUTTON

Front LED Mode	Status	LED Pattern
Bootup	System Off	Off
	System Booting	Soft blink White
	Firmware update (FOTA)	Fast blink white
Cellular signal (or after single click pair button)	Passing signal	Solid White
	No Signal, Cold SIM	Solid Red
	No SIM Card	Hard blink red
Regular usage	Setup complete	50% bright White
	WiFi disabled by user	Solid Green
Paring	WPS Paring	Hard blink Blue
Other	Factory Reset	Fast blink yellow
	FW Error	Soft blink red

The rear panel's WPS Button allows quick access to the Wi-Fi Protected Setup (WPS) feature and handset paging/paring mode. In addition, the WPS Button provides a visual display of the Verizon Internet Gateway's current condition. Refer to the chart above for details.

6.0h/ BOTTOM LIGHTED INDICATORS

Ethernet Port LED Mode	Status	Left LED	Right LED
Wired LAN connection * Threshold level can be decided based on port capability	Ethernet > 100M* Link	Off	Solid White
	Ethernet > 100M* Activity	Off	Blinking White
	Ethernet < 100M* Link	Solid Yellow	Off
	Ethernet < 100M* Activity	Blinking Yellow	Off
	No Ethernet connection	Off	Off

6.1/ FREQUENTLY ASKED QUESTIONS

6.1a/ I'VE RUN OUT OF ETHERNET PORTS ON MY VERIZON INTERNET GATEWAY. HOW DO I ADD MORE COMPUTERS OR DEVICES?

Plugging in an Ethernet hub or switch expands the number of ports on your Verizon Internet Gateway.

- Run a straight-through Ethernet cable from the Uplink port of the new hub to the Verizon Internet Gateway.

FREQUENTLY ASKED QUESTIONS

Use a crossover cable if there is no Uplink port/switch on your hub, to connect to the Verizon Internet Gateway.

- Remove an existing device from the Ethernet port on your Verizon Internet Gateway and use that port.

6.1b/ HOW DO I CHANGE THE PASSWORD ON MY VERIZON INTERNET GATEWAY UI?

To change the password:

1. On the main screen, select **Advanced**, then select **System Settings** in the **System** section.
2. In the **User Settings** section, set a new password.

6.1c/ IS THE WI-FI OPTION ON BY DEFAULT ON MY VERIZON INTERNET GATEWAY?

Yes, your Verizon Internet Gateway's Wi-Fi option is activated out of the box.

6.1d/ IS THE WI-FI SECURITY ON BY DEFAULT WHEN THE WI-FI OPTION IS ACTIVATED?

Yes, with the unique WPA2 (Wi-Fi Protected Access II) key that is printed on the sticker on the bottom of your Verizon Internet Gateway.

6.1e/ ARE MY VERIZON INTERNET GATEWAY'S ETHERNET PORTS AUTO-SENSING?

Yes. Either a straight-through or crossover Ethernet cable can be used.

6.1f/ CAN I USE AN OLDER WI-FI DEVICE TO CONNECT TO MY VERIZON INTERNET GATEWAY?

Yes, your Verizon Internet Gateway can interface with 802.11b, g, n, ac or ax devices. Your Verizon Internet Gateway also can be setup to handle only n Wi-Fi cards, g Wi-Fi cards, b Wi-Fi cards, or any combination of the three.

6.1g/ CAN MY WI-FI SIGNAL PASS THROUGH FLOORS, WALLS, AND GLASS?

The physical environment surrounding your Verizon Internet Gateway can have a varying effect on signal strength and quality. The denser the object, such as a concrete wall compared to a plaster wall, the greater the interference. Concrete or metal reinforced structures experience a higher degree of signal loss than those made of wood, plaster, or glass.

FREQUENTLY ASKED QUESTIONS

6.1h/ HOW DO I LOCATE THE IP ADDRESS THAT MY COMPUTER IS USING?

In Windows 8 or Windows 10, click the Windows button and select **Settings**, then click **Network & Internet** and **Status**. Click **View your network properties** for details of IP address.

On Mac OS X, open System Preferences and click the Network icon. The IP address displays near the top of the screen.

To find the IP address from the router GUI:

1. From the **Basic** menu, select **Devices** from the left pane.
2. Click the Settings icon to access the **Device Settings** page for that device to view detailed IP address information for the device.

6.1i/ I USED DHCP TO CONFIGURE MY NETWORK. DO I NEED TO RESTART MY COMPUTER TO REFRESH MY IP ADDRESS?

No. In Windows 8, Windows 10 and Mac OSX, unplug the Ethernet cable or Wi-Fi card, then plug it back in.

6.1j/ I CANNOT ACCESS MY VERIZON INTERNET GATEWAY UI. WHAT SHOULD I DO?

If you cannot access the UI, verify the computer connected to your Verizon Internet Gateway is set up to dynamically receive an IP address.

6.1k/ I HAVE A FTP OR WEB SERVER ON MY NETWORK. HOW CAN I MAKE IT AVAILABLE TO USERS ON THE INTERNET?

For a web server, enable port forwarding for port 80 to the IP address of the server. Also, set up the web server to receive that port. Configuring the server to use a static IP address is recommended.

For a FTP server, enable port forwarding for port 21 to the IP address of the server. Also, set up the web server to receive that port. Configuring the server to use a static IP address is recommended.

6.1l/ HOW MANY COMPUTERS CAN BE CONNECTED THROUGH MY VERIZON INTERNET GATEWAY?

Your Verizon Internet Gateway is capable of 254 connections, but we recommend having no more than 132 connections. As the number of connections increases, the available speed for each computer decreases.

07 /

SPECIFICATIONS

7.0 General Specifications

7.1 Connections

The specifications for your Verizon Internet Gateway are as follows.

This includes standards, cabling types and environmental parameters.

GENERAL SPECIFICATIONS

Note: The specifications listed in this chapter are subject to change without notice.

7.0/ GENERAL SPECIFICATIONS

Model Number:	ARC-XCI55AX
Technical Standard:	LTE Category 18, 5G NR Sub 6
Frequency band:	LTE Band: B2/B5/B13/B48/B66, DL 4x4 MIMO 5G Band: 256 QAM, DL 4x4 MIMO n2/n5/n48/n66/n77
Wi-Fi Standard:	802.11 a/b/g/n/ac/ax
Dimensions:	130mm x 136mm x 130mm (L x W x H)
Certifications:	FCC, UL 60950-1
Operating Temperature:	5° C to 40° C (41° F to 104° F)
Storage Temperature:	-5° C to 50° C (23° F to 122° F)
Operating Humidity:	5% to 85%
Storage Humidity:	5% to 93% (non-condensing)

7.1/ CONNECTIONS

DC Input: source adapter: 12V/ 3.5A

Ethernet: RJ-45 LAN * 2

08 /

NOTICES

8.0 Regulatory Compliance Notices

This chapter lists various compliance and modification notices, as well as the NEBS requirements and GPL.

REGULATORY COMPLIANCE NOTICES

8.0/ REGULATORY COMPLIANCE NOTICES

8.0a/ Class B Equipment

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

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

FCC Caution: Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

FCC regulations restrict the operation of this device to indoor use only.

RF Exposure:

To comply with FCC RF exposure compliance requirements, the antenna used for this transmitter must be installed to provide a separation distance of at least 28cm from all persons (indoor), and must not be co-located or operating in conjunction with any other antenna or transmitter.

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.

8.0b/ Safety Warning:

1. The circuit of cable distribution system under consideration is TNV-1 circuit.
2. The common sides or earthed side of the circuit are connected to the screen of the coaxial cable through an antenna connector of tuner and to all accessible parts and circuits (SELV, LCC and accessible metal parts).
3. The screen of the coaxial cable is intended to be connected to earth in the building installation.

REGULATORY COMPLIANCE NOTICES

8.0c/ Alerte de sécurité:

1. Le circuit de distribution par câble considéré est le circuit TNV-1.
2. Les côtés communs ou côté terre du circuit sont connectés à l'écran du câble coaxial via un connecteur d'antenne du syntoniseur et à toutes les parties et circuits accessibles (SELV, LCC et parties métalliques accessibles).
3. L'écran du câble coaxial est destiné à être mis à la terre dans l'installation du bâtiment.

The cable distribution system should be grounded (earthed) in accordance with ANSI/NFPA 70, the National Electrical Code (NEC), in particular Section 820.93, Grounding of Outer Conductive Shield of a Coaxial Cable.

Le système de distribution par câble doit être mis à la terre conformément à ANSI / NFPA 70, Code national de l'électricité (NEC), en particulier à la section 820.93, Mise à la terre du blindage conducteur extérieur d'un câble coaxial.

8.0d/ NEBS (Network Equipment Building System) Statement

An external SPD is intended to be used with ARC-XCI55AX.

WARNING: The intra-building ports of the equipment or subassembly is suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port(s) of the equipment or subassembly **MUST NOT** be metallically connected to

interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 4 ports as described in GR-1089) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.

***Caution:** The Verizon Internet Gateway must be installed inside the home. The Router is not designed for exterior installation.*

8.0e/ GENERAL PUBLIC LICENSE

This product includes software made available under open source licenses. Additional information about that software, applicable licenses, and downloadable copies of source code, is available at:

<https://verizon.com/opensource/>

All open source software contained in this product is distributed WITHOUT ANY WARRANTY. All such software is subject to the copyrights of the authors and to the terms of the applicable licenses included in the download.

This information is provided for those who wish to edit or otherwise change such programs. You do not need a copy of any of such open source software source code to install or operate the device.