User Guide

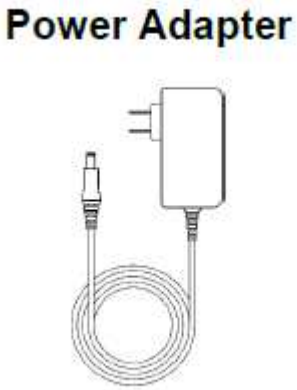
Verizon Internet Gateway

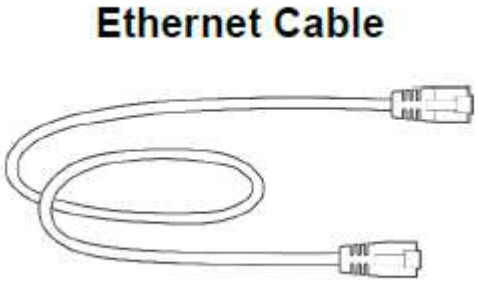
1. Inside the box

Inside the product package you should find the following items:

1) LTE Home router
2) Power adapter
3) Ethernet cable

Contact Verizon if any item is missing or damaged.





2. Your 5G NR Home Router

Front:

The logo, LED indicator

LEDs

The LEDs indicate the system and connection status, and WPS activity.

Mode	Status	LED1 Pattern	Indication Duration
Bootup	System Off	Off	--
	System Booting	Soft blink White	Show until device is ready to show signal status
	Firmware update (FOTA)	Fast blink white	Show only while firmware is being installed or before FOTA reboot for 1~2 seconds
LTE/Sub6 indication (or after single click pair button)	Passing signal	Solid White	Show after device is ready If the device has passing signal
	No Signal	Solid Red	Show after device is ready If the device has no signal
	No SIM Card	Hard blink red	If device has removable sim, then the device needs to show 'no sim' indication
Regular usage	Setup complete	50% bright White	Lower the brightness after 5 minutes of getting passing signal
	WiFi disabled by user	Solid Green	Show if user disables WiFi through settings, but device is still has passing signal
Pairing	WPS Pairing	Hard blink Blue	Show for 2 minutes (time-out) after WPS button press or until pairing is complete
Other	Factory Reset	Fast blink yellow	Show only for 2~3 seconds after pressing hard-reset button until device restarts
	FW Error	Soft blink red	Show while device has fatal error that makes it stop working

Back:

WPS Button

Bottom:

DC Jack, 2 x LAN Ethernet ports, SIM card slot, Reset button

Reset Button

Slide the needle tool into the hole and push the reset button for more than **3 seconds** to perform a factory reset (resets all settings back to factory defaults)

WPS

Press the WPS button on the button of the router to activate WPS. WPS is an easy way to add Wi-Fi devices to your network. Refer to **Wi-Fi Settings > WPS** for more information.

3. Setting Up Your 5G NR Home Router

Disconnect any existing router from your network before installation.

1. Plug the router into a power outlet with the included power adapter.

2. Wait for a couple of minutes for the router to power up, and then go to **4. Login to your LTE Home Router** to login to your router and configure settings such as Wi-Fi security.

3.1 Positioning your router

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

- Place the router in a central area.
- Keep the router away from metal obstructions and away from direct sunlight.
- Keep the router 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.

3.2 Setup requirements

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

- Ethernet RJ-45 (LAN) port (10Base-T/100Base-TX/1000BaseTX)
- IEEE 802.11a/b/g/n/ac/ax wireless capability
- An installed TCP/IP service
- Web browser such as Internet Explorer, Firefox, Safari, or Google Chrome

4. Login to Your Home Router

You can configure your router’s network settings by computer or mobile app, using the Web User Interface (Web UI).

First connect to your router, then access the Web UI, as shown below. Your router is pre-set with WPA2 security, but it’s recommended to immediately change the default Wi-Fi password, as well as the Web UI login password.

4.1 Connect by Mobile App

1. Scan available Wi-Fi networks with your mobile device:

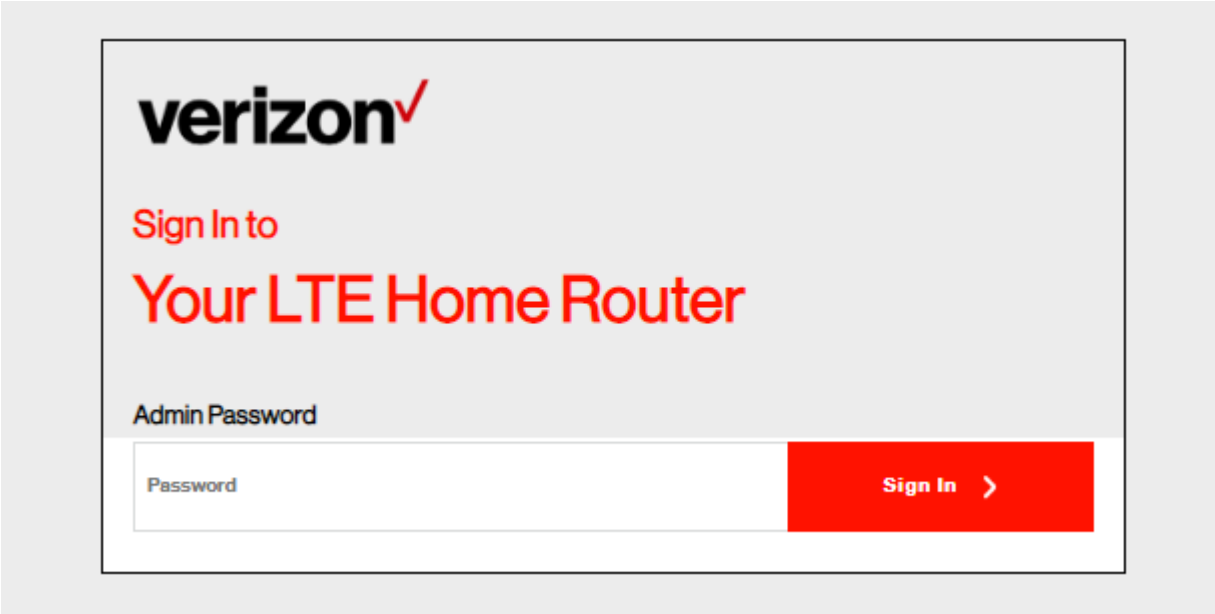
2. Select either of the networks named:

Verizon_xxxxxx

3. Enter your password, which can be found on your router’s product label.

Login to the Web User Interface

1. Open the Verizon router App.
2. Log in using the default username: **admin** and password: **admin**



3. Go to **Wi-Fi Settings** to change your Wi-Fi password and **Device Settings > Admin Password** to change your Web UI login password, and remember to save your settings.
4. Check **5. Web User Interface** in this guide for more information about your router's settings.

4.2 Connect by computer

1. Scan available Wi-Fi networks with your computer.

2. Select either of the networks named:

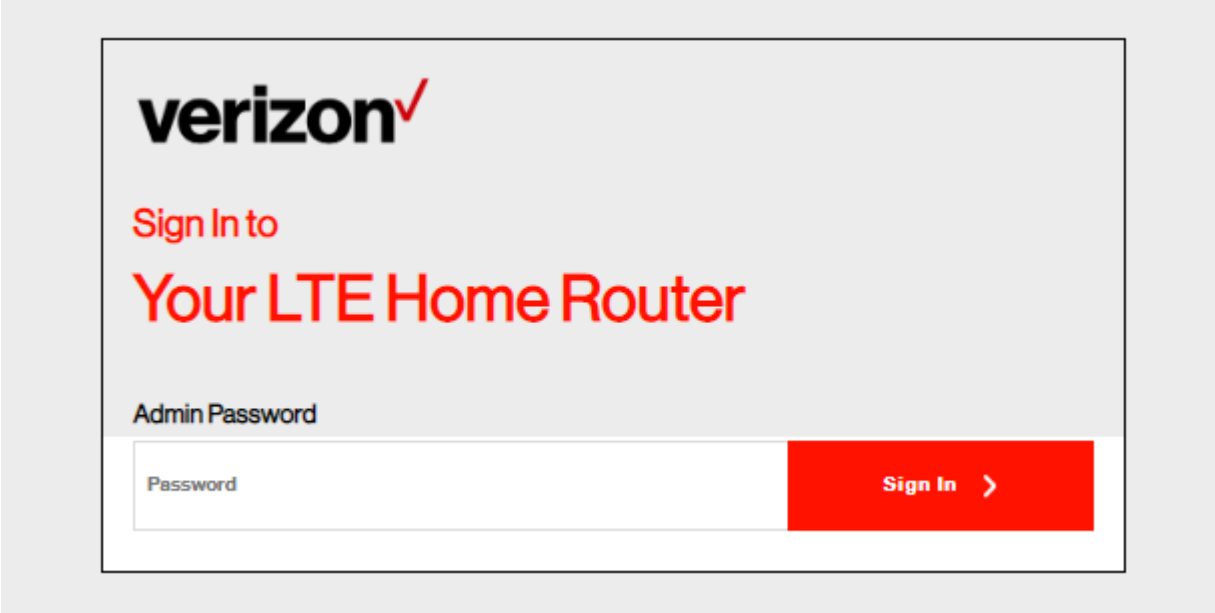
   Verizon_xxxxxx

3. Enter your password, which can be found on your router’s product label

4. If preferred, you can use an Ethernet cable to connect your computer to the router’s LAN port for configuration (instead of Wi-Fi). Simply connect the two devices’ LAN ports by Ethernet cable.

Login to the Web User Interface

1. Open a web browser and enter the router's default address **http://192.168.0.1** in the address bar.
2. Log in to the Web UI using the default username: **admin** and password: **admin**



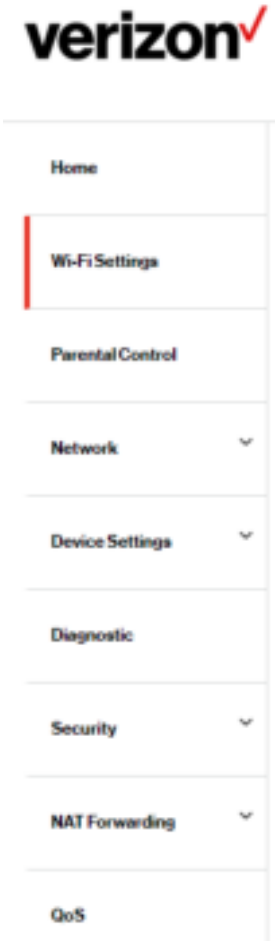
3. Go to **Wi-Fi Settings** to change your Wi-Fi password and **Device Settings > Admin Password** to change your Web UI login password, and remember to save your settings.
4. Check **5. Web User Interface** in this guide for more information about your router's settings.

5. Web User Interface

Your router's Web User Interface (Web UI) allows you to setup and configure its various functions.

Menu

Use the left side menu to navigate:



Save

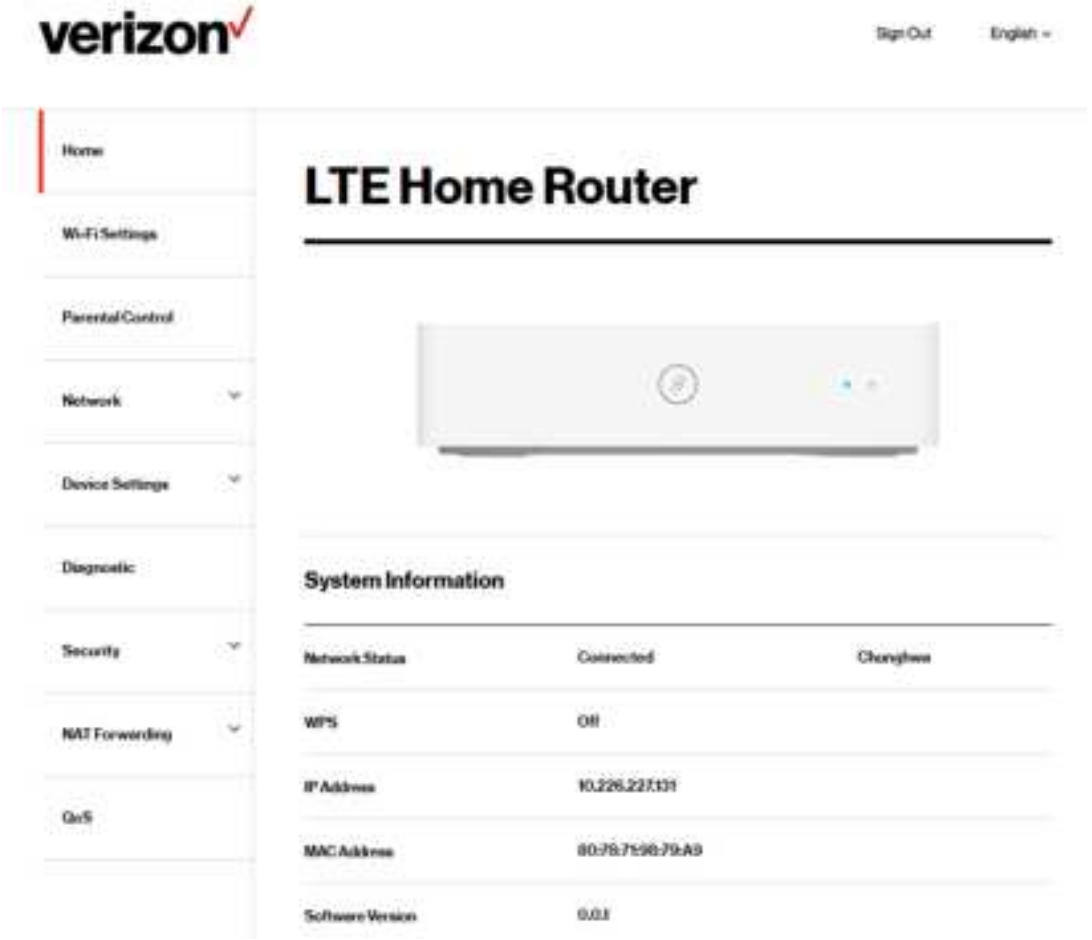
Remember to save your settings with the save button after making changes.

5.1 Home

> Home

The Home page shows a snapshot of your network status and key system information.

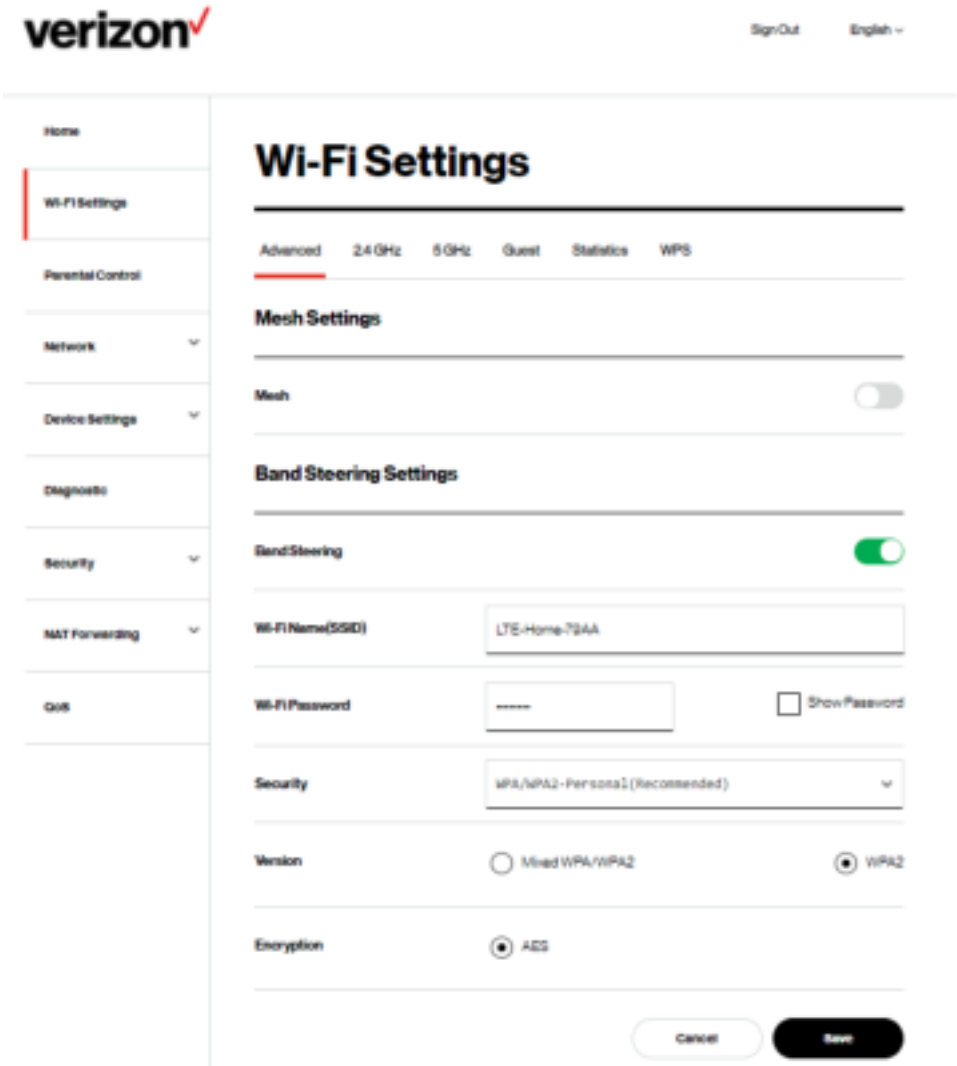
Network Status should display **Connected** to indicate an LTE connection. If you don't see this, check the router's LEDs and refer to **Troubleshooting** to diagnose the problem.



System Information	
Network Status	Displays the MAC address of your router. A MAC Address is a unique fixed identifier for any device on a network.
WPS	Specify the IP address here. This IP address will be assigned to your router and will replace the default IP address.
IP Address	Specify a subnet mask. The default value is 255.255.255.0
MAC Address	Displays the MAC address of your router. A MAC Address is a unique fixed identifier for any device on a network.
Software Version	Displays the current software version your router is running.

5.2 Wi-Fi Settings

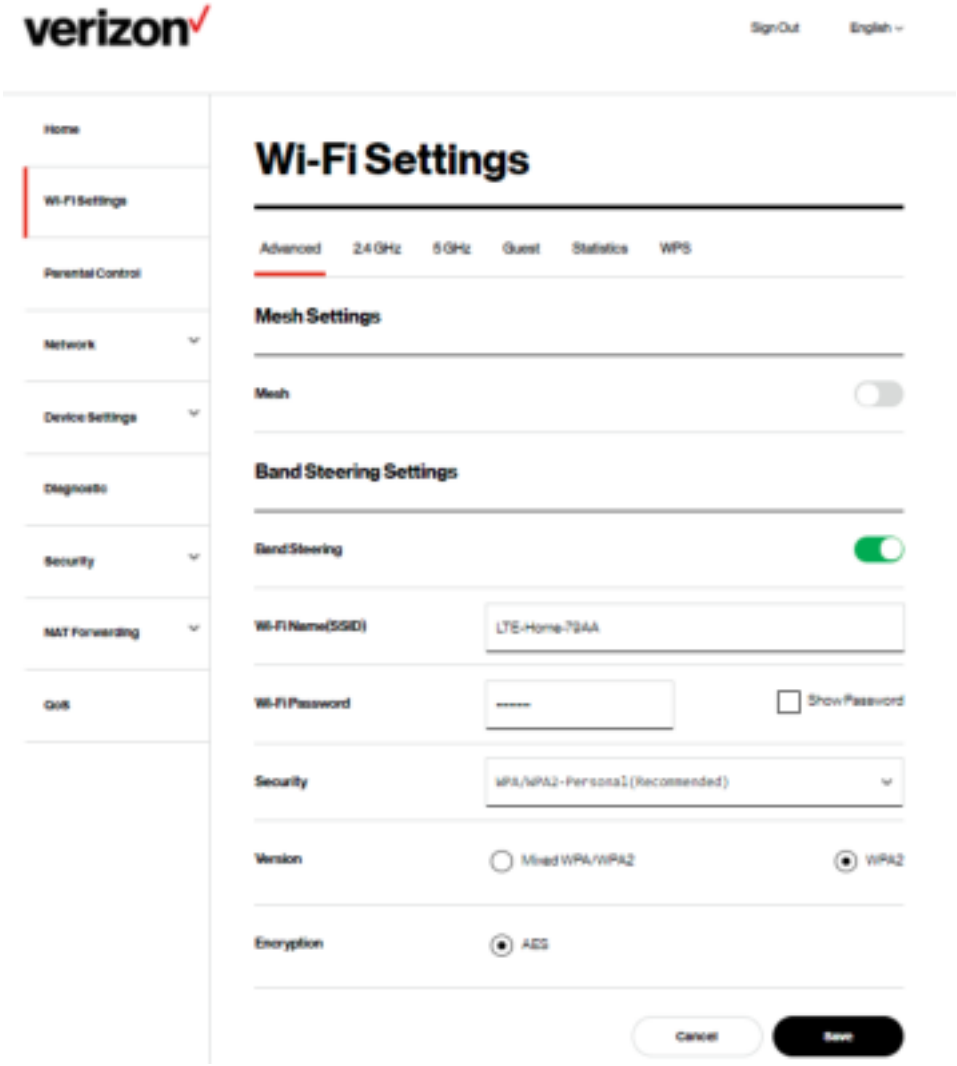
The **Wi-Fi Settings** screen displays advanced settings for your router's Wi-Fi.



Advanced

Wi-Fi Settings > Advanced

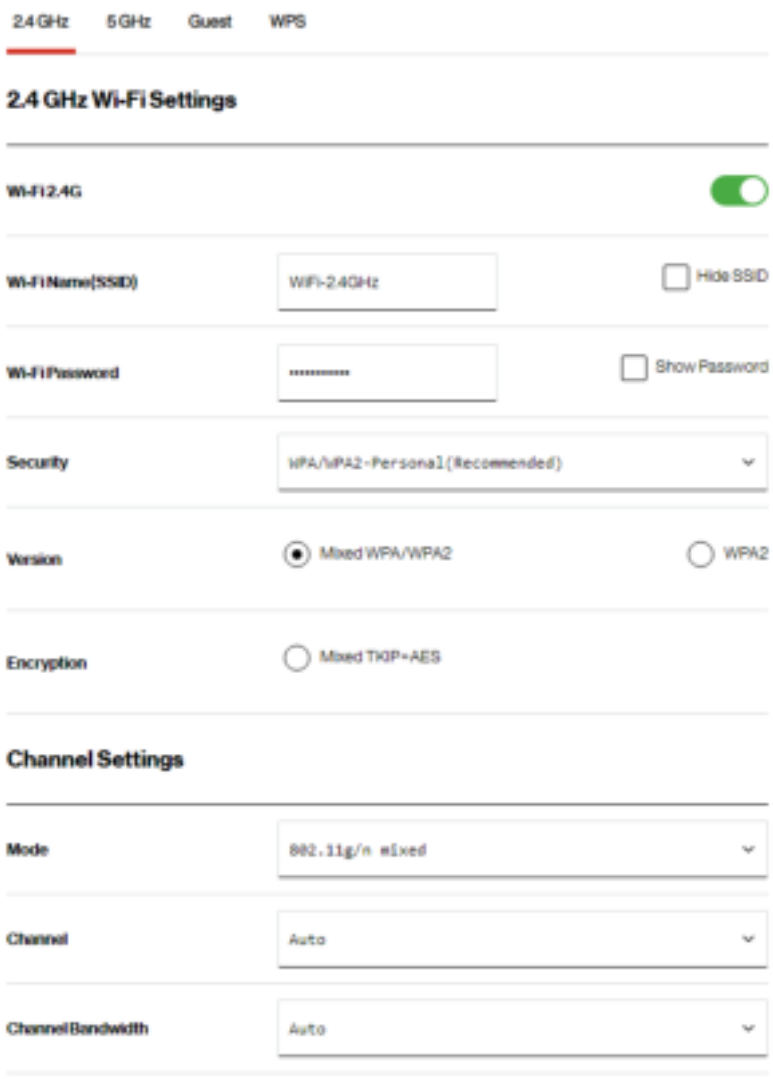
The **advanced page including the Mesh and Band Steering settings**. You can enable the Mesh function to connect the other RE devices easily. The Band Steering function is default enable. It can detect clients capable of 5 GHz operation and steers them to that frequency which leaves the more crowded 2.4 GHz band available for legacy clients.



2.4GHz / 5GHz

Wi-Fi Settings > 2.4GHz / 5GHz

The router is dual-band and uses two Wi-Fi frequencies (2.4GHz & 5GHz) for better wireless performance on your devices. You can edit advanced settings for 2.4GHz or 5GHz frequency bands by selecting the respective tab. Please be noted, if the Band steering is enabled, you cannot edit the settings in the 2.4GHz or 5GHz page individually.



2.4 / 5 GHz Wi-Fi Settings	
Wi-Fi 2.4GHz/5GHz	Toggle to enable or disable this Wi-Fi frequency.
Wi-Fi Name (SSID)	This is the name of your Wi-Fi network for identification, also sometimes referred to as “SSID”. The SSID can consist of any combination of up to 32 alphanumerical characters.
Hide SSID	Check the box to hide your SSID. When hidden, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden SSID is typically more secure than a visible SSID.
Wi-Fi Password	Enter your Wi-Fi password. A complex, hard-to-guess key is recommended.
Security	Select a Wi-Fi security type from the drop-down menu. WPA/WPA2 is the default setting and the higher secure. Security can be disabled by selecting None but this is not recommended.
Version	Select which version of security type to use. WPA2 is the higher secure but not supported by all wireless clients. Selecting Mixed WPA/WPA2 ensures wireless client compatibility.
Encryption	Displays encryption type according to version. AES encryption is the default setting for WPA2, while Mixed TKIP+AES is default for Mixed WPA/WPA2.

2.4 / 5 GHz Channel Settings	
Mode	Select the wireless standard used for the router’s Wi-Fi. **802.11b/g mixed** means 802.11b and 802.11g wireless clients can connect to the router, **802.11 b/g/n/ax mixed** means 802.11b, 802.11g 802.11n and 802.11ax wireless clients can connect to the router, and so on.
Channel	Select a wireless radio channel or use the default “Auto”

	setting from the drop-down menu. Changing radio channel can improve Wi-Fi signal depending on how crowded the channel is with other radio signals and interference.
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference), 40MHz (better performance but likely more interference), or Auto (automatically select based on interference level). The 5GHz page 20/40/80/160MHz is the same.

Guest

> Wi-Fi Settings > Guest

You can setup additional “Guest” Wi-Fi networks (2.4GHz and/or 5GHz) so guest users can enjoy Wi-Fi connectivity without accessing your primary networks. The “Guest” tab displays settings for your guest Wi-Fi networks.

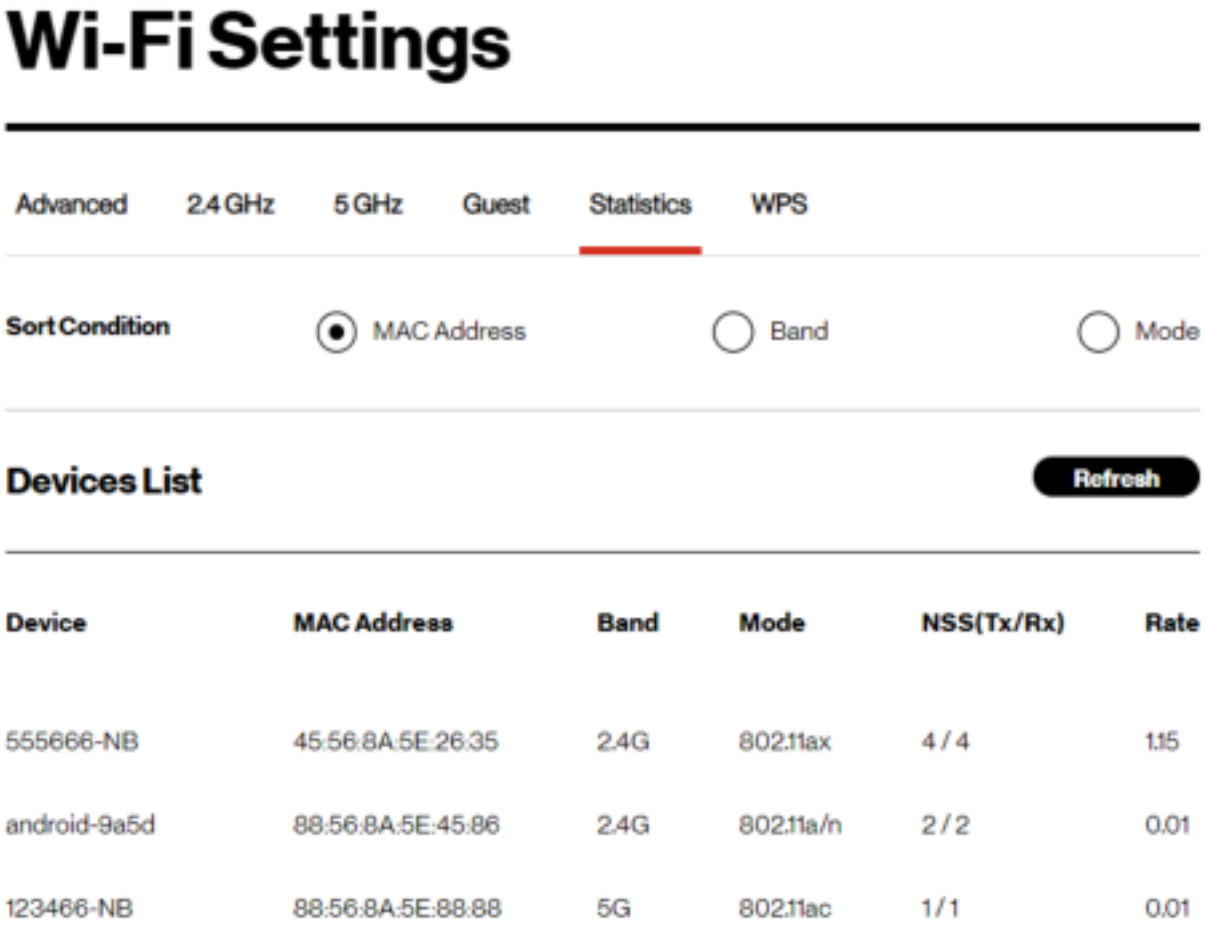
Guest	
Guest Network	Toggle to enable or disable all guest networks.

2.4GHz / 5GHz Guest Network	Toggle to enable or disable guest network for displayed frequency, either 2.4GHz or 5GHz.
Wi-Fi Name (SSID)	This is the name of your Wi-Fi network for identification, also sometimes referred to as “SSID”. The SSID can consist of any combination of up to 32 alphanumerical characters.
Hide SSID	Check the box to hide your SSID. When hidden, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden SSID is typically more secure than a visible SSID.
Wi-Fi Password	Enter your Wi-Fi password. A complex, hard-to-guess key is recommended.
Security	Select a Wi-Fi security type from the drop-down menu. WPA/WPA2 is the default setting and the higher secure. Security can be disabled by selecting None but this is not recommended.
Version	Select which version of security type to use. WPA2 is the higher secure but not supported by all wireless clients. Selecting Mixed WPA/WPA2 ensures wireless client compatibility.
Encryption	Displays encryption type according to version. AES encryption is the default setting for WPA2, while Mixed TKIP+AES is default for Mixed WPA/WPA2.

Statistics

> Wi-Fi Settings > Statistics

The Statistics displays the client devices which connect via Wi-Fi. The list can sort by MAC address, Band or Mode.

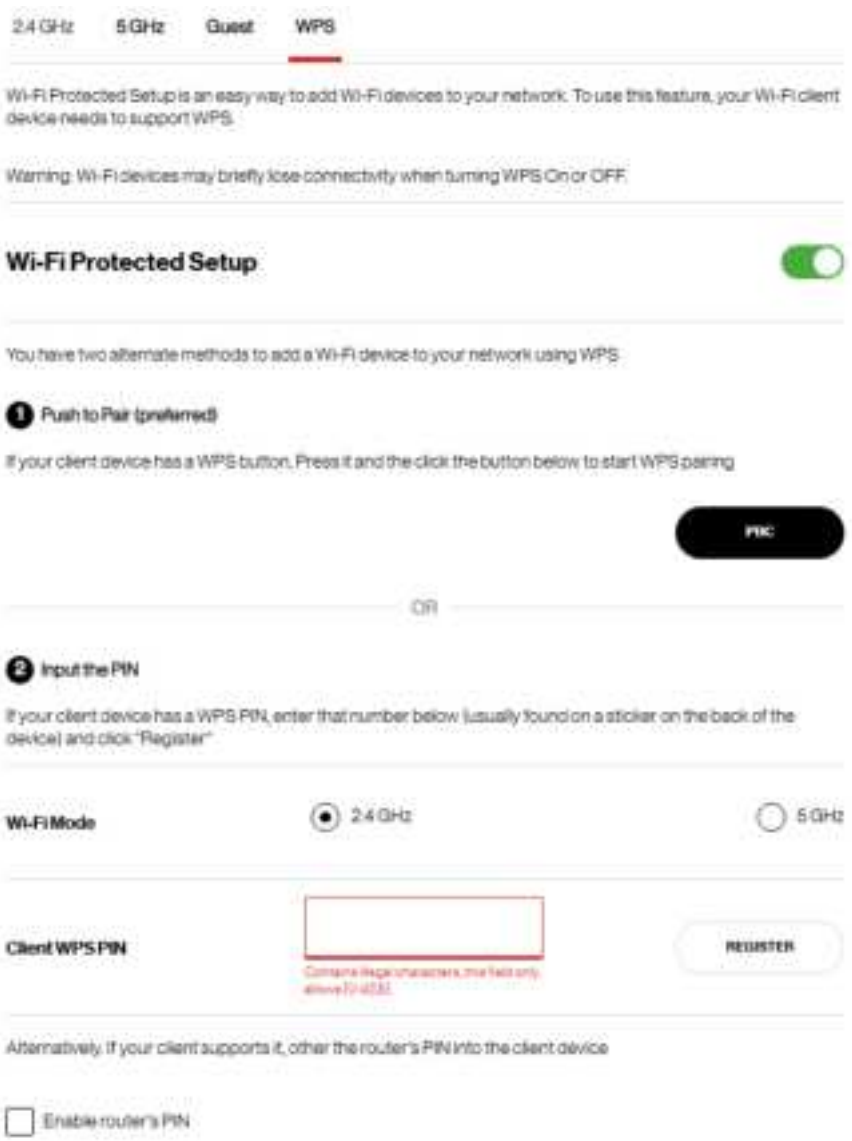


WPS

> Wi-Fi Settings > WPS

Wi-Fi Protected Setup (WPS) is a simple way to establish connections between WPS compatible devices. WPS can be activated on compatible devices by pushing a WPS button on the device or from within the device's firmware/configuration interface (known as PBC or "Push Button Configuration"). When WPS is activated in the correct manner and at the correct time for two compatible devices, they will automatically connect. "PIN code WPS" is a variation of PBC which includes the additional use of a PIN code between the two devices for verification.

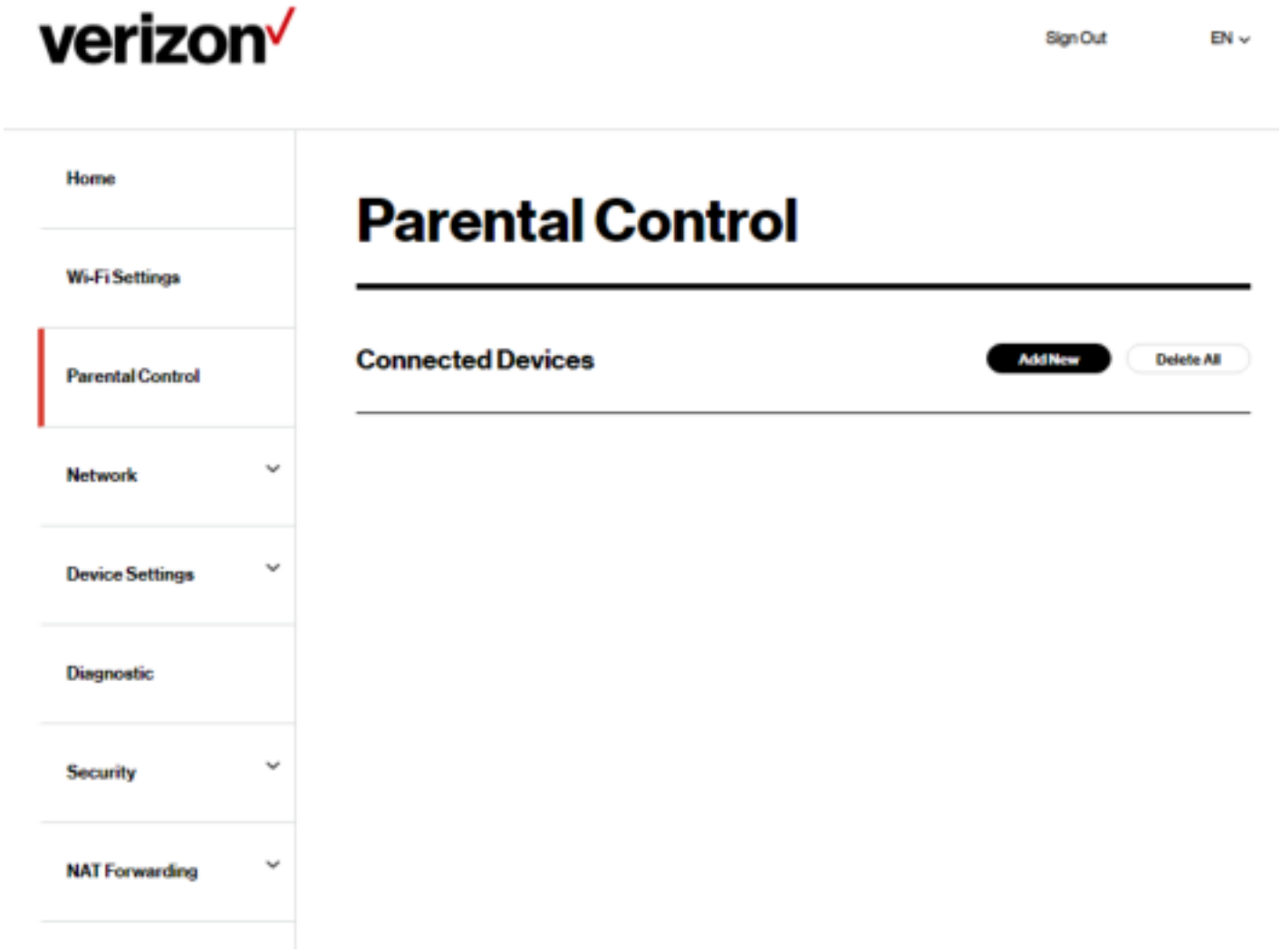
Follow the instructions on screen.



5.3 Parental Control

> Parental Control

The **Parental Control** feature allows you to restrict Internet access to selected devices on your network at specified times e.g. disabling Internet access for a child's smartphone.



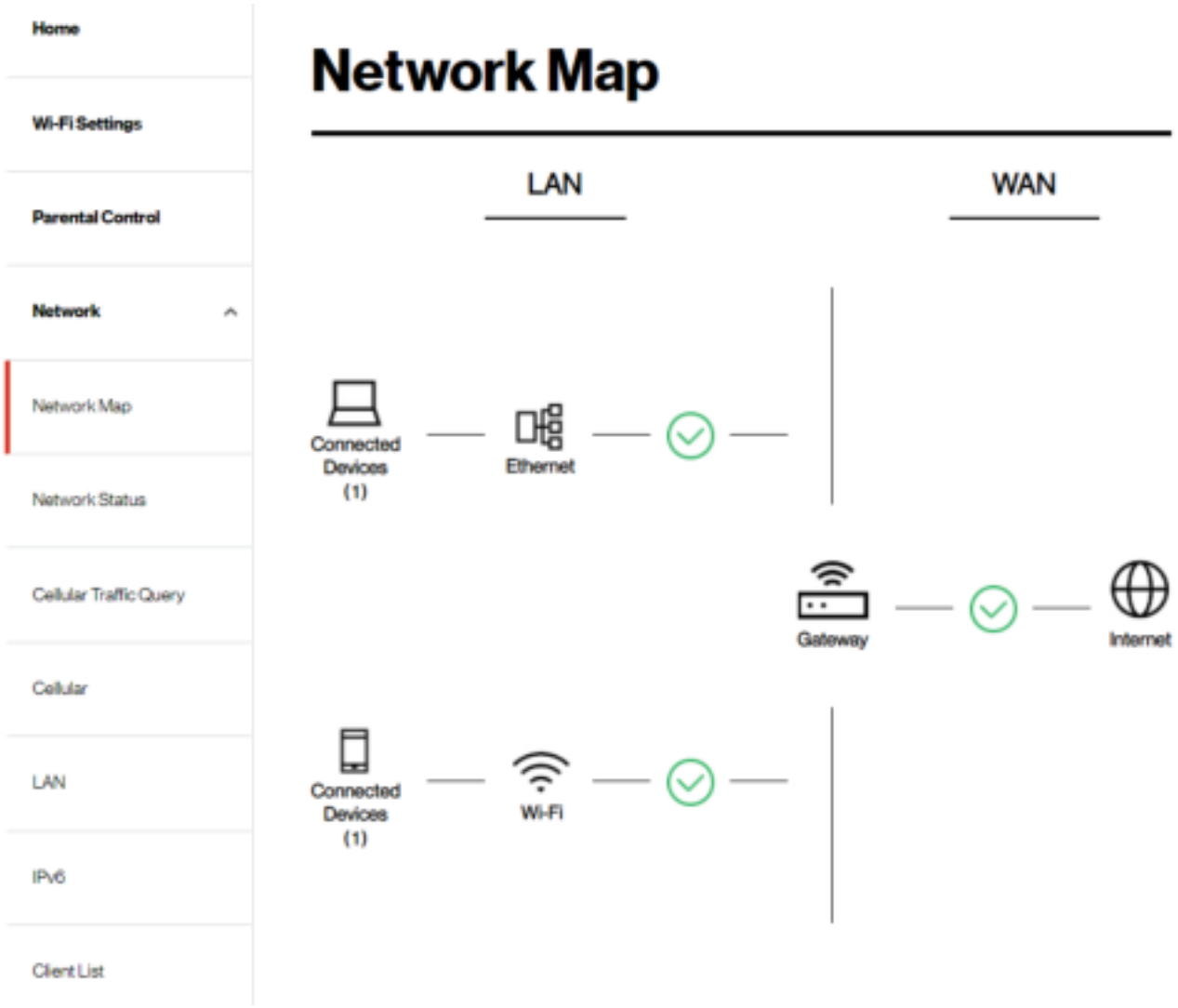
1. Click **Add New** to add and setup a new device for parental controls.
2. Toggle **Enable This Entry** to enable/disable this parental control setup.
3. Toggle **Schedule Internet Access** to enable/disable the schedule for Internet access:
4. Select a device from the Client menu or enter the MAC address manually below.
5. Specify a Device Name and enter a Description of the device for easy reference.

6. Click to select and specify which days to apply the parental control restrictions, and set the start and end times.
7. Click **Save** to save the schedule and the device's Internet access will now be restricted according to the schedule.

5.4 Network

> Network

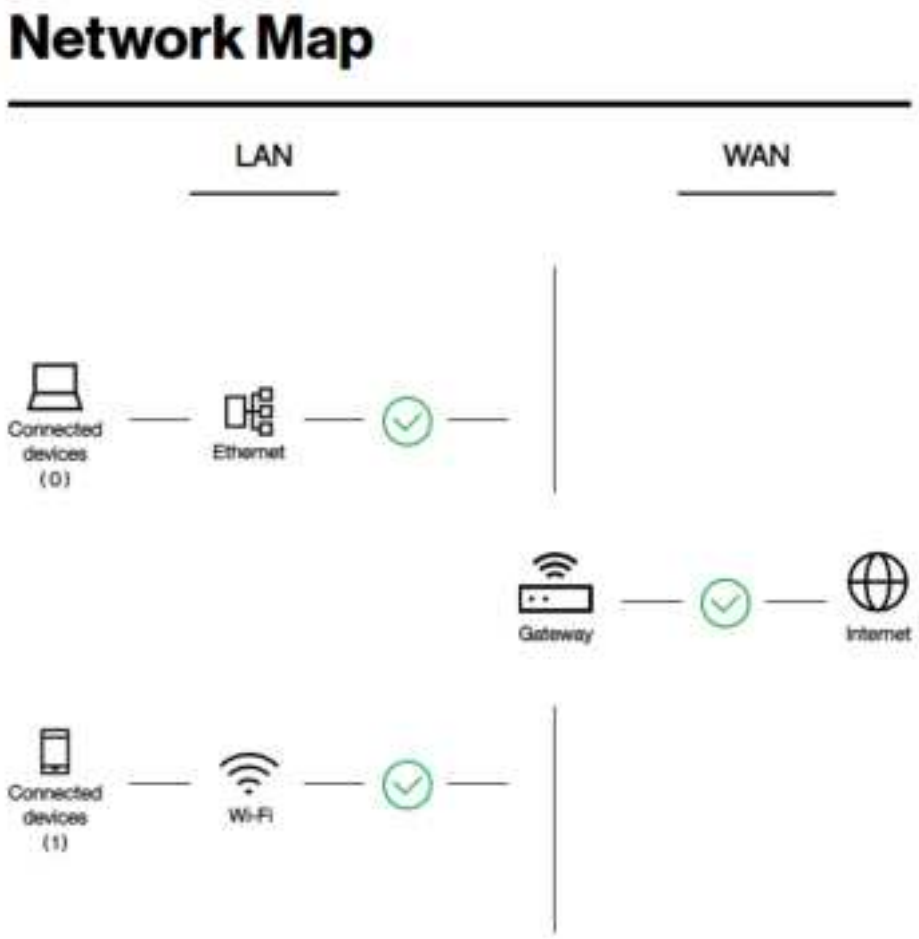
The Network menu provides quick links to the networking functions of your router. When you select the Network menu, the Network Map page is displayed as below.



Network Map

> Network > Network Map

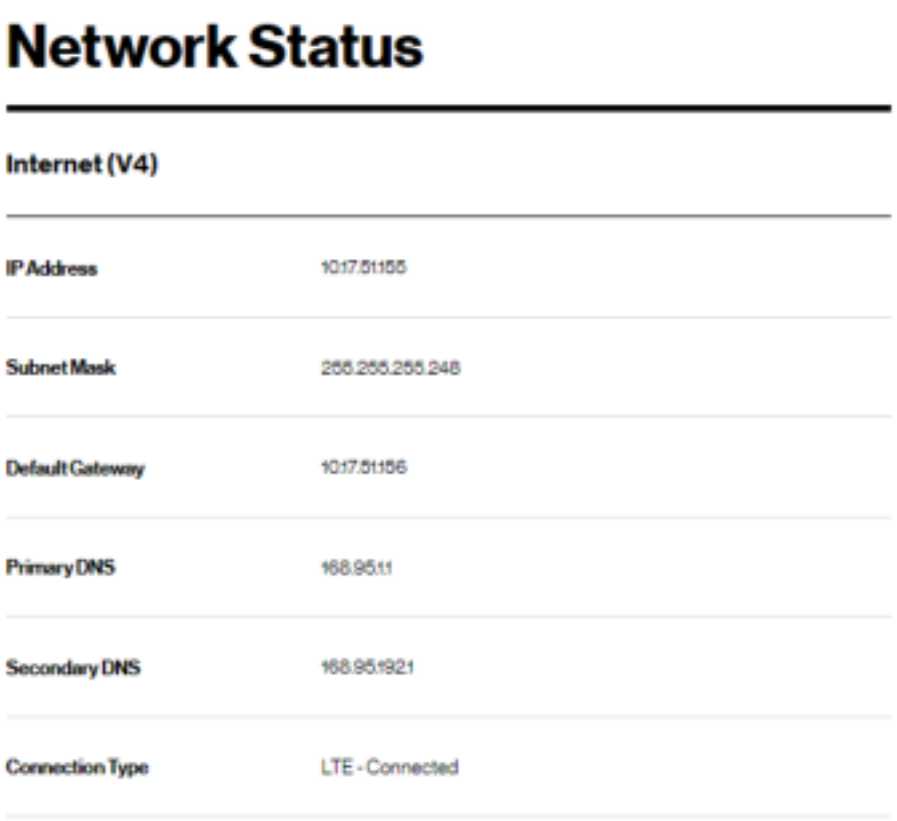
The network map provides a visual overview and status information of the network and devices on the network, with quick links to LAN & WAN settings and connected device / client lists. Green check marks indicate everything is working correctly.



Status

> Network > Status

Network Status displays the status of the network across six categories: Internet v4, Internet v6, LTE, LAN, Wireless & System Information.



Internet v4

Displays IPv4 Wide Area Network WAN information about your router's LTE connection. IPv4 is the default Internet protocol widely used across the Internet.

Internet v6

Displays IPv6 Wide Area Network WAN information about your router's LTE connection. IPv6 is an alternative Internet protocol

which is not yet widely supported. To setup IPv6 go to **Network > IPv6.**

Cellular
Displays Cellular information including operator name, SIM status…etc. To edit Cellular settings, go to **Network > Cellular.**

LAN
Displays the router's Local Area Network (LAN) information including MAC Address, IP Address and Subnet Mask, and DHCP Server status. To edit LAN settings go to **Network > LAN.**

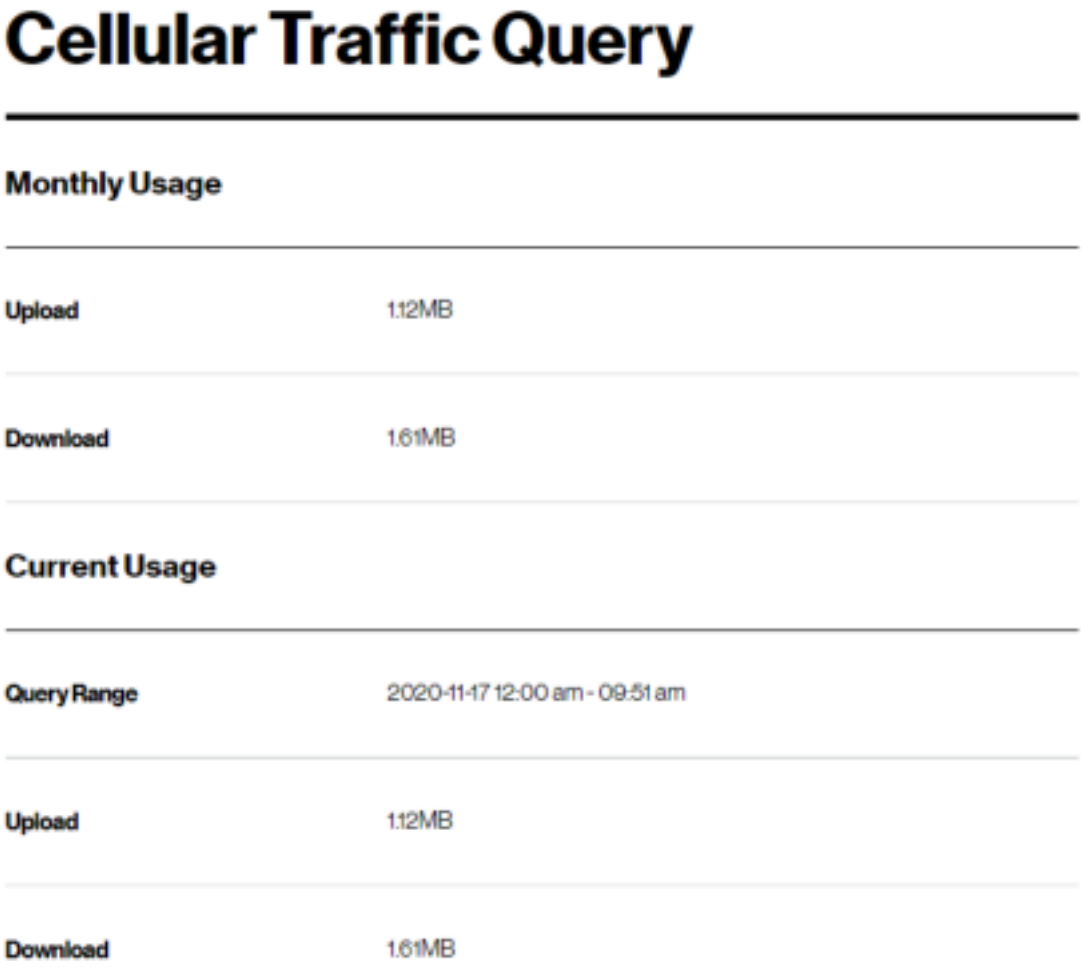
Wireless 2.4GHz & 5GHz
Displays your router's Wi-Fi information for both 2.4GHz & 5GHz frequencies. Includes network name (SSID) and radio & channel information. To edit these Wi-Fi settings go to **Wi-Fi Settings.**

System Information
Displays system identifiers unique to your hardware.

Cellular Traffic Query

> Network > Cellular Traffic Query

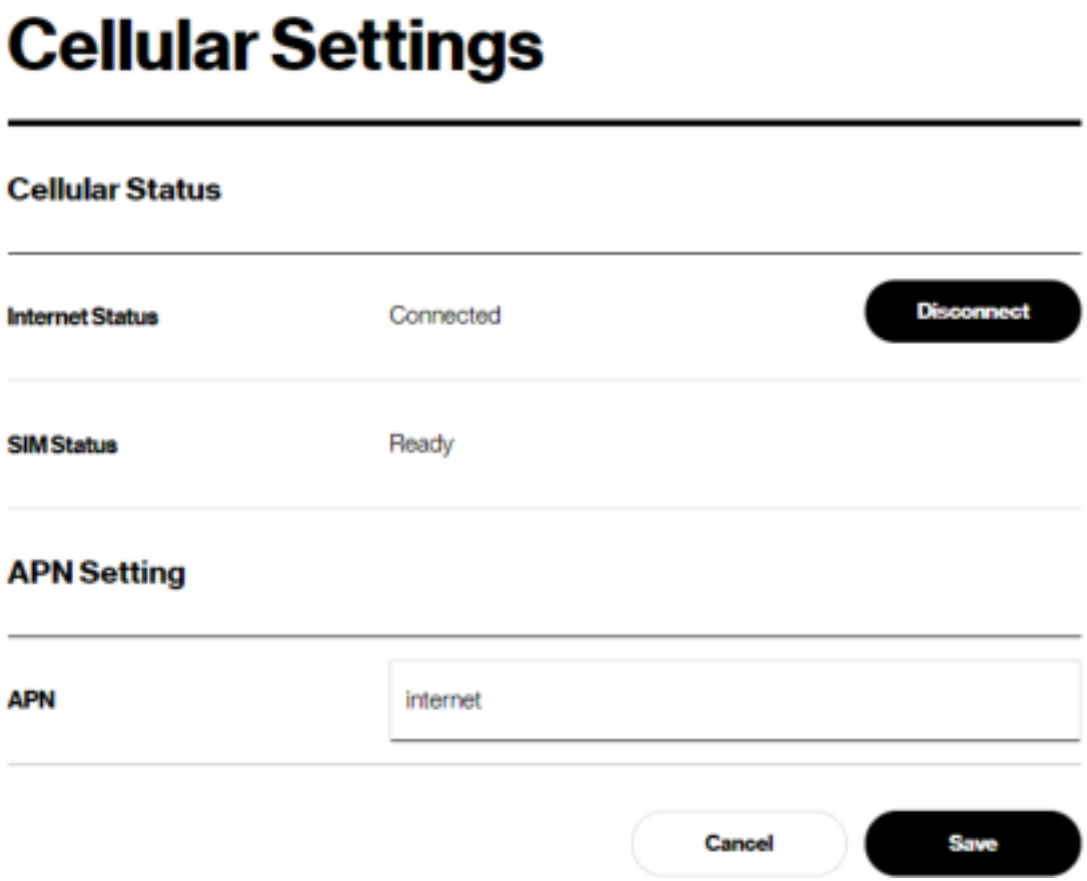
Traffic Query displays your network data usage, with upload, download and total traffic displayed in MB. Ensure that your router's date and time settings are correct in **Device Settings > Date / Time** for accurate Monthly usage information.



Cellular

> Network > Cellular

Cellular settings are pre-configured by default. You can disconnect the Cellular connection using the Disconnect button if needed, and the connection and SIM status are displayed accordingly. It’s not recommended to modify APN Setting unless instructed by your ISP.



LAN

> Network > LAN

The **LAN Settings** page allows you to configure your router on your Local Area Network (LAN). You can specify a static IP address for your router, and configure your router as a DHCP server to assign IP addresses to other devices on your LAN.

Basic	
MAC Address	Displays the MAC address of your router. A MAC address is a unique fixed identifier for every device on a network.
IP Address	Specify the IP address here. This IP address will be assigned to your router and will replace the default IP address.
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0

Advanced	
DHCP	Toggle the switch to enable or disable DHCP server.
IP Address Pool	Enter the start and end IP address of the IP address range which your router's DHCP server will assign to devices on the network.
Address Lease Time	Enter an address lease time in hours. IP addresses will be assigned for this period of time before being reassigned.
Primary DNS Address	Enter a primary DNS address, the default setting is the gateway IP.
Secondary DNS Address	Enter a secondary DNS address.

IPv6

> Network > IPv6

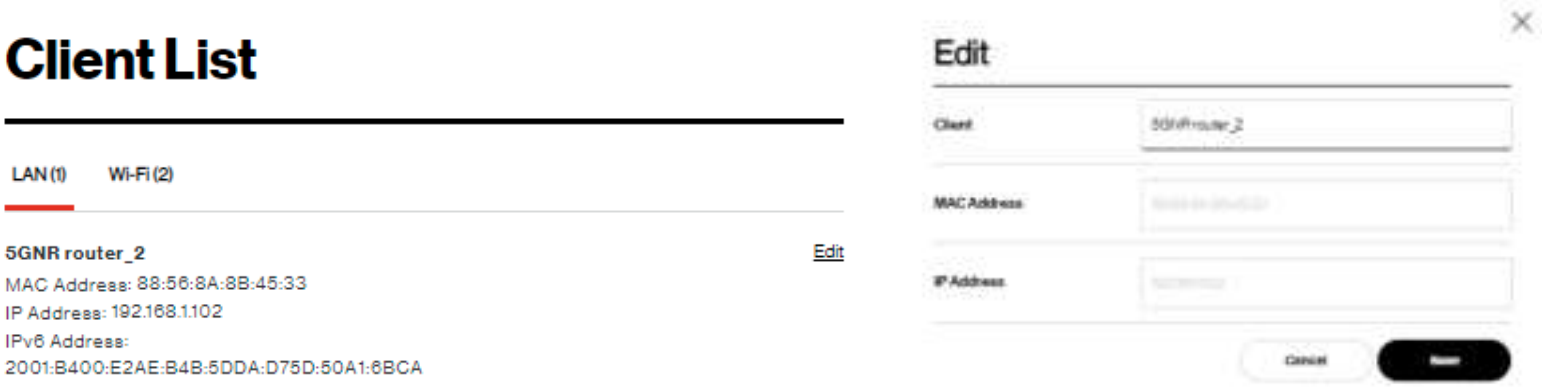
This wireless router supports IPv6 addressing: a system that supports more IP addresses. Here can enable the IPv6 address support.

Client List

> Network > Client List

Displays all devices (clients) connected to your router, by Ethernet (LAN) or Wi-Fi (wireless) e.g. laptops, smartphones. The device name, MAC address and IP address is listed for each device.

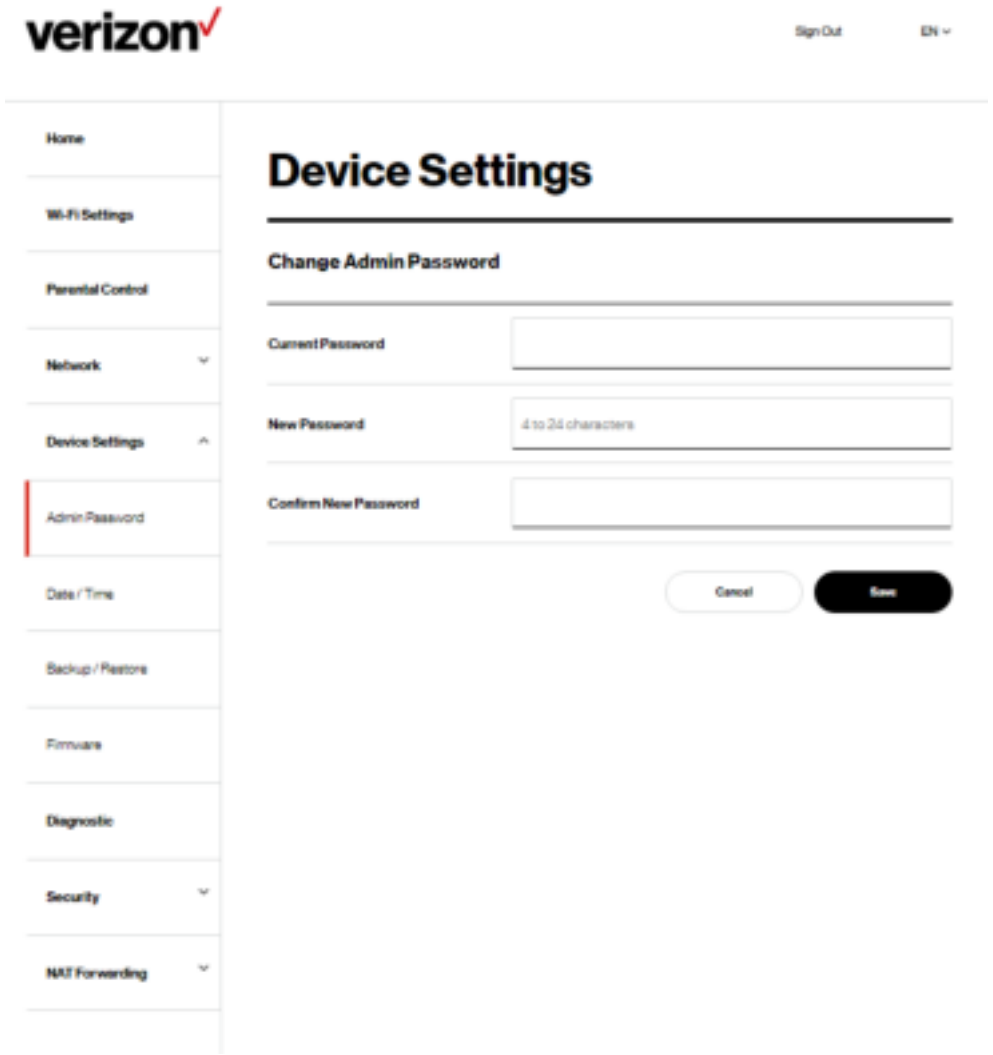
Click **Edit** to edit the client name to help identify the device.



5.5 Device Settings

> Device Settings

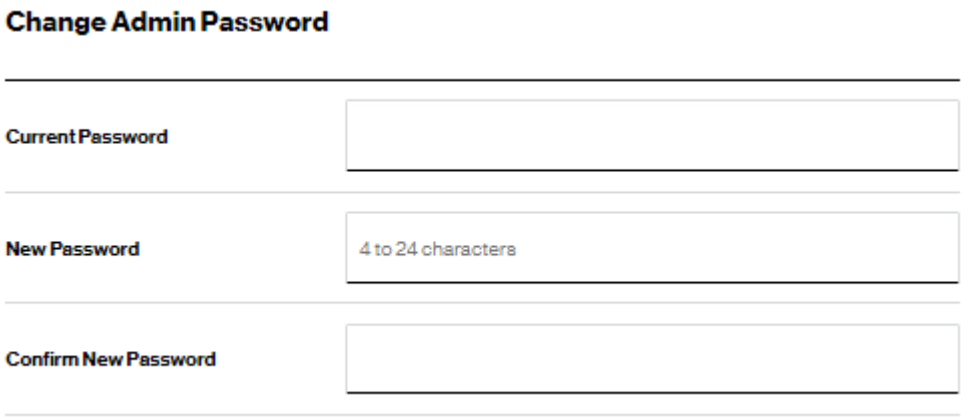
Various administrative functions of your router can be configured from the **Device Settings** menu, including the Web UI login password, router date & time settings, backup, router firmware and system logs.



Admin Settings

> Device Settings > Admin Settings

The **administration** function allows you to change the login password for the router's Web UI. It's essential to change this password for the security of your router. Use hard-to-guess password which include combinations of numbers, letters and symbols, and change your password regularly.

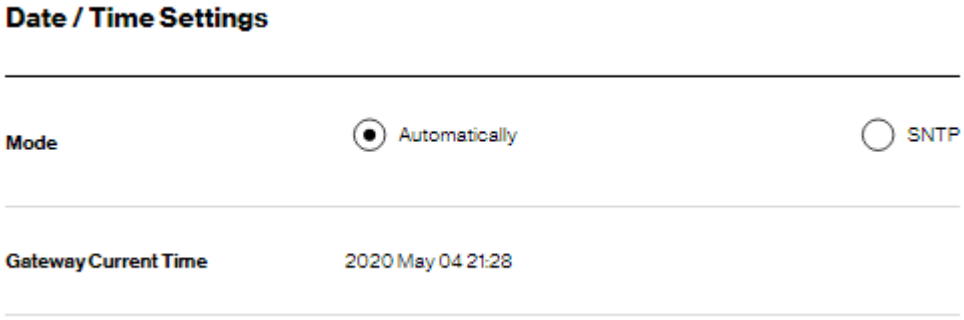


1. Enter the current password for authentication.
2. Enter your name password in the New Password field and again to confirm, and choose **Save** to save the new settings.

Date & Time

> Device Settings > Date & Time

Set the **date and time** for your router. You can use a Simple Network Time Protocol (SNTP) which synchronizes the date and time with public time servers, or the router can get the date and time automatically based on your selected time zone.



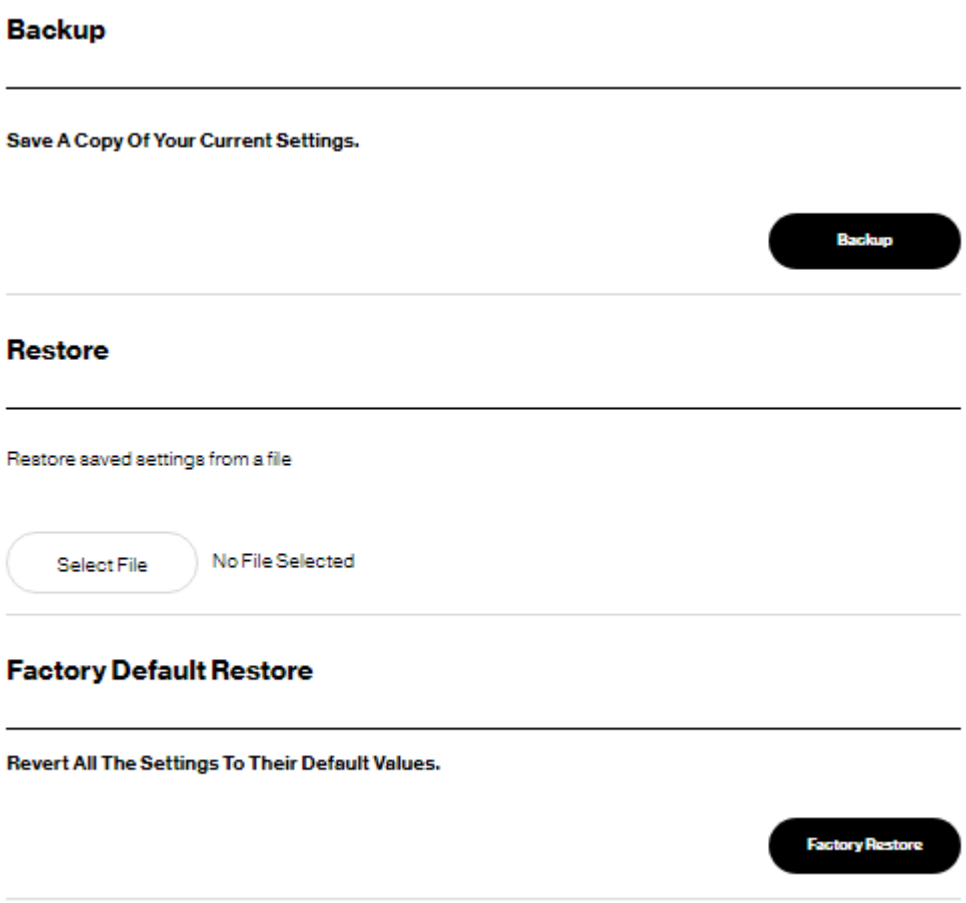
1. Select Automatically or SNTP for the mode.
2. For automatic, select your time zone from the drop-down menu.
3. For SNTP, to synchronize date and time with public time servers, enter the NTP Servers.

Examples of commonly used NTP Servers include time.microsoft.com or time.google.com.

Backup / Restore

> Device Settings > Backup / Restore

The Backup / Restore page enables you to save/backup the router's current settings as a file to your local computer, or restore your router to previously saved settings by loading a backed up file. You can also reset the router back to factory default settings. If the router malfunctions or is not responding, then it is recommended that you first reboot the device, and if still experiencing problems reset the device back to its factory default settings. You can reset the router back to its default settings using the Reset button on the back of the router (press and hold for 4-7 seconds).

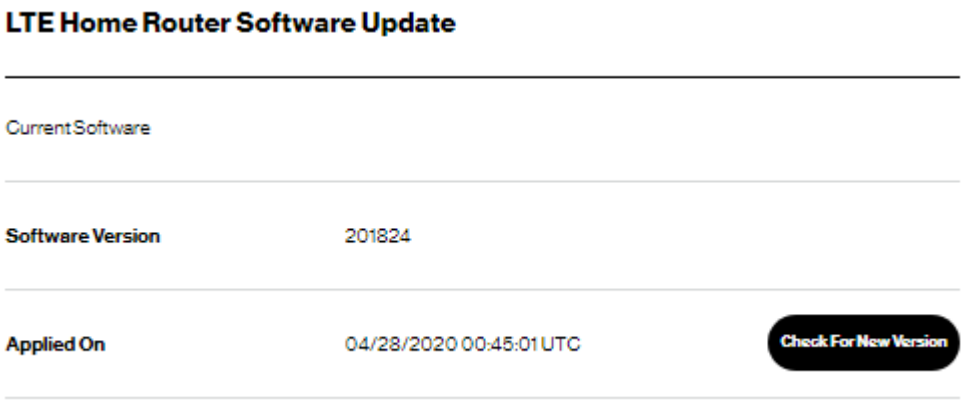


Backup	
Save a copy of your current settings	Click the Backup button to save the settings file to your local computer.
Restore	
Restore saved settings from a file	Choose Select File to locate a previously saved settings file on your computer and select it to load the file to your router.
Factory Default Restore	
Revert all the settings to their default values.	Select Factory Restore to revert your router to its original factory default state. This resets all settings.

Firmware

> Device Settings > Firmware

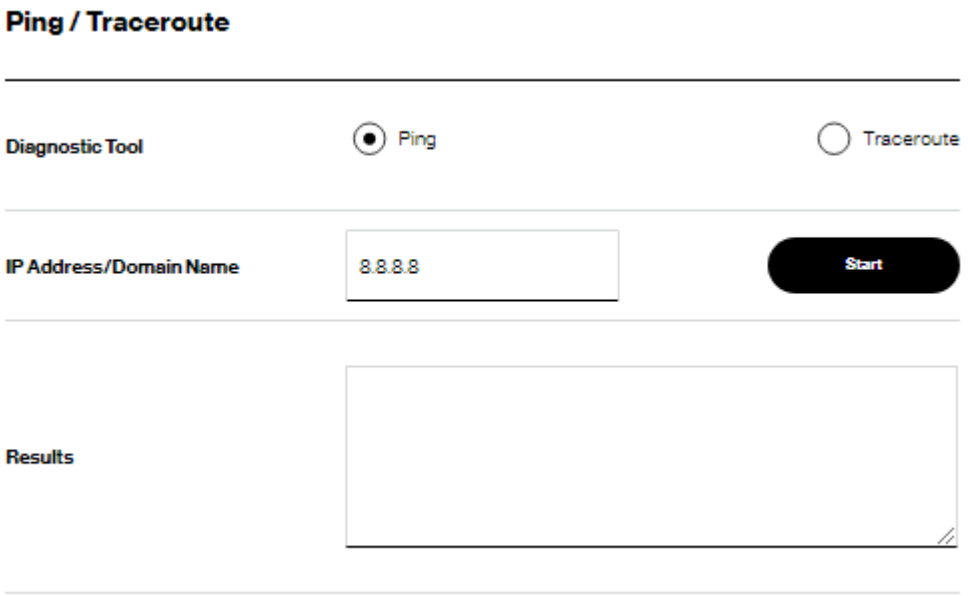
The **Firmware** page displays your router's firmware version information. Firmware is the software that your router runs on. You can click **Check For New Version** to manually initiate a check to see if new firmware is available.



5.6 Diagnostic

> Diagnostic

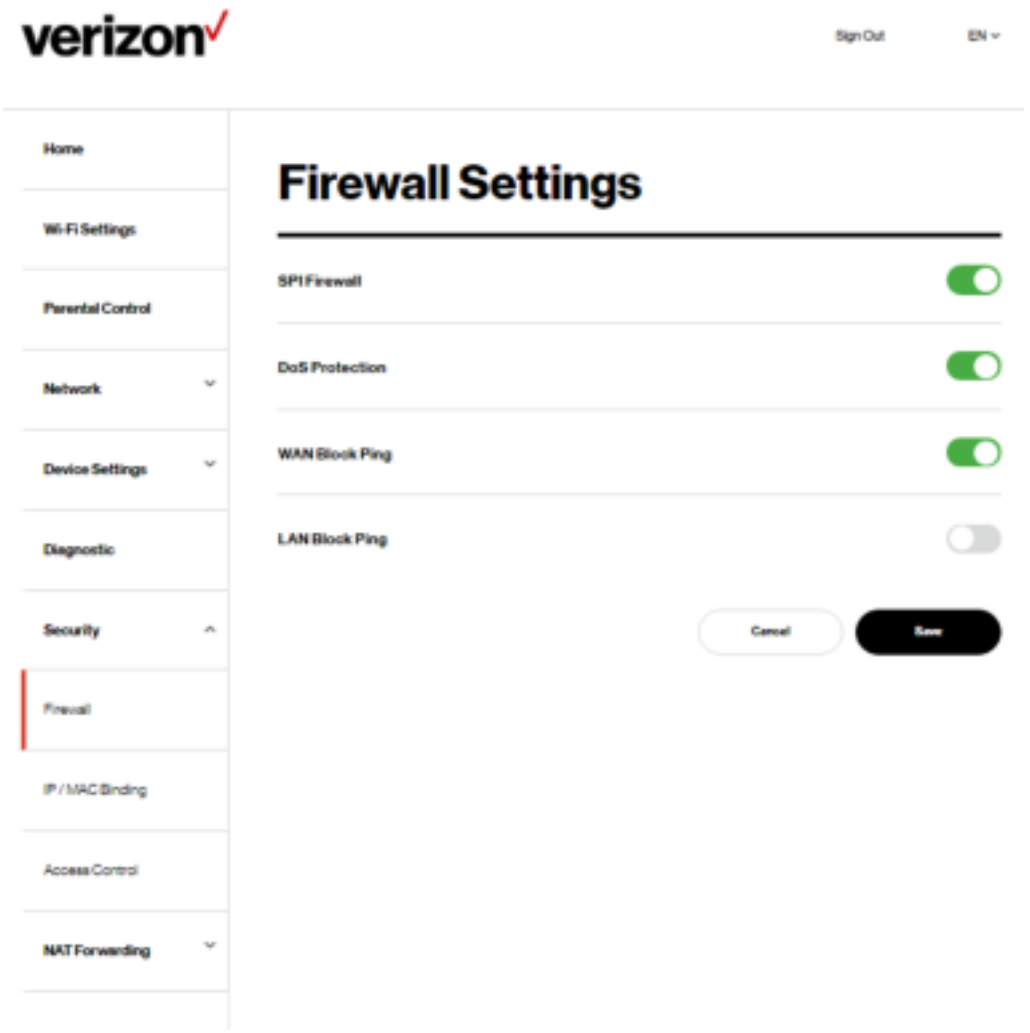
You can run **Ping & Traceroute diagnostic** tests with the router. Enter the IP address to use for the test and click Start, results are displayed in the box.



5.7 Security

> Security

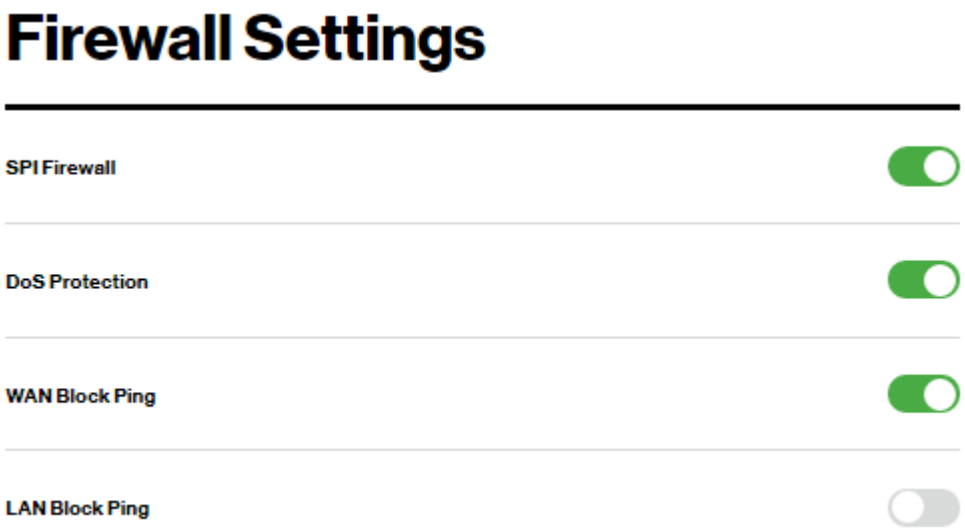
Use the **Security** menu to configure various security functions if needed, including Firewall, IP/MAC Binding and Access Control.



Firewall

> Security > Firewall

The router features a built-in firewall that provides protection to your network from unauthorized intrusions from the Internet. The firewall features four modules which can be enabled or disabled using the switches.



SPI Firewall

Stateful Packet Inspection (SPI) firewall protection means only packets matching a known active connection will be allowed by the firewall, and others will be rejected. An SPI firewall goes beyond stateless filtering and checks an entire packet's content rather than only packet headers. This is a security feature to help distinguish between legitimate packets of information and potentially harmful packets, and provides greater security for your network.

DoS Protection

Denial-of-Service (DoS) is a common form of malicious attack against a network. The router's firewall can protect against such attacks by filtering unreasonable packets that could flood and disable network with large amounts of traffic.

WAN Block Ping

When active the router will not answer ping requests from the Internet. This can increase security as pinging is a common method used by hackers to test networks.

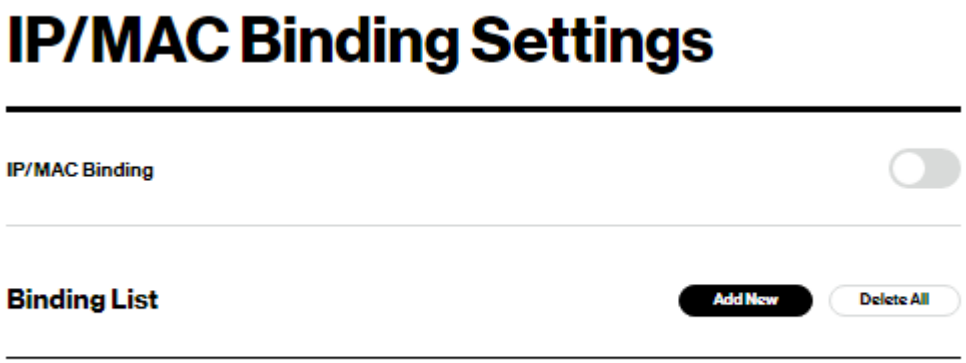
LAN Block Ping

When active the router will not answer ping requests from the local network. This can increase security as pinging is a common method used by hackers to test networks.

IP / MAC Binding

> Security > IP / MAC Binding

IP/MAC Binding allows you to reserve a static IP address for a device on the network, rather than being assigned a new (dynamic) IP address by the router's DHCP Server every time the device connects to the router. Static IP addresses can be useful for using various services on the local network. Every device is identified by a unique MAC address, and the IP address can be bound to the MAC address.



1. Switch **IP**/**MAC** Binding on using the toggle switch.
2. Click **Add New** to setup a new client for IP/MAC Binding.
3. Select a device from the Client menu or enter the MAC address manually.
4. Specify the IP Address the client will use, and enter a Description of the device for easy reference.

Add New

Enable This Entry

Client Manually

MAC Address

The MAC address should be 12-digit hexadecimal numbers like following format: XX:XX:XX:XX:XX:XX

IP Address

The value should be an IP address.

Description

Contains illegal characters, this field only allows [a-zA-Z0-9@=_/:-?]*#$&,%-]

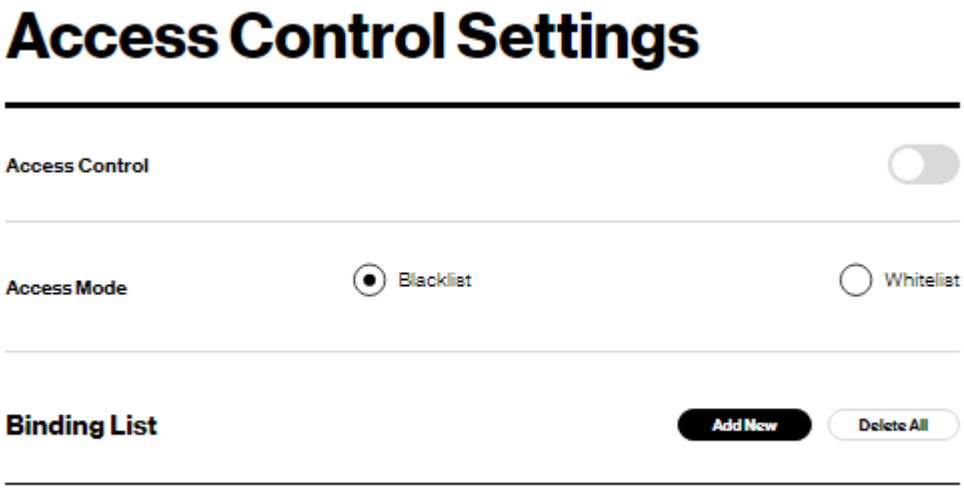
You will need to disconnect and reconnect the device to the router for the IP binding settings to tak

Cancel Save

Access Control

> Security > Access Control

Access Control is a security feature that can help to prevent unauthorized users from connecting to your router. You can define a list of network devices permitted (whitelist) or denied (blacklist) to connect to the router. Devices are each identified by their unique MAC address or IP address.



1. Switch Access Control on using the switch.
2. Select Blacklist (not permitted) or Whitelist (permitted), and click **Add New**.
3. Select a device from the Client menu or enter the MAC address manually.
4. Enter the Name of the device for easy reference.

Add New

Enable This Entry

Client Manually

MAC Address

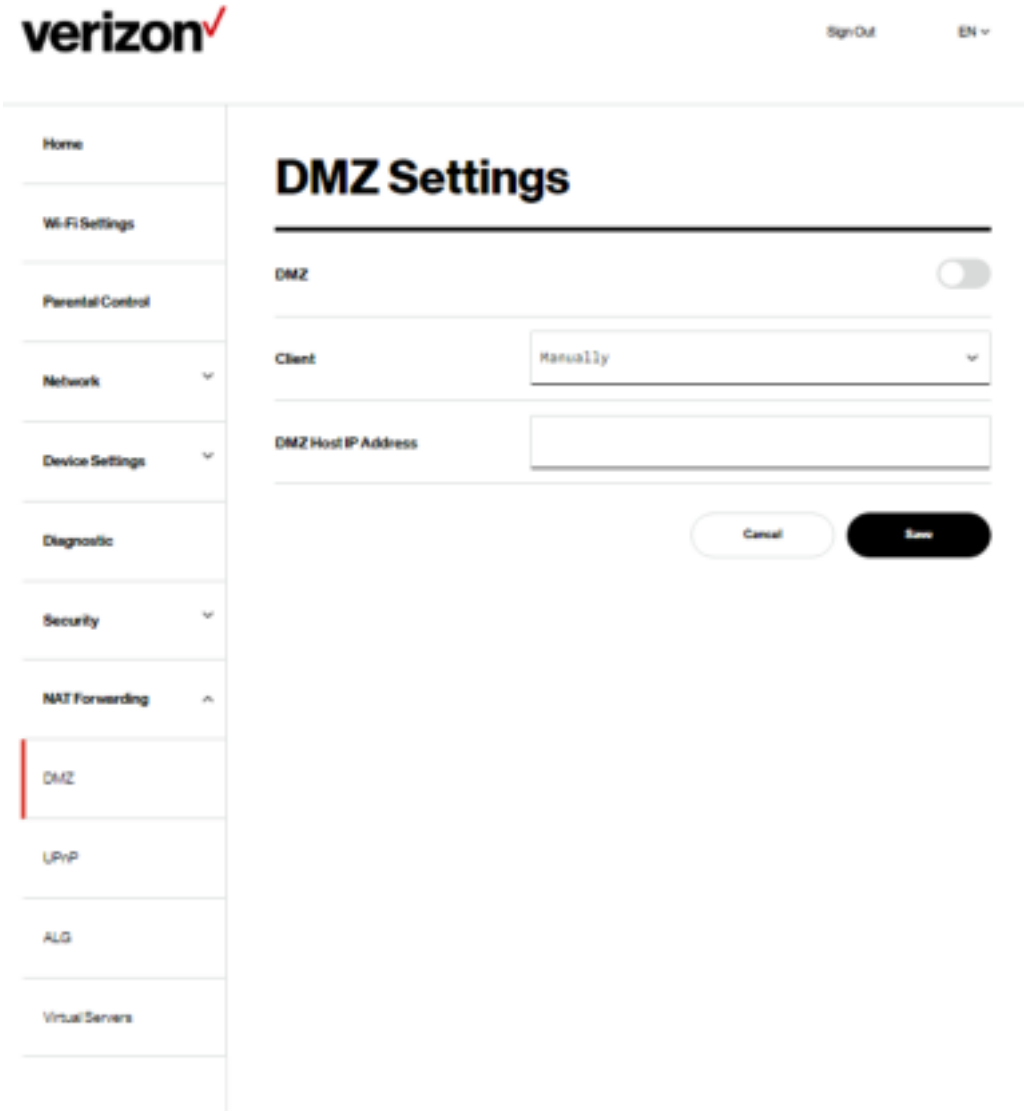
Device Name

Cancel Save

5.8 NAT Forwarding

> NAT Forwarding

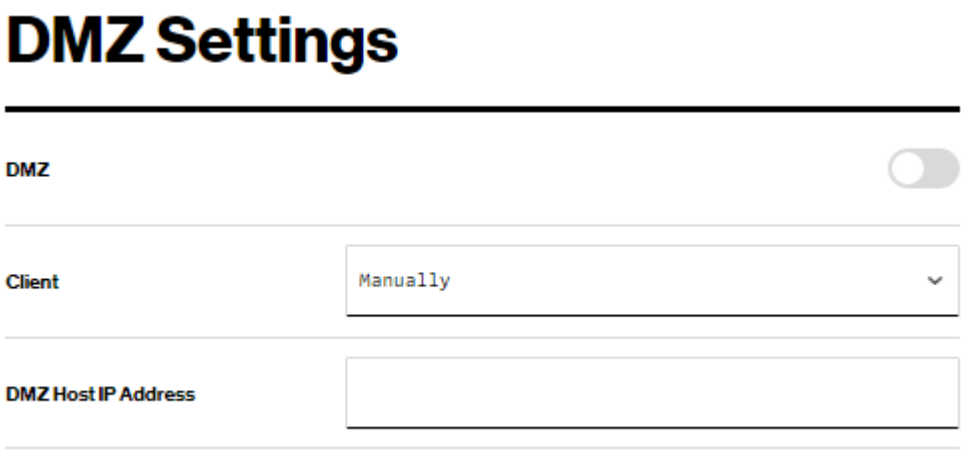
Functions in the **Network Address Translation** (**NAT**) **Forwarding** menu can improve network performance and security.



DMZ

> NAT Forwarding > DMZ

A Demilitarized Zone (DMZ) is an isolated area in your local network where a computer runs outside the firewall and receives/intercepts all incoming Internet traffic. This can provide an extra layer of security to the rest of the network, or can be useful if a network client PC cannot run an application properly from behind an NAT firewall. However since it opens the client up to unrestricted two-way access this computer is vulnerable. DMZ should be configured only by expert network users aware of the security risks.



1. Use the switch to set DMZ to **active**.
2. Enter the IP Address of the computer to provide the DMZ service (ensure this computer is using a Static IP Address)

UPnP

> NAT Forwarding > UPnP

Universal plug-and-play (**UPnP**) is a set of networking protocols which enables network devices to communicate and automatically establish working configurations with each other, such as computers, printers, mobile devices etc.

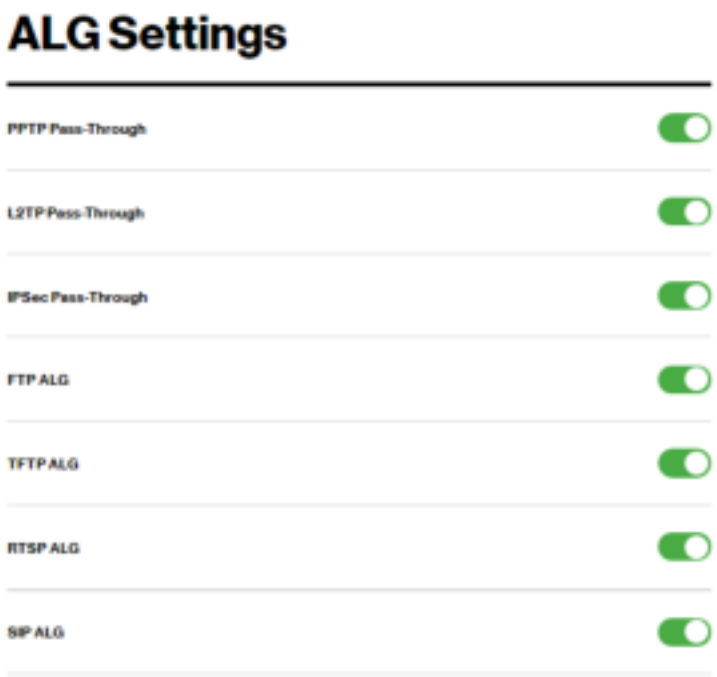
It’s typically used for data sharing, communications and entertainment purposes, although sometimes not preferred due to security concerns. Some devices may require UPnP to be enabled to function properly. Use the switch to set UPnP to active or inactive, according to your requirements.

ALG

> NAT Forwarding > ALG

Application Level Router (ALG) settings are advanced functions that can resolve issues where services are disrupted by the firewall. Each ALG module is a security component that augments the firewall. Services such as VPNs or Virtual Servers may require ALG modules enabled. By default all ALG modules are active. Use the switches to disable any ALG module required. ALG Settings are recommended for expert users only.

SIP ALG may disrupt Wi-Fi calling for cellphones connected to the network.



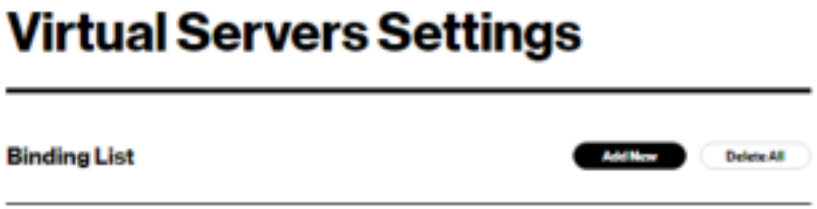
Manage ALG Settings	
PPTP Pass-Through	Point-to-Point Tunneling Protocol (PPTP) is a module for implementing virtual private networks.
L2TP Pass-Through	Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs)

	or as part of the delivery of services by ISPs.
IPSec Pass-Through	Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.
FTP ALG	File Transfer Protocol is a widely and commonly used method of exchanging files over IP networks. The FTP ALG monitors PORT, PASV, and 227 commands. It performs NAT on the IP, port, or both in the message and gate opening on the device as necessary
TFTP ALG	Trivial File Transfer Protocol (TFTP) is a simple protocol used for files transfer *(RFC 1350)*. TFTP is implemented on top of UDP, with destination port 69 as the well-known port. The TFTP Application Layer Router (ALG) processes TFTP packets that initiate the request.
RTSP ALG	The Real Time Streaming Protocol (RTSP) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.
SIP ALG	The Session Initiation Protocol (SIP) is a communications protocol for signaling and controlling multimedia communication sessions. The most common applications of SIP are in Internet telephony for voice and video calls, as well as instant messaging all over Internet Protocol (IP) networks.

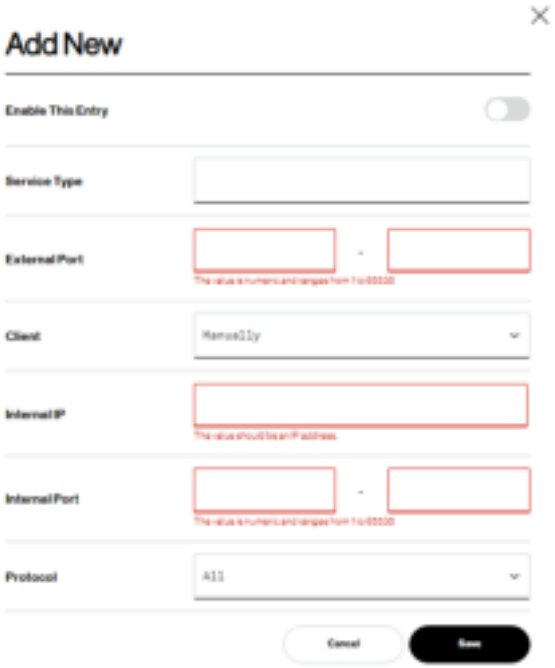
Virtual Servers

> NAT Forwarding > Virtual Servers

This function allows you to set up an internet service on a local computer, without exposing the local computer to the internet. Internet traffic is directed to a specific port or range of ports on a device or devices on your local network. You can also build various sets of port redirection, to provide various internet services on different local computers via a single Internet IP address. It also allows PCs outside the network to access services provided by a computer in the local network.



1. Click **Add New** and enter the parameters to setup a virtual server:

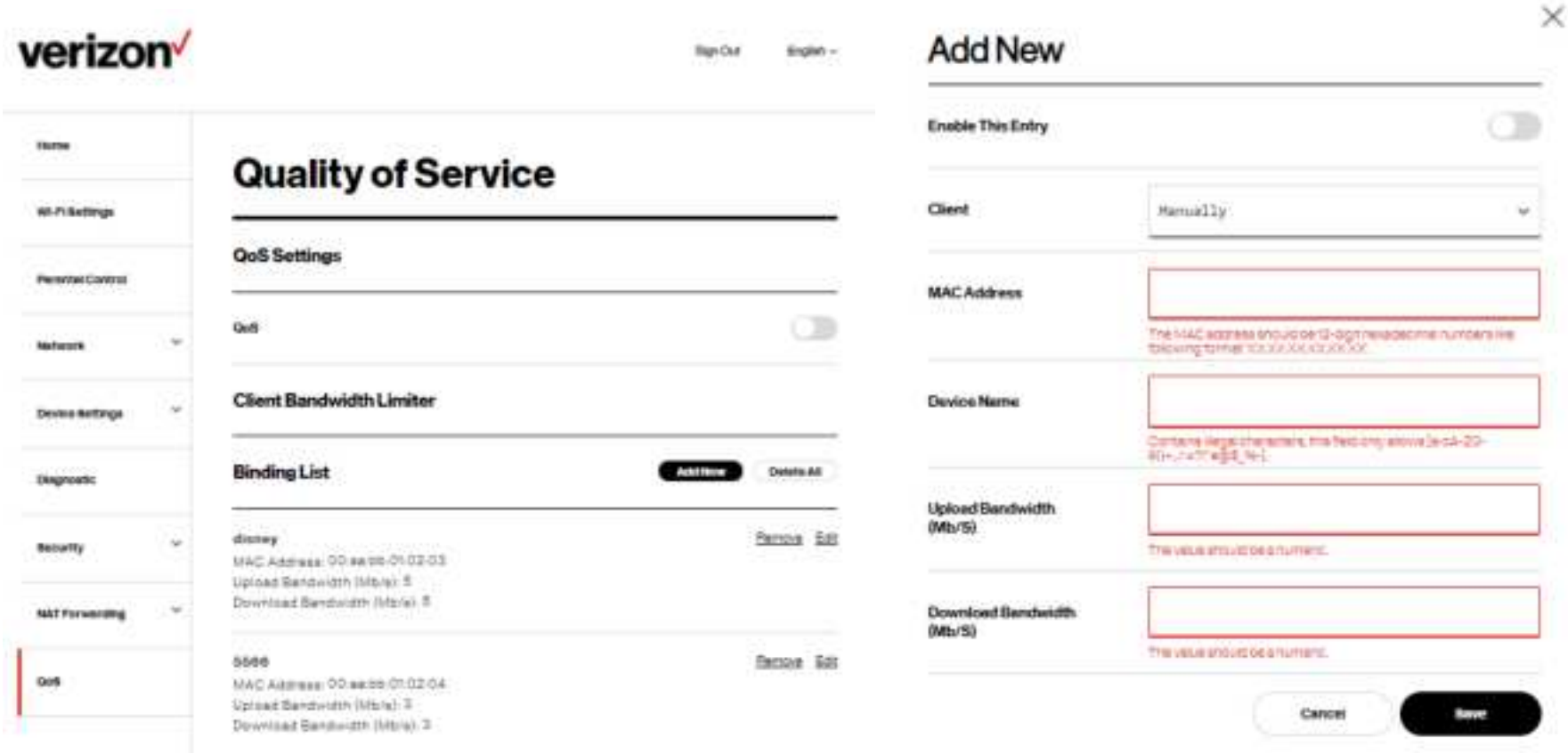


Service Type	Specify the service type e.g. HTTP, FTP etc.
External Port Start	Specify the external/public port to access the computer on your local network.
Client	Select whether to manually assign Internal (Private) IP & Port.
Internal IP	Enter the IP address of the computer on your local network.
Internal Port	Specify the internal/private port you wish to use on the computer in your local network.
Protocol	Select the connection protocol: TCP, UDP or All.

5.9 QoS

> QoS > Quality of Service

Quality of Service (QoS) is the manipulation of traffic. If you wish to limit the amount of bandwidth that connected devices can use.
Enable Qos then click **Add New** can add the device to limit the Upload/Download bandwidth.
Click **Edit** can modify the exist device limit bandwidth.



6. Troubleshooting

If you are having problems with your router, try these basic steps in this section before looking for further solutions.

Where can I get more help?
Visit support.verizon.com/router to find your nearest Verizon store or for 24/7 help with live chat and device-specific support.

7. Technical Specification

General

Technical Standard	LTE Category 18, 5G NR Sub 6
Frequency band	LTE Band: B2/B4/B5/B13/B48/B66, DL 4x4 MIMO 5G Band: 256 QAM, DL 4x4 MIMO n2/n5/n66/n77
Wi-Fi Standard	802.11 a/b/g/n/ac/ax
Dimensions (L x W x H)	130mm x 130mm x 136mm
Operating temperature range	+5°C to +40°C
Storage temperature range	-45 – 70 °C

Connections

DC input	1st source adapter: 12V/ 3A 2nd source adapter: 12V/2A
Ethernet plugs	RJ-45 LAN * 2

Federal Communication Commission Interference Statement

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.

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 party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

Radiation Exposure Statement
The product comply with the FCC portable RF exposure limit set forth for an uncontrolled environment and are safe for intended operation as described in this manual. The further RF exposure reduction can be achieved if the product can be kept as far as possible from the user body or set the device to lower output power if such function is available.

RF Exposure Information (MPE)
This device has been tested and meets applicable limits for Radio Frequency (RF) exposure.
This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.