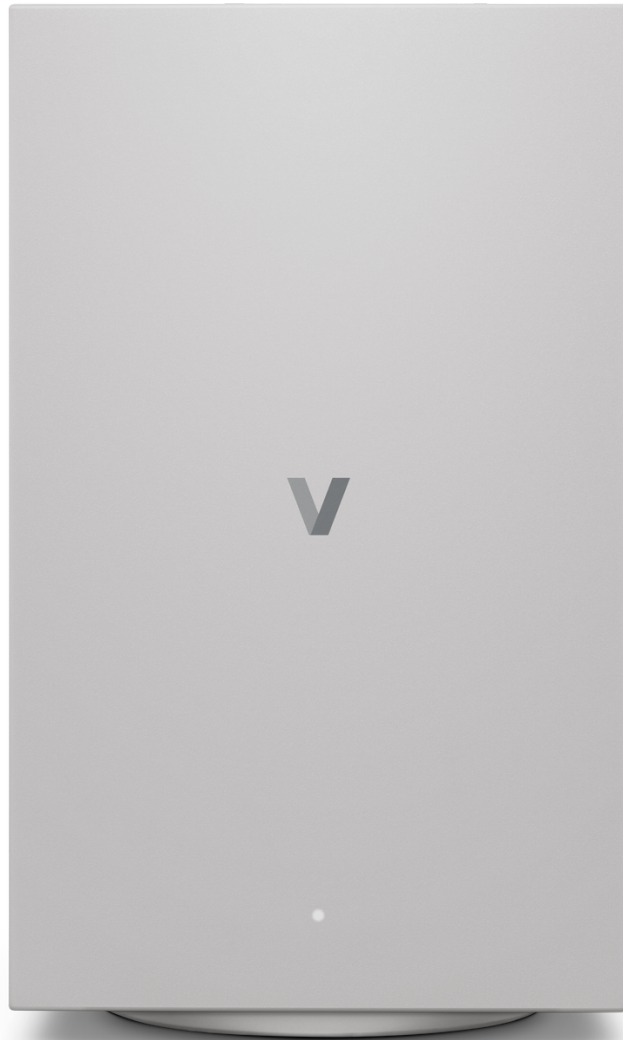




Wi-Fi Access Point

CHR30A

User manual



Table of contents

CHR30A	1
Table of contents	2
1 Introduction	5
1.0 Package contents	5
1.1 System requirements	5
1.2 Features	5
1.3 Getting to know your Wi-Fi Access Point	7
1.3a Front panel	7
1.3b Rear panel	8
1.3c Rear lighted indicators	9
1.3d Mounting the Wi-Fi Access Point to a wall	9
02 Connecting your Wi-Fi Access Point	13
2.0 Setting up your Wi-Fi Access Point	13
2.0a Installation instructions	14
2.0b Configure your Wi-Fi Access Point	15
2.1 Expanding Wi-Fi coverage	18
2.2 Computer network configuration	18
2.2a Configuring dynamic IP addressing	18
2.2b Connecting other computers and network devices	19
2.3 Main screen	21
2.3a System	21
03 Wi-Fi settings	23
3.0 Overview	23
2.4 GHz	23
5 GHz	23
6 GHz	23
3.1 Basic settings	24
3.1a Primary network	24
3.1b Guest network	25
3.1c IoT network	26
3.1d Wi-Fi Protected Setup (WPS)	27
3.2 Advanced settings	28
3.2a Primary network	28
3.2b Radio management	30
04 Connected devices	33
4.0 Device settings	33
4.1 Setting Parental controls	36
4.2 Universal plug & play	36



05 Configuring advanced settings	37
5.0 Security & firewall	38
5.0a Setting firewall configuration	39
5.0b Access control	40
5.0c DMZ host	42
5.0d IPv6 pinholes	43
5.0e Port forwarding	44
5.0f Port forwarding rules	45
5.0g Port triggering	47
5.0h Scheduler rules	48
5.0i SIP ALG	49
5.1 Network settings	50
5.1a ARP table	50
5.1b DNS server	50
5.1c Dynamic DNS	51
5.1d IPv4 address distribution	52
5.1e IPv6	55
5.1f IPv6 address distribution	59
5.1g NDP table	60
5.1h Network connections	60
5.1i Network objects	71
5.1j Port configuration	72
5.1k Routing	73
5.1l Static NAT	74
5.2 Diagnostics & monitoring	75
5.2a Bandwidth monitoring	75
5.2b Diagnostics	75
5.2c System logging	76
5.2d System-wide connections	77
5.2e Backhaul logging	78
5.3 System	79
5.3a System status	79
5.3b Date & time settings	80
5.3c Factory reset	80
5.3d LED brightness	82
5.3e Open source software	83
5.3f Reboot internet equipment	83
5.3g Remote administration	84
5.3h System settings	85
06 Troubleshooting	86



6.0 Troubleshooting tips	86
6.1 Frequently asked questions	89
07 Specifications	90
7.0 General specifications	91
7.1 LED indicators	92
7.2 Environmental parameters	92
08 Notices	92
8.0 Regulatory compliance notices	93
8.0a Class B equipment	93
8.0b Safety warning	93
8.0c Alerte de sécurité	94
8.0d NEBS (Network Equipment Building System) statement	94
8.0e General public license	94



1 Introduction

The Wi-Fi Access Point is Verizon's primary router suitable for residential and small business, featuring high performance, high capacity and advanced routing capabilities.

Your Wi-Fi Access Point features wide Wi-Fi channels, efficient spectrum usage, and fast single-device connection speeds, meeting the demands of customers who require end-to-end Multi-Gig connection services. The superior performance powered by the tri-band architecture and Wi-Fi 7 can meet the low latency and high-speed requirements of video conferencing and voice applications.

1.0 Package contents

Inside the product package for the Wi-Fi Access Point, you should find the following items:

	Quantity
Wi-Fi Access Point	1
Power adapter	1
Ethernet cable, 10 ft (3 meters), white	1

1.1 System requirements

System and software requirements are:

- A computer or other network device supporting Wi-Fi or wired Ethernet
- A web browser such as Chrome™, Firefox®, Internet Explorer 8® or higher, or Safari® 5.1 or higher

1.2 Features

Your Wi-Fi Access Point features include:

- Support for multiple networking standards, including
 - WAN - 10 Gigabit Ethernet
 - LAN - 802.11 a/b/g/n/ac/ax/be
 - LAN - 10 / 2.5 Gigabit Ethernet
 - LAN - 2.5 MoCA interface (requires the MoCA Expansion Module)
- Integrated wired networking with 3-port Ethernet switch and expansion port
 - Ethernet supports speeds up to 10 Gbps
 - Expansion port supports MoCA LAN with speeds over 2500 Mbps
- One Type-C USB 3.0 port
- Integrated Wi-Fi networking with 802.11 a/b/g/n/ac/ax/be access point featuring:
 - backward compatible to 802.11a/b/g/n/ac/ax
 - 2.4 GHz 11ax 4x4
 - 5 GHz 11ax 4x4
 - 6 GHz 11ax 4x4
 - 2.4 / 5 / 6 GHz with MLO
- Enterprise-level security, including:



- Fully customizable firewall with Stateful Packet Inspection (SPI)
- Content filtering with URL-keyword based filtering, parental controls, and customizable filtering policies per computer
- Intrusion detection with Denial of Service protection against IP spoofing attacks, scanning attacks, IP fragment overlap exploit, ping of death, and fragmentation attacks
- Virtual server functionality; providing protected access to internet services such as web, FTP, email, and telnet
- DMZ (demilitarized zone) host support of a network security neutral zone between a private network and the internet
- Event logging
- SIP ALG
- Static NAT
- Port forwarding
- Port triggering
- Access control
- Advanced Wi-Fi protection featuring WPA2 & WPA3 modes and MAC address filtering
- Wi-Fi Multimedia (WMM) for Wi-Fi QoS (quality of service)
- Dual-stack network configuration of IPv4 and IPv6
- DHCP server
- WAN interface auto-detection
- Dynamic DNS
- DNS server
- LAN IP and WAN IP address selection
- MAC address cloning
- QoS support (end-to-end layers 2 and 3) featuring: Differentiated Services (Diffserv), 802.1p/q prioritization, and pass-through of WAN-side DSCPs, Per Hop Behaviors (PHBs), and queuing to LAN-side devices
- Secure remote management using HTTPS or Verizon app
- Static routing
- VPN (VPN pass through only)
- IGMP
- Daylight savings time support



1.3 Getting to know your Wi-Fi Access Point

1.3a Front panel

The Status LED is located towards the bottom of the front panel. It will be solid white when the Wi-Fi Access Point is turned on, connected to the internet, and functioning as intended.



Mode / Type	LED	Wi-Fi Access Point
System	Soft blink white (fading)	Booting
	Solid white	Working as intended (Setup complete)
	50% brightness solid white	Sign of life
	Fast blink red	Overheating
	Slow blink red	Hardware/System Failure/Provisioning Failure
	Solid yellow	No internet connectivity
	Slow blink green	Backend support staff triggerable status
	Fast blink white	Before firmware reboot
Wi-Fi connectivity	Solid white	Wi-Fi active (connected to network)
	Solid green	Wi-Fi disabled (not connected to network)
Pairing	Slow blink blue	DPP pairing in progress on extender (Touchless or QR) ; WPS pairing begins ; Ethernet cable is plugged into an unpaired router/extender ; Coax cable is plugged into an unpaired router/extender MoCA
	Solid yellow (extender only)	DPP pairing failed ; WPS failed ; Ethernet pairing failed ; Coax pairing failed



Extender interactions	Fast blink yellow (extender only)	Extender is too close to router
	Slow blink yellow (extender only)	Extender is too far from router

1.3b Rear panel

The rear panel of your Wi-Fi Access Point has a peel-off label that contains a QR code for setup and support. You can scan it with your smartphone, tablet, or other camera-equipped Wi-Fi device.

There is a permanent label underneath the peel-off label that contains important information about your equipment, including the default settings for the Wi-Fi Access Point's Wi-Fi name (SSID), Wi-Fi password (WPA2 key), local URL for accessing the Wi-Fi Access Point network settings, and network settings password. The permanent label also contains a QR code that you can scan with your camera-equipped Wi-Fi device to allow you to automatically connect your device to your Wi-Fi network without typing in a password (requires a QR code reading app with support for Wi-Fi QR codes).



Rear panel with peel-off label



Rear panel with permanent label

Beneath the labels is a WPS button; beneath the WPS button are 3 Ethernet LAN ports and 1 Ethernet WAN port; lastly there is a USB-C, factory reset button, DC power jack, and an expansion port.

- WPS button - allows quick access to the Wi-Fi Protected Setup (WPS) feature and pairing mode.

The WPS button is used to initiate Wi-Fi Protected Setup. To activate the WPS function, press and hold the WPS button located on the rear of your Wi-Fi Access Point for two to five seconds. When WPS is initiated from your Wi-Fi Access Point, its Status LED slowly flashes blue for up to two minutes, allowing time to complete the WPS pairing process on your Wi-Fi device (also known as a Wi-Fi client). When a device begins connecting to your Wi-Fi Access Point WPS, its Status LED rapidly flashes blue for a few seconds, and then solid white as the connection completes. If the Status LED blinks amber, the Wi-Fi Access Point that functions as an extender is too close to the Wi-Fi Access Point that functions as a router.

If there is an error during the WPS pairing process, the Status LED rapidly flashes red for two minutes.

Refer to section 2.2b "Connecting A Wi-Fi Device Using WPS" for more details.

WPS is one of several ways to connect a Wi-Fi Access Point that functions as an extender. Press the WPS button for three to five seconds on your Wi-Fi Access Point that functions as a router. Within two minutes,



press the WPS button for three to five seconds on the Wi-Fi Access Point that will function as an extender. As the two units establish a connection, the Status LED blinks a blue light. The Status LED will turn solid white when the pairing completes successfully.

- Ethernet LAN - connects devices to your Wi-Fi Access Point using Ethernet cables to join the local area network (LAN). There are three Ethernet LAN ports:
 - one 10 GE LAN port supports 1/2.5/5/10 Gbps auto-sensing
 - two 2.5 GE LAN ports support 10/100 Mbps and 1/2.5 Gbps auto-sensing
- 10 GE WAN - connects your Wi-Fi Access Point to the internet using an Ethernet cable
- Type-C USB - provides up to 1 A at 5 V dc (for power/charging)
- Reset button - allows you to perform a soft reboot or reset to the factory default settings. For a soft reboot, press and hold the button for at least three seconds. For a reset to factory default settings, press and hold the button for at least ten seconds
- Power - connects your Wi-Fi Access Point to an electrical wall outlet using the supplied power adapter

Warning: The included power adapter is for home or office use only, supporting voltages from 105-125 Vac. Do not use it in environments with greater than 125 Vac.

1.3c Rear lighted indicators

LAN/WAN Ethernet

- Unlit - Indicates no Ethernet link or dims after 5 minutes idle

Left LED

- Solid yellow - Indicates less than 1 Gbps link
- Flash yellow Indicates LAN/WAN activity. The traffic can be in either direction

Right LED

- Solid white - Indicates 1/2.5/5/10 Gbps link
- Blinking white - Indicates LAN/WAN activity. The traffic can be either direction

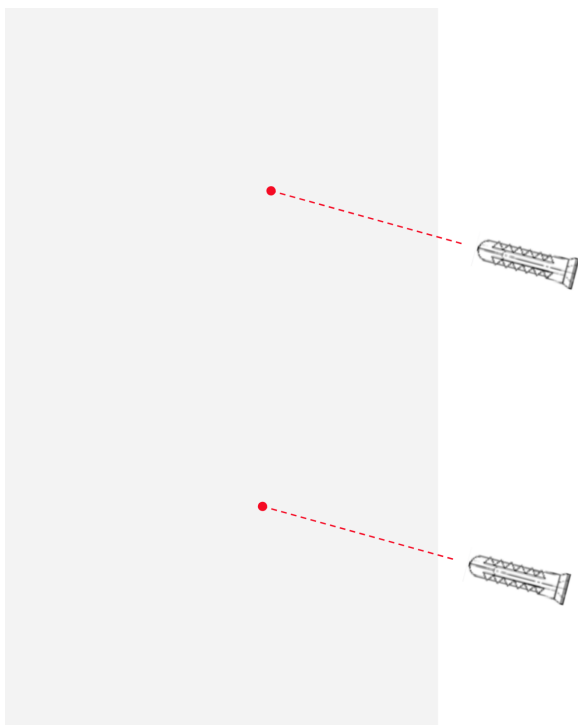
1.3d Mounting the Wi-Fi Access Point to a wall

For optimum performance, the Wi-Fi Access Point is designed to stand in a vertical upright position. Verizon does not recommend wall mounting the Wi-Fi Access Point. However, if you wish to mount your Wi-Fi Access Point, you can purchase a mounting bracket from the Verizon Accessories Store at verizon.com/smallbusiness/accessories/mounting-bracket/

To mount your Wi-Fi Access Point to a wall:

1. Select a mounting spot near a power outlet and the Ethernet port of the device that provides internet on your premises.
2. Mark screw hole positions on the wall. Drill holes for the wall anchors using a 1/4 inch (6.35 mm) drill bit.
3. Insert the anchors in the drilled holes and hammer until they are flush with the wall.



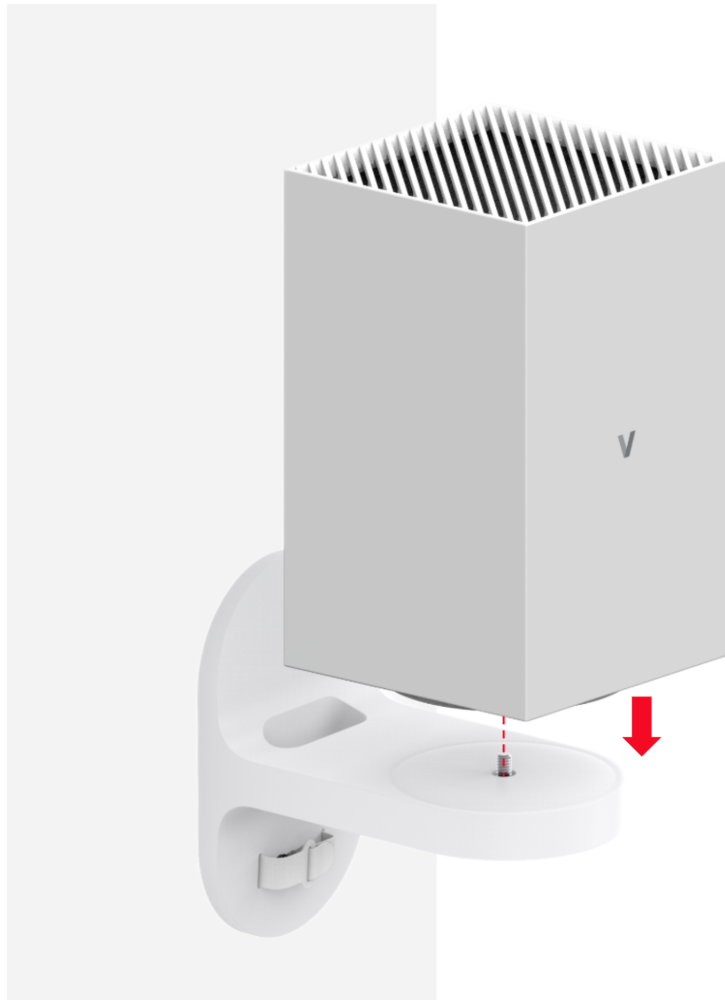


4. Place the screws into the small holes of the bracket and tighten the screws into your wall for securing the wall mount bracket.



5. Align the mounting hole located on the bottom of the Wi-Fi Access Point to the screw of the wall mount bracket.



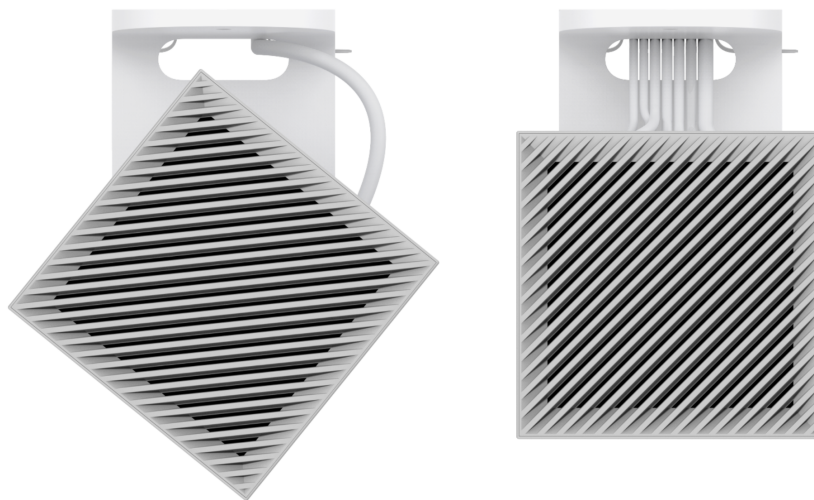


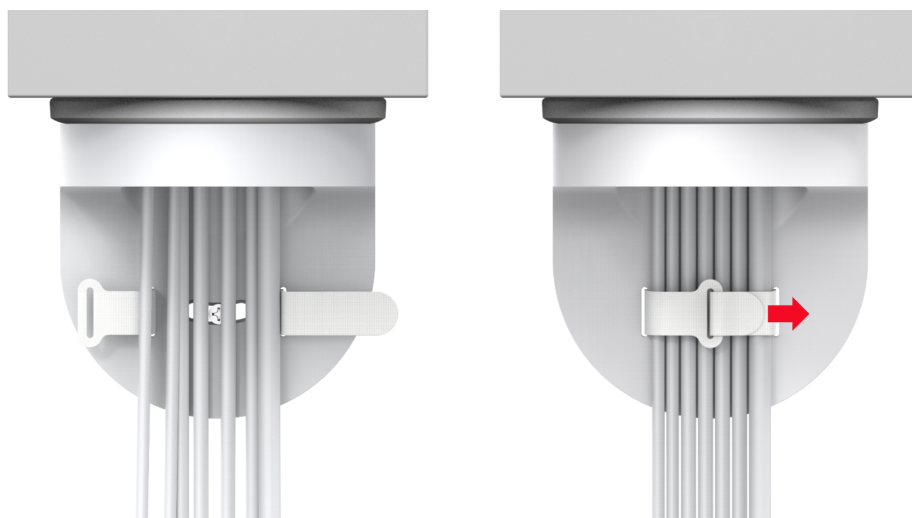
6. Rotate and align the router to the preferred position. While using the hole in the mounting bracket, connect the Ethernet cable providing internet to the router's WAN port and other cables as needed. Tighten the bracket screw to lock the device in place.





7. To fasten the attached cables of the Router, manage the cables, then tighten the Velcro® strap with buckle.





02 Connecting your Wi-Fi Access Point

Connecting your Wi-Fi Access Point and accessing its web-based User Interface (UI) are simple procedures. Accessing the UI may vary slightly depending on your device's operating system and web browser.

2.0 Setting up your Wi-Fi Access Point



Scan the QR code to use the app for step-by-step setup instructions or follow these instructions.

Before you begin, if you're replacing an existing router, disconnect it. Remove all old internet equipment as they will not work with your new Wi-Fi Access Point.



2.0a Installation instructions

Static IP

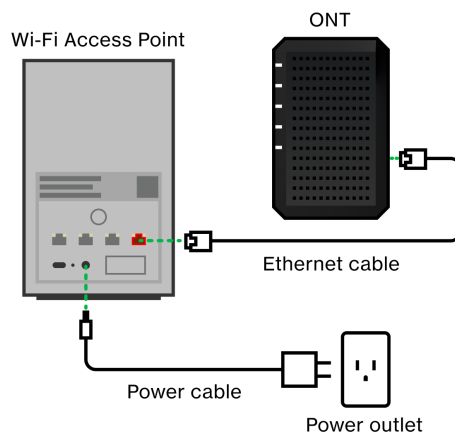
Most customers with Fios Business Internet have Dynamic IP addressing. If this is what you ordered, or if you ordered Fios TV only, then proceed to the instructions below for Dynamic IP.

If you ordered Fios Internet with Static IP, then:

1. Perform step 1 (only) in the Dynamic IP section below.
2. Call 800.verizon and follow the prompts to Repair to connect with an agent. The agent will guide you through the installation including auto-configuring the Static IP address on your Wi-Fi Access Point router.

Dynamic IP

1. Connect the Wi-Fi Access Point to the ONT.
 - Connect the red WAN port on the Wi-Fi Access Point to the ONT using an Ethernet cable.
 - If your ONT was installed in another room, you may have an Ethernet outlet on the wall or a loose Ethernet cable coming from the ONT location.
 - If you have a wall plate, connect one end of the Ethernet cable that came with your Wi-Fi Access Point to the wall plate and the other end to the red WAN port on the ONT.
 - If you have a loose Ethernet cable, connect it to the red WAN port on the Wi-Fi Access Point.
2. Connect the Wi-Fi Access Point to power.
 - Connect the Wi-Fi Access Point's power adapter and plug it into a power outlet.
3. Wait for the Wi-Fi Access Point's light to turn solid white.
 - The Wi-Fi Access Point will take up to 10 minutes to update. Continue to step 4 when the light turns solid white.



4. Connect your devices

Wired or Wi-Fi? Your choice.

Wired

- Connect the Ethernet cable to any LAN port on your Wi-Fi Access Point.
- Connect the other end to your computer.
- **Note:** You can also connect the Wi-Fi Access Point to a Coax port using a MoCA Expansion Module (not included). (May be required for Fios TV)
 - Separate subscription required for Fios TV; not available in all areas.

Wi-Fi

- Get the Wi-Fi name and password off the label at the back of your Wi-Fi Access Point.
- On your device, choose your Wi-Fi name when it appears.
- Enter the Wi-Fi password exactly as it appears on your router label.

Wi-Fi Network

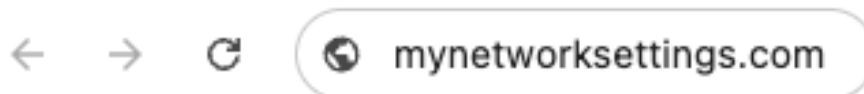
The Wi-Fi Access Point has one Wi-Fi name supporting 2.4, 5, and 6 GHz signals. The Self-Organizing Network (SON) feature lets your devices move between these signals automatically for an optimized Wi-Fi connection.

5. Complete Activation

Activate your service by opening a web browser on your computer and following the prompts.

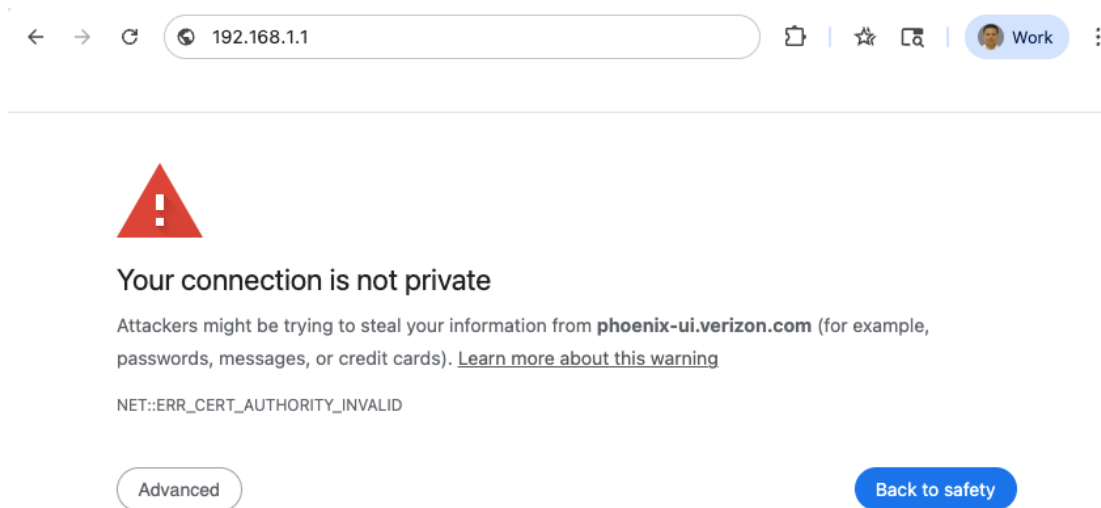
2.0b Configure your Wi-Fi Access Point

1. Open a web browser on the device connected to your Wi-Fi Access Point network.
2. In the browser address field (URL), enter mynetworksettings.com then press the Enter key on your keyboard. Alternatively, 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 UI management. To get to the login screen, click the ADVANCED button, then on Proceed to 192.168.1.1 (unsafe) link.

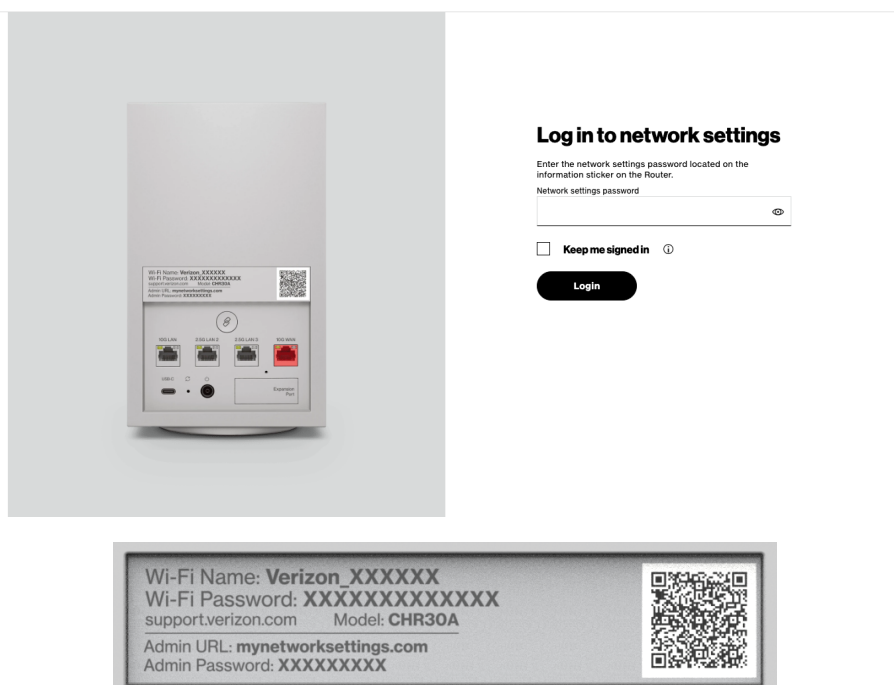




4. The login screen will appear.

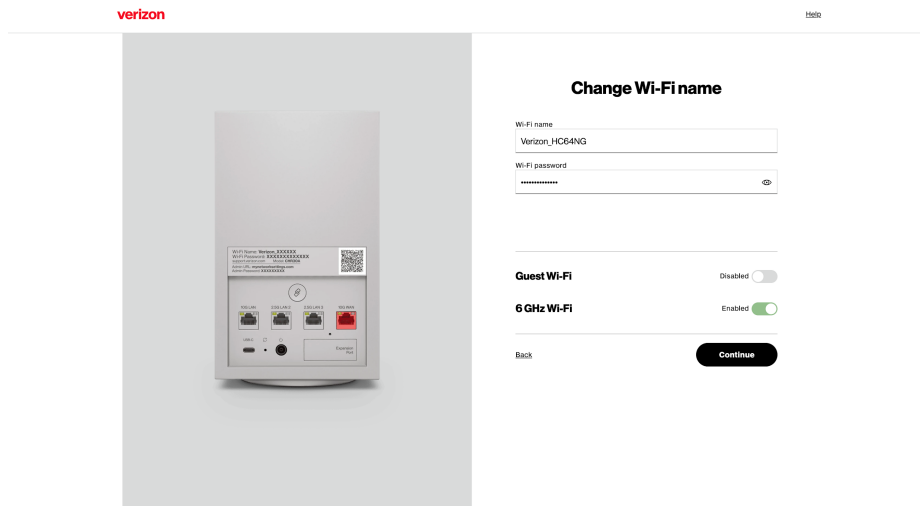
The first time you access your Wi-Fi Access Point, the Quick Setup Wizard displays to help you step through the setup process.

5. On the **Log in to network settings** screen, enter the password that is printed next to the Admin Password on the label on the rear of your Wi-Fi Access Point. Click **Login**.

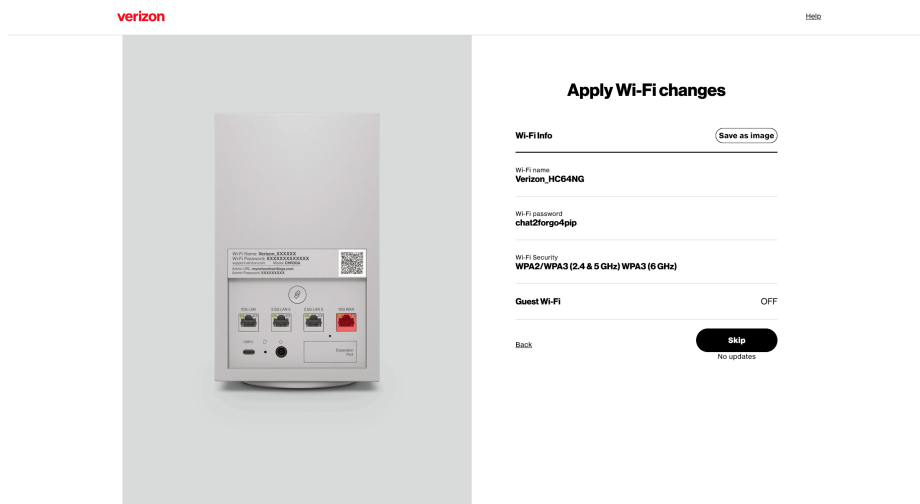


6. The Change Wi-Fi name screen displays. You can continue with the default settings or customize them as needed. This is the best setting for most users and allows the most devices to securely connect.





7. You can optionally set up the Guest Wi-Fi network by toggling the selection to On. You can continue with the default settings or customize them as needed.
8. The IoT Wi-Fi will also be enabled for any devices that do not support WPA3, and this will use a unique Wi-Fi name and password based on the default SSID & Password. Devices on this Wi-Fi will be able to communicate with other devices on the Primary network with no firewall restrictions separating them.
9. Click Continue to review your settings.
10. The Apply Wi-Fi changes screen is displayed. Review your current settings. You may optionally save your settings as an image on your device by selecting the button, Save as Image. Click Apply to save the Wi-Fi changes to your Wi-Fi Access Point.

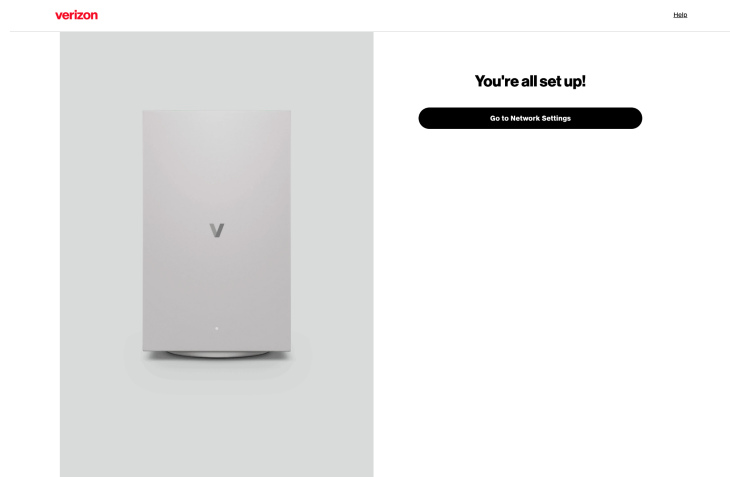


Note: If you select Save as image, the image file is saved to your web browser's download folder.

Important: Your Wi-Fi connected device will disconnect from the Wi-Fi Access Point if changes are made to the Wi-Fi name or password. Reconnect by selecting your customized network name, from the list of available Wi-Fi networks, and enter your customized Wi-Fi password.



The **You're all set up!** screen appears once your Wi-Fi Access Point 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 UI screen.



If your Wi-Fi Access Point is subsequently reset to the factory default settings, the settings printed on the permanent label will again be in effect.

If your Wi-Fi Access Point fails to connect, follow the troubleshooting steps in the Troubleshooting section of this guide.

2.1 Expanding Wi-Fi coverage

Connecting one or more Wi-Fi Access Points that function as extenders to a Wi-Fi Access Point that functions as a router allows you to extend the Wi-Fi signal range and eliminate Wi-Fi dead zones in your Wi-Fi network. Refer to the self-setup flow in My Verizon app.

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 is.

2.2a Configuring dynamic IP addressing

To configure a computer to use dynamic IP addressing:

Windows 11

1. On the Windows desktop, open the **Control Panel** by searching for it in the **Start** menu.
2. Navigate to **Network and Internet > Network and Sharing Center**.
3. Click **Change adapter settings** in the left-hand pane.
4. Right-click your Ethernet adapter and choose **Properties**.
5. Select **Internet Protocol Version 4 (TCP/IPv4)** from the list, and then click **Properties**.
6. Ensure that both of the following options are selected:
 - Obtain an IP address automatically
 - Obtain DNS server address automatically



7. Click OK on both windows to apply the changes and close them.

Macintosh OS X

1. Click the **Apple** icon in the top left corner of the desktop. A menu appears.
2. Select **System Preferences**. The System Preferences window appears
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

Your devices such as computers and set top boxes can wirelessly connect to the Wi-Fi Access Point using Wi-Fi connectivity. Or you can have wired connections using cables such as Ethernet or coax.

Ethernet

1. Plug one end of an Ethernet cable into one of the three LAN Ethernet ports on the back of the Wi-Fi Access Point.
2. Plug the other end of the Ethernet cable into the Ethernet port on the computer.
3. Repeat the above two steps for each computer to be connected to an available LAN Ethernet port on the back of the Wi-Fi Access Point.

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 Wi-Fi Access Point creates a secure Wi-Fi network connection.

In most cases, WPS only requires the pressing of two buttons - one on your Wi-Fi Access Point and the other on the Wi-Fi client. The WPS buttons can be physical or virtual buttons.

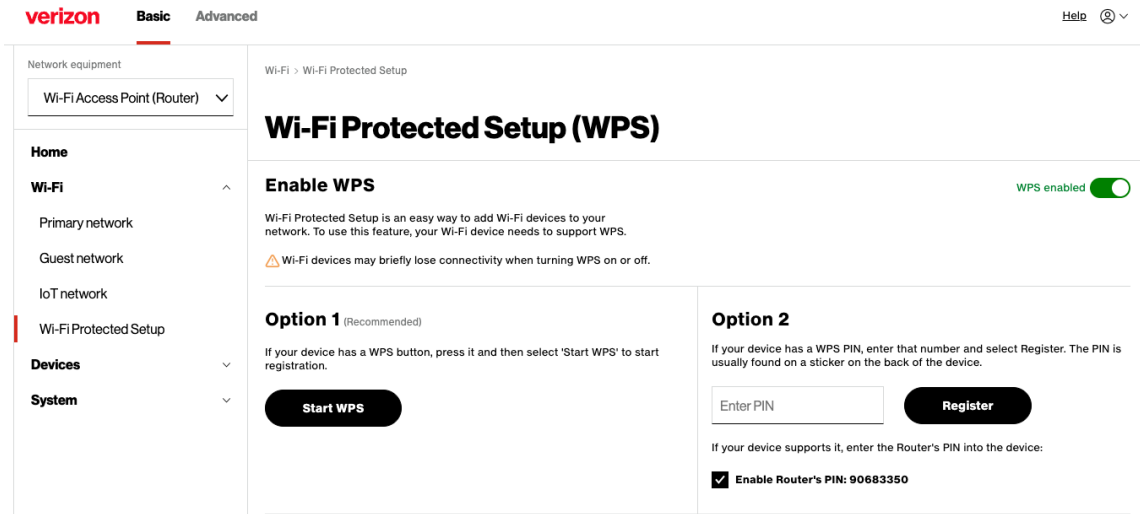
To initiate the WPS process, you can either press and hold the WPS button located on the rear of your Wi-Fi Access Point for more than two seconds or use the UI and press the on-screen button.

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 WPS button on your Wi-Fi Access Point for more than two seconds, then click the Start WPS button in 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 Enter PIN field located in Option 2 on the user interface. Click Register.
 - Alternatively, you can enter the Wi-Fi Access Point'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 Wi-Fi Access Point, 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 Wi-Fi Access Point is pressed, the Status LED begins flashing blue. The flashing continues until WPS pairing to the client device completes successfully. At this time, the Wi-Fi Access Point's Status LED turns solid white.

If WPS fails to establish a connection to a Wi-Fi client device within two minutes, the Wi-Fi Access Point's Status LED 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 WPS3 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 Wi-Fi Access Point's Wi-Fi network name (SSID) from the device's list of discovered Wi-Fi networks.
4. When prompted, enter your Wi-Fi Access Point's Wi-Fi password (WPA2 or WPA3 key) into the device's Wi-Fi settings. Your Wi-Fi Access Point's default Wi-Fi network name and password are located on the permanent label on the rear panel of your Wi-Fi Access Point.

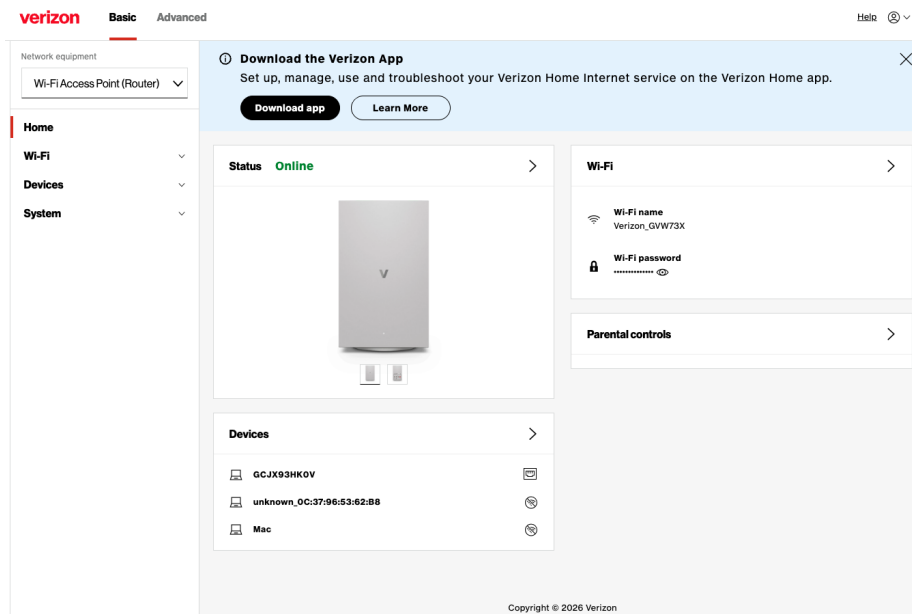




5. Verify the changes were implemented by using the device's web browser to access a site on the internet.
6. Repeat these steps for every device that you are connecting with Wi-Fi to your Wi-Fi Access Point.

2.3 Main screen

When you log into your Wi-Fi Access Point, the dashboard main page shows Basic and Advanced menus along the top, and displays summary tiles for connection Status, Devices, Wi-Fi, and Parental Controls, and also provides navigation links via the left-hand menu.



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

- Basic settings
 - Home & 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 Wi-Fi Access Point's status by clicking System\ System Status on the screen.
This section displays the status of your Wi-Fi Access Point's local network (LAN) and internet connection



(WAN), firmware and hardware version numbers, MAC Address, IP settings of the Wi-Fi Access Point that functions as a router and the Wi-Fi Access Points that function as extenders (if connected).

verizon

Basic

Advanced

Help

Network equipment

Wi-Fi Access Point (Router)

Home

Wi-Fi

Devices

System

System status

Open source software

System > System status

System status

Auto-refresh

Refresh

Broadband IPv4

Status
Connected

IPv4 address is from:
DHCP

IPv4 address
10.76.216.149

Subnet mask
255.255.255.0

IPv4 default gateway
10.76.216.1

IPv4 DNS address 1
208.52.253.24

IPv4 DNS address 2
208.52.253.88

NATs supported (used / max)
47/30000

Broadband IPv6

Status
Connected

IPv6 address is from:
DHCPv6-PD

Delegated prefix

IPv6 address
2001:d10:226:57:1

Link-local address
fe80:2641:feff:fe11:9410

IPv6 default gateway
fe80:2ef8:9bff:fe90:2abf

IPv6 DNS address 1

IPv6 DNS address 2

Network equipment

Wi-Fi Access Point (Router)

Home

Wi-Fi

Devices

System

System status

Open source software

System > System status

System status

Auto-refresh

Refresh

Router

Firmware version
4.1.6.26d

Hardware version
0.0.3

Wi-Fi chipset version
WLAN.WBE1.3.1-00130-QCAHKSWPL_SILICONZ-1.852031.887341

Model name
CHR30A-R

Serial number
ACY44200101

LAN IPv4 address
192.168.1.1

Broadband MAC address
24:41:FE:1F:94:10

Broadband physical connection
Ethernet

Router has been active for
0 day(s) 6 hours 4 minutes 24 seconds

LED status
Normal Operation

Open source software

verizon

Basic

Advanced

Help

Network equipment

Wi-Fi Access Point (Router)

Home

Wi-Fi

Devices

System

System status

Open source software

System > Open source software

Open source software

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.

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



03 Wi-Fi 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.

3.0 Overview

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

The Wi-Fi Access Point supports 2.4 GHz, 5 GHz, and 6 GHz Wi-Fi bands, and the operation modes and speeds are listed as follows:

2.4 GHz

- Legacy operation mode:
 - Supports IEEE 802.11b/g/n with maximum theoretical rate of 600 Mbps
- Compatibility mode:
 - Supports IEEE 802.11ax
 - Backward compatible with IEEE 802.11b/g/n/ac
 - Maximum theoretical rate up to 1.1 Gbps

5 GHz

- Legacy operation mode:
 - Supports IEEE 802.11a/n/ac with maximum theoretical rate of 2.2 Gbps
- Compatibility mode:
 - Supports IEEE 802.11ax
 - Backward compatible with IEEE 802.11a/n/ac
 - Maximum theoretical rate up to 2.4 Gbps

6 GHz

- Operation mode:
 - Supports IEEE 802.11ax
 - Maximum rate up to 4.8 Gbps

The Wi-Fi service and Wi-Fi security are activated by default.

The level of security is preset to WPA2/3 (2.4 & 5 GHz) & WPA3 (6 GHz) encryption using a unique default key (also referred to as a passphrase or password) pre-configured at the factory. This information is displayed on a sticker located on the rear of your Wi-Fi Access Point.

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

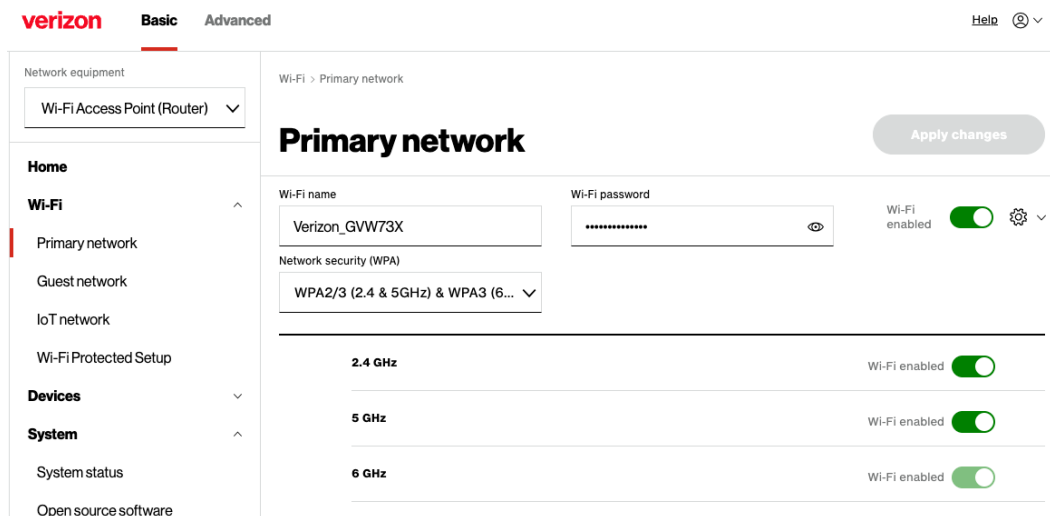




3.1 Basic settings

3.1a Primary network

You can configure the basic security settings for 2.4 GHz, 5 GHz, or 6 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 office 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.
4. To configure the Wi-Fi Security, click the setup button and select WPA2 or WPA3. You can optionally enable the 6 GHz Wi-Fi band by toggling the selection to On. Enabling 6 GHz will modify the existing 2.4 & 5 GHz security from WPA2 to WPA2/WPA3 and 6 GHz will be enabled using WPA3.

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

Broadcast Wi-Fi network name (SSID)

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

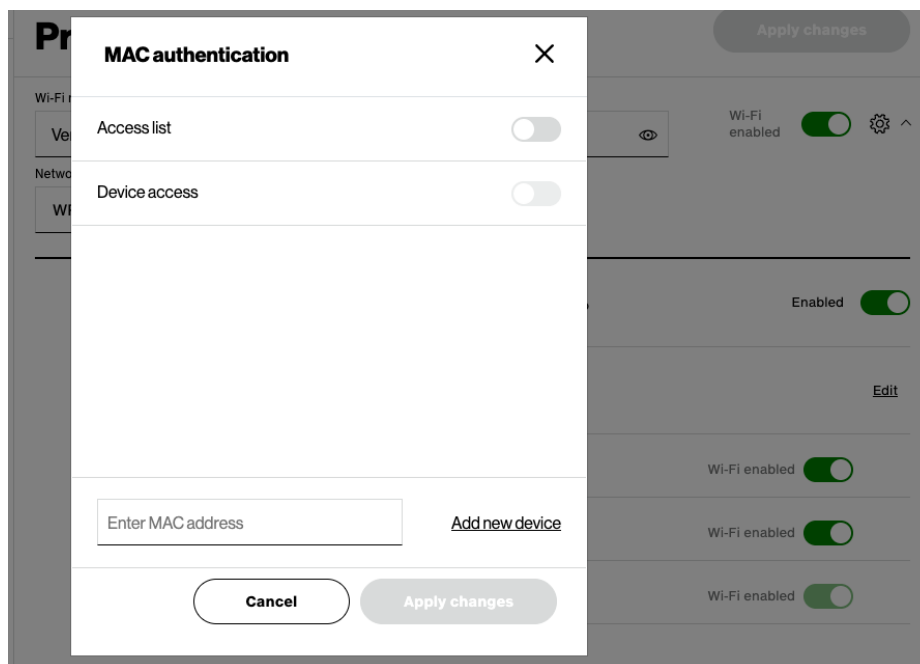
- To enable SSID broadcasting, move the selector to on. SSID broadcast is enabled by default. The SSID of the Wi-Fi network will be broadcasted to all Wi-Fi devices.



- 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 Wi-Fi Access Point to limit access to your Wi-Fi network to only those devices with specific MAC addresses.



To set Wi-Fi MAC authentication:

1. To set up 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.

 - 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 while restricting 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 Wi-Fi Access Point 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 at the rear of the router followed by hyphen guest (-Guest). For example, if the router is shipped with a default SSID of "Verizon-ABCDE" then the default SSID for Guest Wi-Fi is "Verizon-ABCDE-Guest".



The screenshot shows the Verizon router's configuration interface. At the top, there are tabs for 'Basic' and 'Advanced'. The 'Basic' tab is selected. On the left, there is a sidebar menu with options: 'Home', 'Wi-Fi', 'Primary network', 'Guest network', 'IoT network', 'Wi-Fi Protected Setup', 'Devices', 'System', 'System status', and 'Open source software'. The 'Wi-Fi' option is expanded, and 'Guest network' is selected. The main content area is titled 'Guest network' and contains the following settings:

- Wi-Fi name:** A text field containing 'Verizon_GVW73X-Guest'.
- Wi-Fi password:** A text field with masked characters (dots) and an eye icon to toggle visibility.
- Wi-Fi disabled:** A toggle switch that is currently turned off.
- Network security (WPA):** A dropdown menu showing 'WPA2'.
- Frequency bands:** Three rows for '2.4 GHz', '5 GHz', and '6 GHz'. Each row has a 'Wi-Fi disabled' toggle switch, all of which are currently turned off.

An 'Apply changes' button is located in the top right corner of the configuration area.

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.

3.1c IoT network

The router 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 Wi-Fi Access Point 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 at the rear of the router followed by hyphen IoT (-IoT). For example, if the router is shipped with a default SSID of "Verizon-ABCDE" then the default SSID for IoT Wi-Fi is "Verizon-ABCDE-IoT".



The screenshot shows the Verizon Basic menu interface. On the left, the 'Wi-Fi' section is expanded, and 'IoT network' is selected. The main content area is titled 'IoT network' and includes an 'Apply changes' button. Below the title, there are settings for '2.4 GHz', 'Wi-Fi name' (set to 'Verizon_GVW73X-IoT'), 'Wi-Fi password' (masked with dots), and 'Network security (WPA)' (set to 'WPA2'). A 'Wi-Fi disabled' toggle switch is also present.

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 Wi-Fi Access Point creates a secure Wi-Fi network connection.

In most cases, this only requires the pressing of two buttons – one on your Wi-Fi Access Point 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 WPS button located on the back of your Wi-Fi Access Point 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 and then click Wi-Fi Protected Setup (WPS).



verizon

Basic

Advanced

[Help](#)

Network equipment

Wi-Fi Access Point (Router)

▼

Home

Wi-Fi

Primary network

Guest network

IoT network

Wi-Fi Protected Setup

Devices

System

System status

Open source software

Wi-Fi > Wi-Fi Protected Setup

Wi-Fi Protected Setup (WPS)

Enable WPS

WPS enabled

Wi-Fi Protected Setup is an easy way to add Wi-Fi devices to your network. To use this feature, your Wi-Fi device needs to support WPS.

⚠ Wi-Fi devices may briefly lose connectivity when turning WPS on or off.

Option 1 (Recommended)

If your device has a WPS button, press it and then select 'Start WPS' to start registration.

Start WPS

Option 2

If your device has a WPS PIN, enter that number and select Register. The PIN is usually found on a sticker on the back of the device.

Register

If your device supports it, enter the Router's PIN into the device:

☒ Enable Router's PIN: 90683350

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 Wi-Fi Access Point for more than two seconds, then click the Start WPS button in Option 1 to start the WPS registration process.
 - If the client device has a WPS PIN, you can find it printed on the device's label or in its documentation. Once located, enter this PIN into Option 2 on the user interface. Click Register.
 - Alternatively, if your Wi-Fi device supports PIN mode, you have the option to enter the Wi-Fi Access Point's PIN, which is displayed on this screen, into your device's WPS user interface.
4. After pressing the WPS button on your Access Point, 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 Access Point is pressed, the Status LED on the front of your Access Point begins flashing blue. The flashing continues until WPS pairing to the client device completes successfully. At this time, the Status LED turns solid white.

If WPS fails to establish a connection to a Wi-Fi client device within two minutes, the Status LED on your Access Point 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.

3.2 Advanced settings

3.2a Primary network

Self-Organizing Network (SON)



The Wi-Fi Access Point supports 2.4 GHz, 5 GHz and 6 GHz signals. The Self-Organizing Network (SON) feature lets your devices move between these signals automatically for an optimized Wi-Fi connection.

The screenshot displays the Verizon Advanced settings interface for a Wi-Fi Access Point (Router). The left sidebar contains a navigation menu with options: Home, Wi-Fi (selected), Guest network, IoT network, Wi-Fi Protected Setup, Radio management, Devices, Security & firewall, Network settings, Diagnostics & monitoring, and System. The main content area is titled 'Primary network' and includes an 'Apply changes' button. It features input fields for 'Wi-Fi name' (Verizon_GVW73X) and 'Wi-Fi password' (masked with dots). Below these is a 'Network security (WPA)' dropdown menu set to 'WPA2/3 (2.4 & 5GHz) & WPA3 (6...'. Three frequency bands are listed: 2.4 GHz, 5 GHz, and 6 GHz, each with a 'Wi-Fi enabled' toggle switch (all are turned on) and a settings gear icon. At the bottom, the 'Self-Organizing Network' feature is shown as 'Enabled' with a link to 'Setup'.

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. The disable/enable option for SON is now available.
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.



The screenshot displays the 'Primary network' configuration page for a Verizon router. The interface includes a left-hand navigation menu with categories like Home, Wi-Fi, Devices, Security & firewall, Network settings, Diagnostics & monitoring, and System. The main content area is titled 'Primary network' and contains several settings:

- Wi-Fi name:** A text field containing 'Verizon_GVW73X'.
- Wi-Fi password:** A masked text field with a toggle to show/hide the password.
- Wi-Fi enabled:** A toggle switch that is currently turned on.
- Network security (WPA):** A dropdown menu set to 'WPA2/3 (2.4 & 5GHz) & WPA3 (6...'.
- 2.4 GHz band:** Includes a 'Wi-Fi enabled' toggle (on) and a 'Group Key' section.
- 5 GHz band:** Includes a 'Wi-Fi enabled' toggle (on) and a 'Wi-Fi QoS (WMM)' section.
- Group Key:** A section for updating the WPA shared key, with a text field showing '259200' and an 'Enabled' toggle (on).
- Wi-Fi QoS (WMM):** A section for improving service quality, with an 'Enabled' toggle (on).
- WMM Power Save:** A section for improving battery life, with an 'Enabled' toggle (on).

An 'Apply changes' button is located in the top right corner of the settings area.

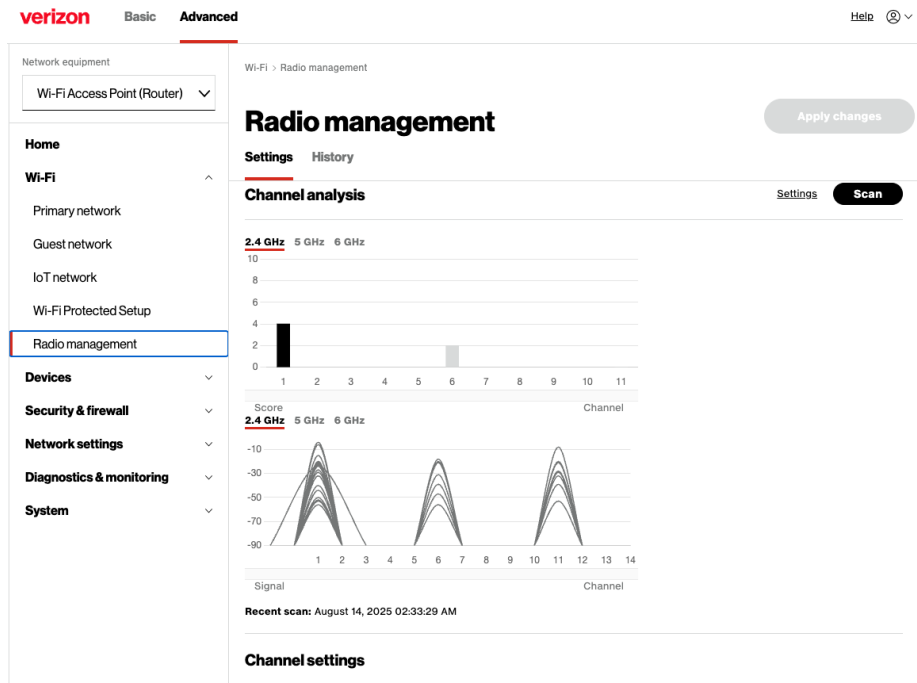
Caution: These settings should only be configured by experienced network technicians. Changing the settings could adversely affect the operation of your router and your local network.

- 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

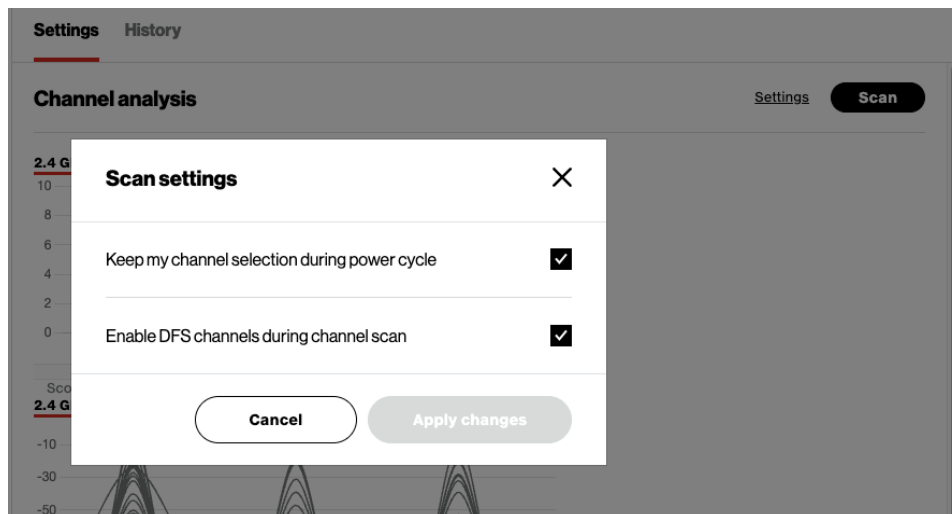
You can configure the channel settings for the 2.4 GHz, 5 GHz and 6 GHz band(s) of your Wi-Fi network.





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 Wi-Fi Access Point 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 routers using them. Examples include some media streaming devices. Disabling this feature will allow the router to select the best available channel to broadcast on and allow these devices to connect.
- Press Apply changes to save the changes.



3. Click Scan to perform a channel availability scan for the Wi-Fi Access Point to identify the radio channels providing the best Wi-Fi performance.
4. On the Radio Management page for 2.4 GHz, 5 GHz or 6 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 zero to ten in each Wi-Fi channel. It can be used to determine which channels to use or to avoid. A higher score indicates less congestion in a channel.
 - Channel Settings - this is the radio channel used by the Wi-Fi Access Point and its clients to communicate with each other. The channel must be the same on the Wi-Fi Access Point 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 Wi-Fi Access Point will automatically assign itself a radio channel.
 - Width - displays the bandwidth available to 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, 5 GHz, 6 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 - The default mode setting for both 5 GHz and 6 GHz. It offers an optimal balance between performance and interoperability, allowing 802.11n, ac, ax, and be Wi-Fi devices to connect.
- Legacy - The default mode for the 2.4 GHz band offers extensive compatibility, supporting both older and newer Wi-Fi devices that use 802.11a, b, g, n, or ac standards.

Note: 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.

To view the channel settings history:

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

Band	Channel	Time	Date
5 GHz	Ch. 149	10:44am	03 / 06 / 25
5 GHz	Ch. 36	10:43am	03 / 06 / 25
5 GHz	Ch. 149	9:27am	03 / 06 / 25
5 GHz	Ch. 36	9:27am	03 / 06 / 25
5 GHz	Ch. 149	9:18am	03 / 06 / 25
5 GHz	Ch. 36	9:18am	03 / 06 / 25
5 GHz	Ch. 149	8:59am	03 / 06 / 25
6 GHz	Ch. 181	8:59am	03 / 06 / 25
2.4 GHz	Ch. 11	8:59am	03 / 06 / 25
6 GHz	Ch. 181	8:59am	03 / 06 / 25



04 Connected devices

You can view the settings of the network devices connected to your Wi-Fi Access Point's network.

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

With that question in mind, your Wi-Fi Access Point's parental controls were designed to allow control of internet access on all locally networked devices.

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.

verizon

Basic

Advanced

Help ⓘ

Network equipment

Wi-Fi Access Point (Router)

Home

Wi-Fi

Devices

Devices

Parental controls

System

Devices > Devices > All

Devices

Add device

All (1) Primary (1) Guest (0) IoT (0)

Online

Name	Connection	Connected to	MAC address	Parental controls
GCJX93HKOV	Ethernet	CHR30A	98:E7:43:0A:32:AF	None

Offline

unknown_0C:37:96:53:62:B8	Offline	CHR30A	0C:37:96:53:62:B8	None
Mac	Offline	CHR30A	9A:21:FC:1C:ED:E1	None

verizon

Basic

Advanced

Help ⓘ

Network equipment

Wi-Fi Access Point (Router)

Home

Wi-Fi

Devices

Devices

Parental controls

System

Devices > Devices > All

Devices

Add device

All (1) Primary (1) Guest (0) IoT (0)

Connection	Connected to	MAC address	Parental controls	Block/Allow	
Ethernet	CHR30A	98:E7:43:0A:32:AF	None	☒	⚙️

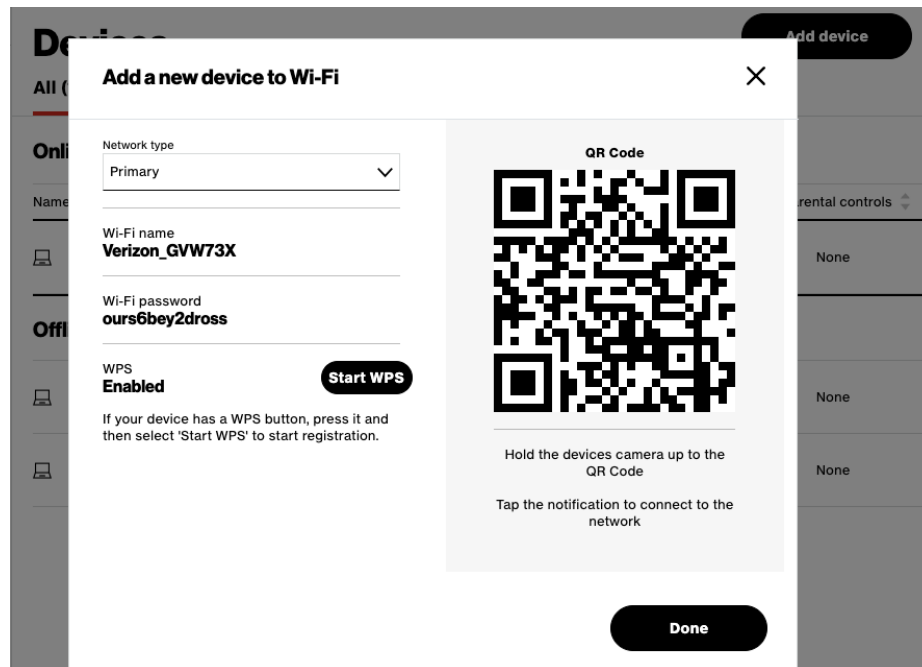
Clear list

Offline	CHR30A	0C:37:96:53:62:B8	None	☒	🗑️ ⚙️
Offline	CHR30A	9A:21:FC:1C:ED:E1	None	☒	🗑️ ⚙️



3. To easily add a new device to the network:

- Click the Add Device button on the screen.
- Select the preferred Network type from the dropdown list (Primary, Guest or IoT).
- Scan the provided QR code with the new device's camera.
- Tap the push notification to connect the device to your network.



- You can add the new device to your Wi-Fi network by clicking the Start WPS button if your Wi-Fi device supports the WPS feature. Refer to “3.1d/ Wi-Fi Protected Setup (WPS)” for detailed information.
 - Click Done to save the changes.
4. Click and drag the horizontal scrolling bar to the right of the screen for device configuration.
5. Click the Block/Allow option to quickly disable/enable a device from having internet access.
6. Click the Settings icon to access the Device Settings page for that device:



verizon Basic Advanced Help

Network equipment
Wi-Fi Access Point (Router)

Home
Wi-Fi
Devices
Parental controls
System

Devices > Devices > Device settings

Device settings

Save

Device information

Edit

Reset to default

Device
Online

Desktop/Laptop

Name
GCJX93HK0V

Host name
GCJX93HK0V

Location
Select

Mobility
Portable

Device Add-Ons

Port forwarding N/A	DMZ host N/A
Access control N/A	Parental controls N/A
Static NAT N/A	IPv6 pinholes N/A
	Static IP GCJX93HK0V

verizon Basic Advanced Help

Network equipment
Wi-Fi Access Point (Router)

Home
Wi-Fi
Devices
Parental controls
System

Devices > Devices > Device settings

Device settings

Save

Device Connection

Connection info

Connection
Ethernet

Phy rate / Modulation rate
1000 Mbps

Network info

Mac address
98:E7:43:0A:32:AF

Connected to
CHR30A

IPv4 address
192.168.1.3

Subnet mask
255.255.255.0

IPv4 DNS
192.168.1.1

IPv4 address allocation
Dynamic

Lease type
DHCP

DHCP lease time remaining
23 hours 30 minutes 25 seconds

IPv6 LAN prefix

IPv6 global

IPv6 type / Address allocation
Stateless

IPv6 link-local
fe80::85c:b8ee:ca6b:db33

- 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.
 - 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 DMZ Host 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 DNS Server 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

You will need to scan the QR code to download the My Verizon app. Parental controls can be set and managed within the app. The My Verizon app is also available in the App Store and Play Store.

My Verizon app

- Apple's App Store: <https://apps.apple.com/us/app/my-verizon/id416023011>
- Google's Play Store: <https://play.google.com/store/apps/details?id=com.vzw.hss.myverizon>

or scan this QR code:



4.2 Universal plug & play

You can use Universal Plug and Play (UPnP) to support new devices without configuring or rebooting your Wi-Fi Access Point.

In addition, you can enable the automatic cleanup of invalid rules. When enabled, this functionality verifies the validity of all UPnP services and rules every five minutes. Old and unused UPnP defined services are removed, unless a user-defined rule depends on it.

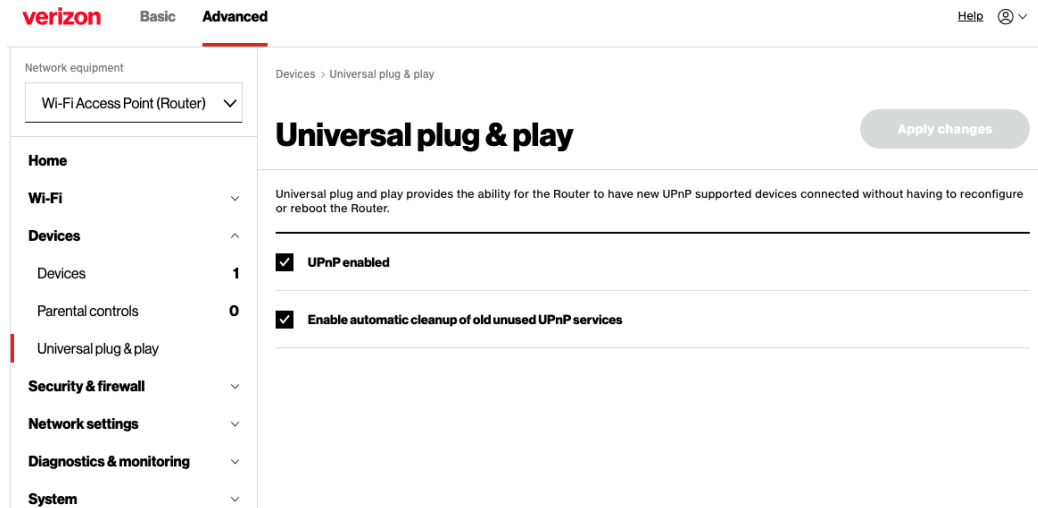
UPnP services are not deleted when disconnecting a computer without proper shutdown of the UPnP applications, such as messenger. Services may often not be deleted and eventually this leads to the



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

Advanced settings cover a wide range of sophisticated configurations for your Wi-Fi Access Point's firmware, security setup and network.

Wi-Fi Access Point'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 - manages the security level for the firewall
- Access control - restricts 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 - provides an access tunnel to a service on a host for a particular application
- Port forwarding - enables access from the internet to specified services provided by computers on the local network
- Port forwarding rules - displays port forwarding rules
- Port triggering - defines 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 - allows multiple static NAT IP addresses to be designated to devices on the network

Diagnostics & monitoring

- 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 Wi-Fi Access Point to its default settings
- LED brightness - controls the Status LED light to either dim or bright
- Reboot router - restarts your Wi-Fi Access Point
- Remote administration - enables remote configuration of your Wi-Fi Access Point 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 Wi-Fi Access Point. It 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 Wi-Fi Access Point or



rejected and barred from passing through, 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.

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 a computer on your local network attempts to access a website on the internet, it sends a request. When the request reaches your Wi-Fi Access Point, the firewall identifies the request type and origin, such as HTTP and a specific computer in the local network. Unless your Wi-Fi Access Point 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 by the web server, the firewall associates the website with this session and allows it to pass. 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.



verizon Basic **Advanced** Help ⓘ

Network equipment
Wi-Fi Access Point (Router) ▼

Home
Wi-Fi ▼
Devices ^
Devices 1
Parental controls 0
Universal plug & play
Security & firewall ^
General
Access control
DMZ host
IPv6 pinholes
Port forwarding
Port forwarding rules
Port triggering
Scheduler rules
SIP ALG
Network settings ▼

Security & firewall > General

General Apply changes

IPv4 settings

☐ **High security**
Remote administration will override the security inbound policy
Inbound rule Outbound rule ▼
Outbound set top box traffic disabled

☒ **Normal security**
Remote administration will override the security inbound policy
Inbound rule Outbound rule

☐ **Low security**
Remote administration will override the security inbound policy
Inbound rule Outbound rule

IPv6 settings

☐ **High security**
Remote administration will override the security inbound policy
Inbound rule Outbound rule ▼

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

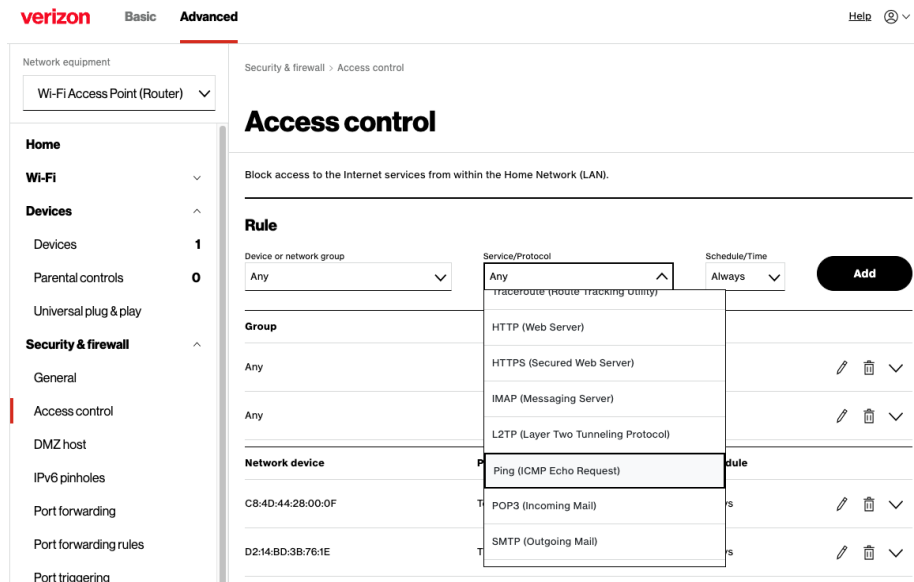
You can block individual computers on your local network from accessing specific services on the internet. For example, you could block one computer from accessing the internet, then block a second computer from transferring files using FTP as well as prohibit the computer from receiving incoming email. Access control incorporates a list of preset services, such as applications and common port settings.

Allow or restrict services

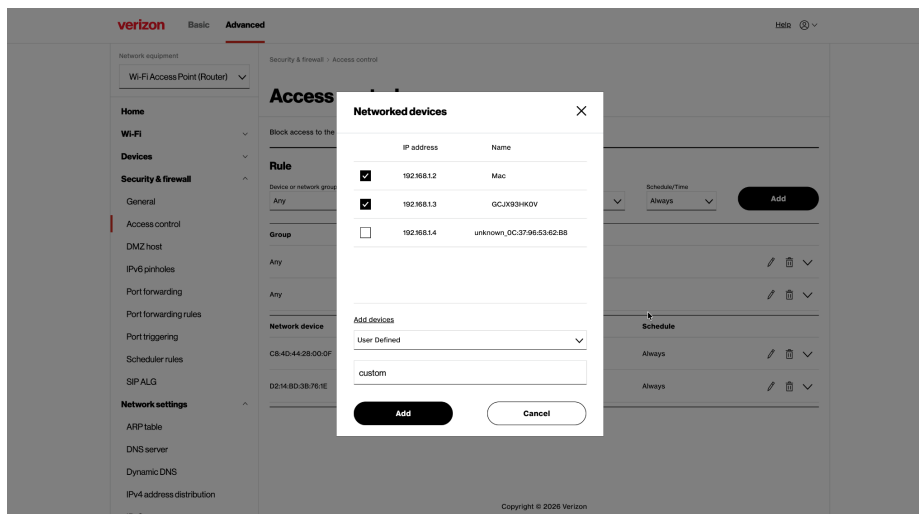
To allow or restrict services:

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.



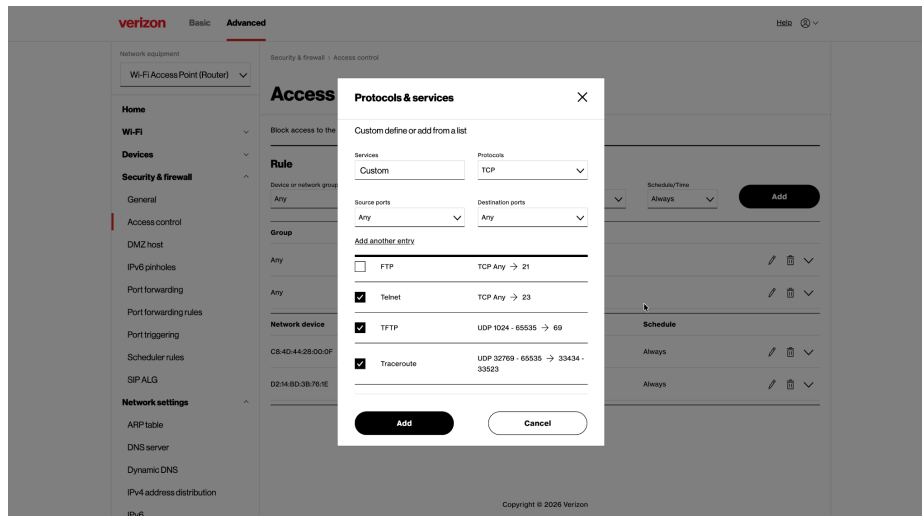


2. To apply the rule to:
 - Networked Device or Network Group - select Any.locked traffic - no access allowed, except as configured in Port Forwarding and Remote Access
 - Specific devices only - select networked device or User Defined.
3. Select the networked device to be allowed or blocked in the list.
4. In the Add devices, enter the group name, then click Add. The new network group is automatically added to the Access Control section.

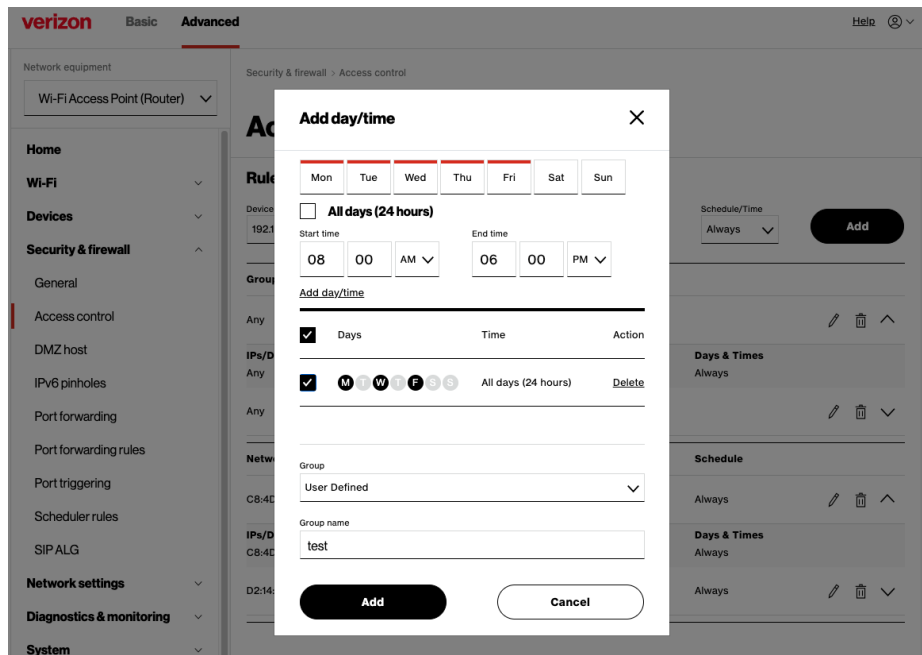


5. To block a service, select the internet protocol to be blocked in the Protocol field.
6. If the service is not included in the list, select User Defined, define the service, then click Add another entry.
7. Click Add. The service is automatically added to the Access Control section.





8. Specify when the rule is active as Always or User Defined.
9. Specify days of the week, and set the start time and end time when the rule will be active or inactive.



10. Click Add to create the schedule time.
11. Click Add to apply the changes.
12. The Access Control page displays a summary of the new access control rule.
13. To modify the current settings, click the edit icon in the action column and then the Apply button.
14. To remove an access restriction, click the trash icon. The rule 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.

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.

The screenshot shows the Verizon router's web interface. The top navigation bar includes the Verizon logo, 'Basic', and 'Advanced' tabs. The left sidebar lists various settings: Home, Wi-Fi, Devices, Security & firewall (selected), General, Access control, DMZ host, IPv6 pinholes, Port forwarding, Port forwarding rules, Port triggering, Scheduler rules, SIP ALG, Network settings, and Diagnostics & monitoring. The main content area is titled 'Security & firewall > DMZ host'. It features a 'DMZ host' section with a toggle switch set to 'Enabled'. Below this, there are two sections: 'DMZ IPv4 host' and 'DMZ IPv6 host'. The 'DMZ IPv4 host' section has a 'Local host' dropdown menu open, showing a list of IP addresses and MAC addresses. The 'Address' field is empty. The 'DMZ IPv6 host' section has a 'Local host' dropdown menu open, showing a list of IP addresses and MAC addresses. The 'Address' field is empty. The 'MAC address' field is also empty. An 'Apply changes' button is located in the top right corner.

4. Click Apply Changes to save changes.

5.0d IPv6 pinholes

The IPv6 pinhole feature of the Wi-Fi Access Point 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.



verizon Basic **Advanced** Help ⓘ

Network equipment
Wi-Fi Access Point (Router) ▾

Home
Wi-Fi ▾
Devices ▾
Security & firewall ▴
 General
 Access control
 DMZ host
IPv6 pinholes
 Port forwarding
 Port forwarding rules
 Port triggering
 Scheduler rules
 SIP ALG
Network settings ▾
Diagnostics & monitoring ▾
System ▾

Security & firewall > IPv6 pinholes

IPv6 pinholes

Apply changes

How it works
 Open a tunnel between remote computers and a device port on your Home Network (LAN). Supports gaming, IoT, home security devices and more.

Create rule

External host: Select external host ▾

Internal host: Select internal host ▾

Port:

Application/Port: Select application / ports ▴

- Custom
- FTP (File Transfer)
- Telnet (Remote Connection)
- TFTP (Trivial File Transfer Protocol)
- Traceroute (Route Tracking Utility)
- HTTP (Web Server)
- HTTPS (Secured Web Server)
- IMAP (Messaging Server)

Rules list

External host	Internal host	Protocol	Application/Port	Schedule
Any	fe80::10b3:158c:3...	UDP	1024	Always

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 media servers or security cameras, to work from the local network as well as allowing internet access to servers within the local network.

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.



verizon Basic Advanced Help

Network equipment

Wi-Fi Access Point (Router)

Security & firewall > Port forwarding

Port forwarding

Open a tunnel between remote computers and a device port on your Home Network (LAN). Supports gaming, IoT, home security devices and more.

Apply changes

Create rule

Application: Original port: Protocol:

Fwd to address: Fwd to port: Schedule:

Add to list

Rules list

Application	Original port	Protocol	Fwd to address	Fwd to port	Schedule
	4577	TCP	127.0.0.1	4577	Always
	4567	TCP	127.0.0.1	4567	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.



The screenshot shows the Verizon Advanced configuration interface. The left sidebar contains a navigation menu with categories: Home, Wi-Fi, Devices, Security & firewall (expanded), Network settings, Diagnostics & monitoring, and System. Under Security & firewall, the 'Port forwarding rules' option is highlighted. The main content area is titled 'Port forwarding rules' and shows a list of currently configured protocols. Below the list is an 'Add new' button.

Protocols	Ports	
FTP	TCP Any → 21	Edit Remove
Telnet	TCP Any → 23	Edit Remove
FTTP	UDP 1024 - 65535 → 69	Edit Remove
Traceroute	UDP 32769 - 65535 → 33434 - 33523	Edit Remove
HTTP	TCP Any → 80	Edit Remove
HTTPS	TCP Any → 443	Edit Remove
IMAP	TCP Any → 143	Edit Remove
L2TP	UDP Any → 1701	Edit Remove
Ping	ICMP Echo Request	Edit Remove
POP3	TCP Any → 110	Edit Remove
SMTP	TCP Any → 25	Edit Remove
SNMP	UDP Any → 161	Edit Remove
ServiceRule1	TCP Any → 13	Edit Remove

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

The screenshot shows the 'Protocol detail' page in the Verizon Advanced configuration interface. The left sidebar is the same as the previous screenshot, with 'Port forwarding rules' highlighted. The main content area is titled 'Protocol' and contains a 'Protocol detail' section with input fields for 'Protocol name' and 'Protocol description'. Below this is a 'Service server ports' section with a table for adding ports. At the bottom are 'Add', 'Cancel', and 'Apply' buttons.

Protocols	Ports

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.



The screenshot shows the Verizon router's configuration page. At the top, there are tabs for 'Basic' and 'Advanced', with 'Advanced' being the active tab. A 'Help' icon is visible in the top right corner. On the left side, there is a navigation menu with options: 'Home', 'Wi-Fi', 'Devices', 'Security & firewall' (which is expanded), 'General', 'Access control', 'DMZ host', 'IPv6 pinholes', 'Port forwarding', and 'Port forwarding rules'. The main content area is titled 'Protocol' and contains a section 'Edit service server ports'. This section has three dropdown menus: 'Protocol' set to 'TCP', 'Destination ports' set to 'Any', and 'Source ports' set to 'Single'. Below these, there is a text input field containing the number '21'. At the bottom of the form, there are two buttons: 'Cancel' and 'Apply'.

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 from those used for outbound traffic. The outbound traffic triggers the ports where the inbound traffic is directed.

For example, an implicit messaging controller is accessed using UDP protocol on port 2222. The controller then responds by connecting the user using UDP on port 3333, when a 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 Wi-Fi Access Point 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 Wi-Fi Access Point 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.



Network equipment: Wi-Fi Access Point (Router)

Security & firewall > Port triggering

Port triggering

Trigger opening of ports incoming data.

Create rule

Application: test

Trigger port range: Start 11, End 22

Protocol: TCP

Fwd port range: Start 33, End 44

Schedule: Always

Add to list

Rules list

Application	Trig port range	Protocol	Fwd port range	Schedule
test	11 22	TCP	33 44	Always

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 Wi-Fi Access Point is correct.
2. Select Scheduler Rules in the Security & Firewall section.

Network equipment: Wi-Fi Access Point (Router)

Security & firewall > Scheduler rules

Scheduler rules

Scheduler rules are used for limiting the activation of firewall rules to specific time periods, either for days of the week, or for hours of each day.

Rule name	Settings	Status
test	Mon and Tue between 09:00 - 00:00 on the next day	Inactive

Add

3. Click Add. The Rule Scheduler 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 or inactive at the scheduled time.
6. Click Apply Changes to save changes.

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.

verizon

Basic

Advanced

Help ⓘ

Network equipment

Wi-Fi Access Point (Router) ▼

Home

Wi-Fi ▼

Devices ▼

Security & firewall ▼

Network settings ▲

ARP table

Network settings > ARP table

ARP table

Refresh

The ARP Table displays the IPv4 and MAC address of each DHCP connection

IPv4 address	MAC address	State	Device
192.168.2.2	EA:97:DD:43:F8:C5	STALE	Network (Home/Office)
192.168.2.3	C8:4D:44:28:00:0F	STALE	Network (Home/Office)
192.168.2.4	0E:08:9F:BD:43:59	STALE	Network (Home/Office)

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

verizon

Basic

Advanced

Help ⓘ

Network equipment

Wi-Fi Access Point (Router) ▼

Home

Wi-Fi ▼

Devices ▼

Security & firewall ▼

Network settings ▲

ARP table

DNS server

Dynamic DNS

IPv4 address distribution

IPv6

IPv6 address distribution

NDP table

Network connections

Network objects

Routing

Port configuration

Network settings > DNS server

DNS server

test 11.1.1 Manually Edit Remove

Add DNS entry

☒ Enable DNS rebind protection

To disable DNS rebind protection for all devices connected to this router, unselect Enable DNS rebind protection. To disable DNS Rebind Protection for specific IP addresses, create an exception using the dropdown.

Exceptions to DNS rebind protection

IP/Netmask

127.0.0.0/8 Remove

::1/128 Remove

Add IP exception ▼

Apply Changes



2. To disable DNS rebind protection for all devices connected to the Wi-Fi Access Point, untick the check box of Enable DNS Rebind Protection.

Warning: Disabling this protection may create a risk of cyber security attack to devices connected to this Wi-Fi Access Point.

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

The screenshot shows the Verizon network settings interface. At the top, there's a 'verizon' logo and tabs for 'Basic' and 'Advanced'. Below the logo is a breadcrumb trail: 'Network Settings > DNS Server > DNS Server Create'. The main heading is 'DNS server'. On the left, there's a sidebar with a 'Wi-Fi Access Point (Router)' dropdown and a list of settings: 'Wi-Fi', 'Devices', 'Security & firewall', 'Network settings' (expanded), 'ARP table', 'DNS server' (selected), 'Dynamic DNS', 'IPv4 address distribution', and 'IPv6'. The main content area is titled 'DNS entry' and contains three fields: 'DNS entry:' with a dropdown menu showing 'IPv4', 'Host name:' with a text input field, and 'IP address:' with four individual input boxes, each containing a '0'. An 'Apply' button is at the bottom right.

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.

5.1c Dynamic DNS

Typically, when connecting to the internet, your Wi-Fi Access Point is assigned an unused public IP address from a pool, and this address changes periodically.

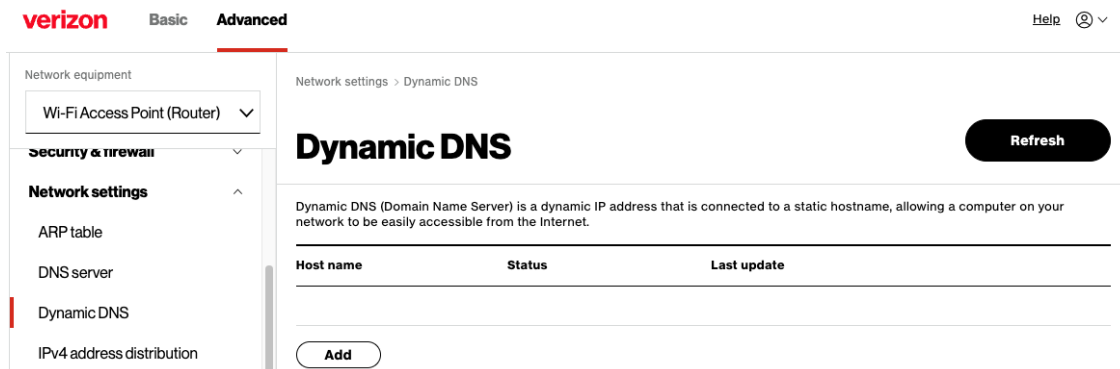
Dynamic DNS allows a static domain name to be mapped to the dynamic IP address, allowing a computer within your network to be more easily accessible from the internet.

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.

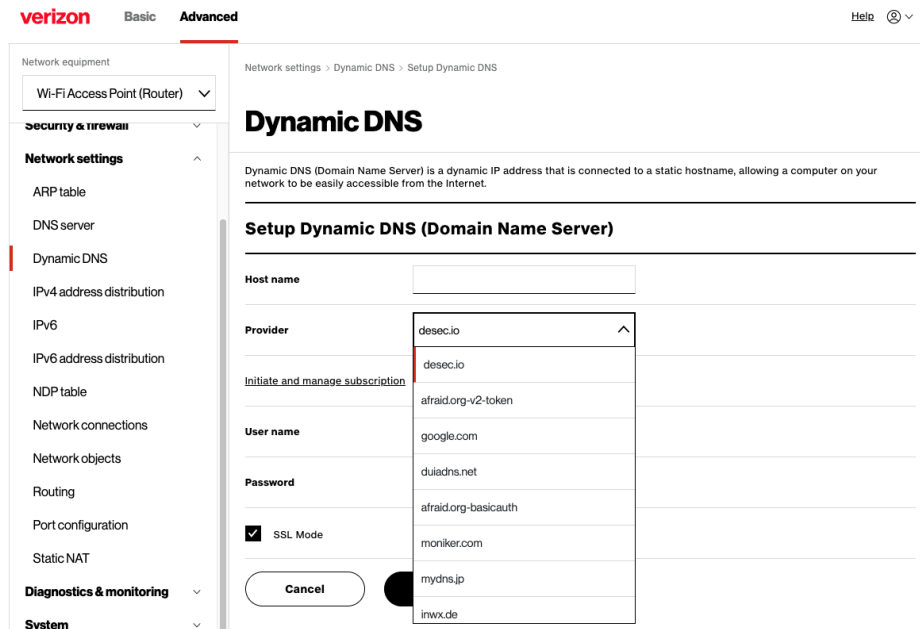
To set up dynamic DNS:

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.

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 Wi-Fi Access Point
- 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

verizon

Basic

Advanced

Help ⓘ

Network equipment

Wi-Fi Access Point (Router) ▾

Security & firewall ▾

Network settings ^

ARP table

DNS server

Dynamic DNS

IPv4 address distribution

Network settings > IPv4 address distribution

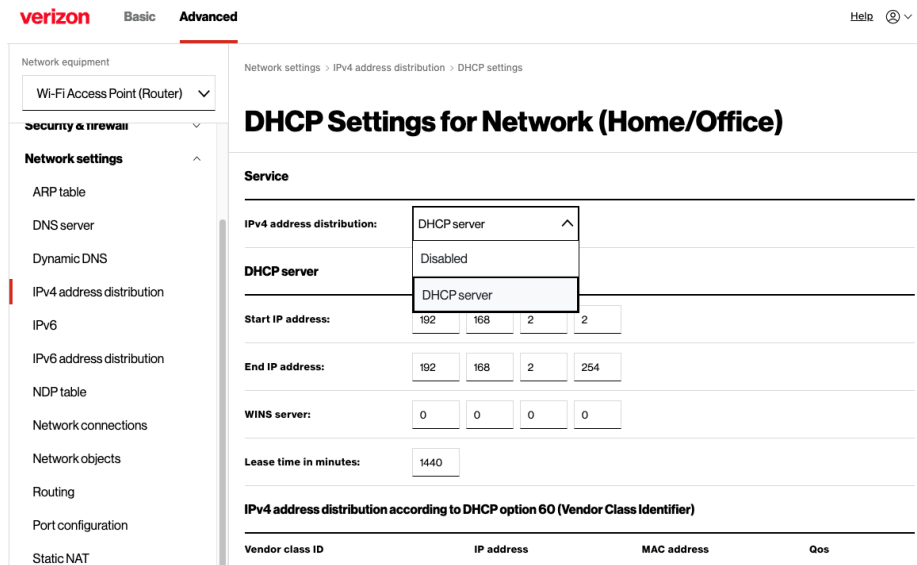
IPv4 address distribution

IPv4 Address Distribution provides the ability to allocate and configure parameters to selected hosts.

Name	Service	Subnet mask	Dynamic IP range	
Network (Home/Office)	DHCP Server	255.255.255.0	192.168.2.2 - 192.168.2.254	Edit

Connection list

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.
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.



Network equipment

Wi-Fi Access Point (Router) ▾

Security & firewall

Network settings

ARP table

DNS server

Dynamic DNS

IPv4 address distribution

IPv6

IPv6 address distribution

NDP table

Network connections

Network objects

Routing

Port configuration

Static NAT

Network settings > IPv4 address distribution > DHCP settings

DHCP Settings for Network (Home/Office)

Service

IPv4 address distribution: DHCP server ▾

Disabled

DHCP server

DHCP server

Start IP address: 192 168 2 2

End IP address: 192 168 2 254

WINS server: 0 0 0 0

Lease time in minutes: 1440

IPv4 address distribution according to DHCP option 60 (Vendor Class Identifier)

Vendor class ID	IP address	MAC address	Qos
-----------------	------------	-------------	-----

5. To configure the DHCP server, complete the following fields:

- Start IP Address – enter the first IP address that your Wi-Fi Access Point will automatically begin assigning IP addresses from. Since your Wi-Fi Access Point's default IP address is 192.168.1.1, the default start IP address should be 192.168.1.2.
- End IP Address – enter the last IP address that your Wi-Fi Access Point 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 Wi-Fi Access Point. Users can add option 60 configurations such that a 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.

To view a list of computers:

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



verizon

Basic

Advanced

Help ⓘ

Network equipment

Wi-Fi Access Point (Router) ▾

Network settings

ARP table

DNS server

Dynamic DNS

IPv4 address distribution

IPv6

IPv6 address distribution

Network settings > IPv4 Address Distribution > DHCP Connections

DHCP Connections

IPv4 Address Distribution provides the ability to allocate and configure parameters to selected hosts.

Host name	IP address	Physical address	Lease type	Connection name	Status	Expired in (min)
Mac	192.168.1.2	9A:21:FC:1C:ED:E1	Dynamic	Network (Home/Office)	Active	1193
GCJX93HK0V	192.168.1.3	98:E7:43:0A:32:AF	Dynamic	Network (Home/Office)	Active	1405

Add static connection

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

verizon

Basic

Advanced

Help ⓘ

Network equipment

Wi-Fi Access Point (Router) ▾

Security & firewall

Network settings

ARP table

DNS server

Dynamic DNS

IPv4 address distribution

IPv6

Network Settings > IPv4 Address Distribution > DHCP Connection Settings

DHCP Connections Settings

Host name:

IP address:

0000

MAC address:

000000000000

Apply

- Enter the host name.
- Enter the fixed IP address to be assigned.
- Enter the MAC address of the network interface of the computer used with this DHCP static connection.
- 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.

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



verizon Basic Advanced Help

Network equipment
Wi-Fi Access Point (Router)

Home
Wi-Fi
Devices
Security & firewall
Network settings
ARP table
DNS server
Dynamic DNS
IPv4 address distribution
IPv6
IPv6 address distribution
NDP table
Network connections
Network objects
Routing
Port configuration
Static NAT
Diagnostics & monitoring

Network settings > IPv6 configuration controls

IPv6 configuration controls

Apply changes

1. Enable IPv6 support Enabled

2. Specify the method to be used to obtain your WAN IPv6 address

IPv6 WAN configuration: DHCPv6-PD

Delegated prefix: None

Expires in: Static (Auto-Configure)

Prefix lifetime: Static (Manually-Configure)

WAN Link-local address: fe80:de4b:a1ff:fec9:ab90

☒ Obtain IPv6 DNS server address automatically

☐ Use the following IPv6 DNS server addresses

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

IPv6 LAN configuration: Stateless

LAN prefix:

2. Select Enabled in the Enable IPv6 Support field.
3. Click Apply Changes to have changes take effect.
- Note:** The Internet IPv6 service is required for this feature to work over the internet.
4. To disable the IPv6 service, move the selector to off in the Enable IPv6 Support field.
5. 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 Wi-Fi Access Point's new IPv6 address.

To view the IPv6 addresses for IPv6-supported devices on your local network, navigate to the Basic/Devices/Devices page. From there, select the **Settings** icon for the desired device to access its Device Settings page, where the IPv6 address will be displayed.

verizon Basic Advanced Help

Network equipment
Wi-Fi Access Point (Router)

Home
Wi-Fi
Devices
Parental controls
Universal plug & play
Security & firewall
Network settings
Diagnostics & monitoring
System

Devices > Devices > All

Devices

Add device

All (1) Primary (1) Guest (0) IoT (0)

Online

Name	Connection	Connected to	MAC address	Parental controls
GCJX93HK0V	Ethernet	CHR30A	98:E7:43:0A:32:AF	None

Offline

unknown_0C:37:96:53:62:B8	Offline	CHR30A	0C:37:96:53:62:B8	None
Mac	Offline	CHR30A	9A:21:FC:1C:ED:E1	None



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 Control page as shown below:

The screenshot shows the Verizon Advanced Network settings interface. On the left is a sidebar with a 'Network settings' section containing options like ARP table, DNS server, Dynamic DNS, IPv4 address distribution, IPv6 (highlighted), IPv6 address distribution, NDP table, Network connections, Network objects, Routing, Port configuration, and Static NAT. Below this are 'Diagnostics & monitoring' and 'System' sections. The main content area is titled 'IPv6 configuration controls' and includes an 'Apply changes' button. It contains three sections: 1. 'Enable IPv6 support' with a toggle switch set to 'Enabled'. 2. 'Specify the method to be used to obtain your WAN IPv6 address' with a dropdown menu for 'IPv6 WAN configuration' showing 'DHCPv6-PD', a 'Delegated prefix' dropdown showing 'None', an 'Expires in' dropdown showing 'Static (Auto-Configure)', and a 'Prefix lifetime' dropdown showing 'Static (Manually-Configure)'. Below these is a 'WAN Link-local address' field with the value 'fe80:de4b:a1ff:fec9:ab90'. 3. 'Specify the method to be used to assign LAN IPv6 addresses' with two radio button options: 'Obtain IPv6 DNS server address automatically' (selected) and 'Use the following IPv6 DNS server addresses'.

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: Wi-Fi Access Point
 - 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.

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 Control page as shown below:



verizon Basic **Advanced** Help ⓘ

Network equipment
Wi-Fi Access Point (Router) ▼

Network settings ^

- ARP table
- DNS server
- Dynamic DNS
- IPv4 address distribution
- IPv6**
- IPv6 address distribution
- NDP table
- Network connections
- Network objects
- Routing

Network settings > IPv6 configuration controls

IPv6 configuration controls

Apply changes

1. Enable IPv6 support Enabled ☒

2. Specify the method to be used to obtain your WAN IPv6 address

IPv6 WAN configuration:	DHCPv6-PD ^
Delegated prefix:	None
Expires in:	Static (Auto-Configure)
Prefix lifetime:	Static (Manually-Configure)

WAN Link-local address: fe80::de4b:a1ff:ec9:ab90

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.

IPv6 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:

verizon Basic **Advanced** Help ⓘ

Network equipment
Wi-Fi Access Point (Router) ▼

Network settings ^

- ARP table
- DNS server
- Dynamic DNS
- IPv4 address distribution
- IPv6**
- IPv6 address distribution
- NDP table
- Network connections

Network settings > IPv6 configuration controls

IPv6 configuration controls

Apply changes

☒ Obtain IPv6 DNS server address automatically

☐ Use the following IPv6 DNS server addresses

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

IPv6 LAN configuration:	Stateless ^
LAN prefix:	Stateless
Subnet ID:	00

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)
 - IPv6 LAN Address (automatically populated)
 - LAN Link Local Address (automatically populated)
 - Router Advertisement Lifetime (minute 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.



IPv6 WAN with LAN IPv6 Stateful (DHCPv6) settings

1. Specify the Stateful (DHCPv6) settings to be used to assign LAN IPv6 addresses by entering the following details:

The screenshot shows the Verizon network settings interface. On the left, a sidebar lists various settings: Network equipment (Wi-Fi Access Point (Router)), Network settings (ARP table, DNS server, Dynamic DNS, IPv4 address distribution, IPv6, IPv6 address distribution, NDP table), and IPv6. The main content area is titled 'IPv6 configuration controls' and includes a sub-header '3. Specify the method to be used to assign LAN IPv6 addresses'. Below this, there are several fields: 'IPv6 LAN configuration' (a dropdown menu with 'Stateful (DHCPv6)' selected), 'LAN prefix' (a dropdown menu with 'Stateful (DHCPv6)' selected), 'DHCPv6 Client Address Range' (a range from 1000 to 2000), and 'Subnet ID' (a field with '00'). An 'Apply changes' button is located in the top right corner.

- IPv6 LAN Configuration (select Stateful from the dropdown list)
 - LAN Prefix (automatically populated)
 - IPv6 LAN Address (automatically populated)
 - 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
2. 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.

The screenshot shows the Verizon network settings interface for IPv6 address distribution. On the left, a sidebar lists various settings: Network equipment (Wi-Fi Access Point (Router)), Network settings (ARP table, DNS server, Dynamic DNS, IPv4 address distribution, IPv6, IPv6 address distribution), and IPv6. The main content area is titled 'IPv6 address distribution' and includes a sub-header 'IPv6 address distribution provides the ability to allocate and configure parameters to selected hosts.' Below this, there is a table with columns: Name, Service, Prefix, and IP range. The table contains one row: Network (Home/Office), Stateless, --, and --. A 'Connection list' button is located at the bottom of the table.

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 make 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 Save to apply 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 Save to apply changes.

5.1g 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.

The screenshot shows the Verizon Network Settings interface. At the top, there are tabs for 'Basic' and 'Advanced', with 'Advanced' selected. Below the tabs, there's a 'Network equipment' section with a dropdown menu set to 'Wi-Fi Access Point (Router)'. A sidebar on the left lists various network settings: ARP table, DNS server, Dynamic DNS, IPv4 address distribution, IPv6, IPv6 address distribution, and NDP table (which is highlighted with a red bar). The main content area is titled 'Network settings > NDP table' and features a 'Refresh' button. Below this, a description states: 'The NDP Table displays the IPv6 and MAC address of each DHCP connection'. A table follows with the following data:

IPv6 address	MAC address	State	Rtr	Device
fe80::1415:258:4881:ca40	C8:4D:44:28:00:0F	REACHABLE	No	Network (Home/Office)
fe80::e897:ddff:fe43:f8c5	EA:97:DD:43:F8:C5	STALE	No	Network (Home/Office)

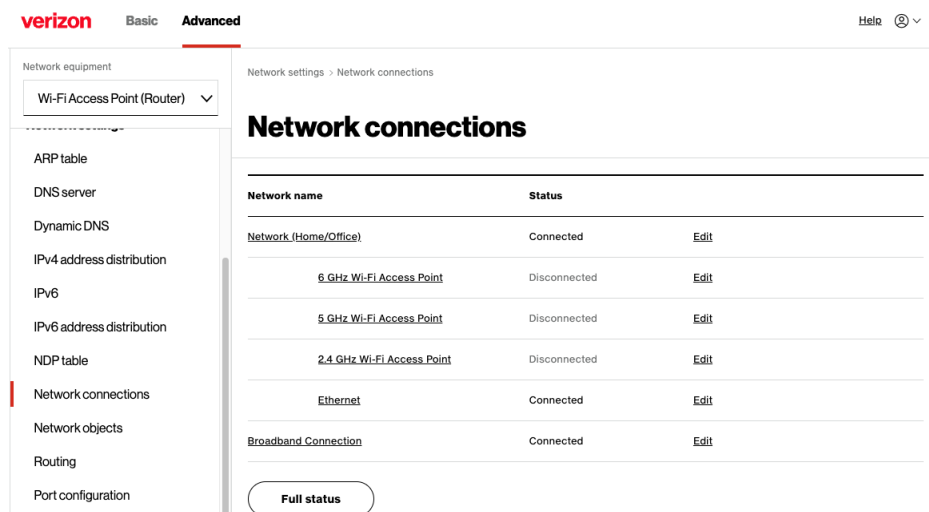
5.1h Network connections

Caution: The settings described in this chapter should only be configured by experienced network technicians. Changes could adversely affect the operation of your Wi-Fi Access Point 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.



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.

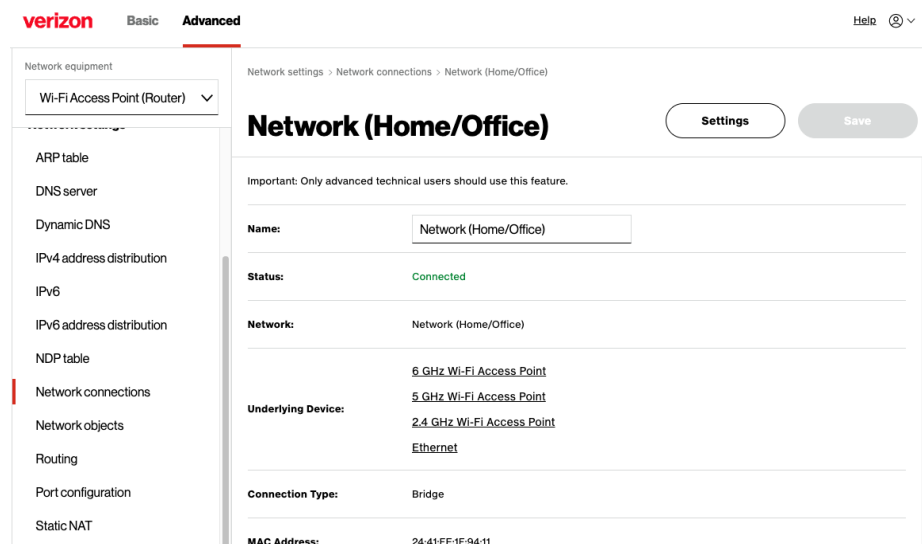
Network (Home/Office) Connection

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 Wi-Fi Access Point 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.



verizon Basic **Advanced** Help ⓘ

Network equipment
Wi-Fi Access Point (Router) ▼

Network settings > Network connections > Network (Home/Office)

Network (Home/Office)

Settings Save

IPv4 Address:	192.168.1.1
Subnet Mask:	255.255.255.0
IP Address Distribution:	DHCP Server
IPv6 LAN Prefix:	
IPv6 Address:	
Link Local Address:	fe80::2641:feff:fe1f:9411
IPv6 Address Distribution:	Stateless
Received Packets:	32540
Sent Packets:	45021
Time Span:	05:56:16

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.

verizon Basic **Advanced** Help ⓘ

Network equipment
Wi-Fi Access Point (Router) ▼

Network settings > Network connections > Network (Home/Office)

Network (Home/Office)

Save changes

Important: Only advanced technical users should use this feature.

General

Status:	Connected
Network:	Network (Home/Office)
Connection Type:	Bridge
MAC Address:	24:41:FE:1F:94:11
MTU:	Automatic ▼ 1500
IPv4 Address:	192 168 1 1
Subnet Mask:	255 255 255 0



ARP table

DNS server

Dynamic DNS

IPv4 address distribution

IPv6

IPv6 address distribution

NDP table

Network connections

Network objects

Routing

Port configuration

Static NAT

Diagnostics & monitoring

System

Routing

Port configuration

Static NAT

Diagnostics & monitoring

System

Bridge

Name	VLAN	Status	
☒ 6 GHz Wi-Fi Access Point	Disable	Disconnected	Edit
☒ 5 GHz Wi-Fi Access Point	Disable	Disconnected	Edit
☒ 2.4 GHz Wi-Fi Access Point	Disable	Disconnected	Edit
☒ Ethernet	Disable	Connected	Edit

IP Address Distribution:

DHCP Server

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 60 (Vendor Class Identifier)

Vendor Class ID	IP Address	Mac Address	Qos

Routing Table

Name	Destination	Gateway	Netmask	Metric	Status	Action
Network (Home/Office)	1.1.1.1	1.1.1.1	255.0.0.0	1	Failed	Edit Remove

Add new route

2. Configure the General section, as needed.

- 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 technicians.

3. Configure the following sections, as needed.

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 Wi-Fi Access Point 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 Wi-Fi Access Point.



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 Wi-Fi Access Point, configure the network devices as DHCP Clients.

There are two basic options in this section: Disabled and DHCP Server.

To set up the Wi-Fi Access Point'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 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 Wi-Fi Access Point will automatically begin assigning IP addresses from. Since your Wi-Fi Access Point'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 where the Wi-Fi Access Point will automatically stop allocating IP addresses. 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 Wi-Fi Access Point 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 Wi-Fi Access Point. Adding option 60 configuration allows a particular vendor to get a lease from a specified pool of addresses.

Routing Table

You can configure your Wi-Fi Access Point 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.

The screenshot shows the Verizon Wi-Fi Access Point (Router) configuration interface. The top navigation bar includes the Verizon logo, 'Basic', 'Advanced' (selected), and a 'Help' icon. The left sidebar shows 'Network equipment' with 'Wi-Fi Access Point (Router)' selected, and 'Network settings' with 'Routing' selected. The main content area is titled 'Route settings' and contains the following fields:

- Routing entry:** A dropdown menu with 'IPv4' selected.
- Name:** A text field containing 'IPv4'.
- Destination:** A text field with four input boxes, each containing '0'.
- Netmask:** A text field with four input boxes, each containing '0'.
- Gateway:** A text field with four input boxes, each containing '0'.
- Metric:** A text field containing '0'.

An 'Apply' button is located at the bottom of the form.

2. Click Apply to save your changes.



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, 5 GHz, or 6 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.

The screenshot shows the Verizon Network Settings interface. At the top, there are tabs for 'Basic' and 'Advanced', with 'Advanced' selected. Below the tabs, there's a breadcrumb trail: 'Network settings > Network connections > 6 GHz Wi-Fi Access Point'. The main heading is '6 GHz Wi-Fi Access Point'. To the right of the heading are 'Settings' and 'Save' buttons. Below the heading, there's a section 'Enable Settings.' with a green toggle switch turned on. A note below the toggle says 'Important: Only advanced technical users should use this feature.' Below this, there's a table of settings:

Name:	6 GHz Wi-Fi Access Point
Status:	Disconnected
Network:	Network (Home/Office)
Connection Type:	6 GHz Wi-Fi Access Point
MAC Address:	24-41FE1F-94:18
IP Address Distribution:	Disable
Received Packets:	0
Sent Packets:	0
Time Span:	05:55:28

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 Wi-Fi Access Point equipment.

Configuring Wi-Fi Access Point Properties

To configure the connection:

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



verizon Basic Advanced Help ⓘ

Network equipment

Wi-Fi Access Point (Router) ▾

Security & firewall ▾

Network settings ▲

ARP table

DNS server

Dynamic DNS

IPv4 address distribution

IPv6

IPv6 address distribution

NDP table

Network connections

Network objects

Routing

Port configuration

Static NAT

Network settings > Network connections > 6 GHz Wi-Fi Access Point

6 GHz Wi-Fi Access Point

Save changes

Important: Only advanced technical users should use this feature.

General

Status: Disconnected

Network: Network (Home/Office)

Connection Type: 6 GHz Wi-Fi Access Point

MAC Address: 24:41:FE:1F:94:18

MTU: Automatic ▾ 1500

Automatic

Automatic By DHCP

Manual

2. Verify the following General information:

- 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.

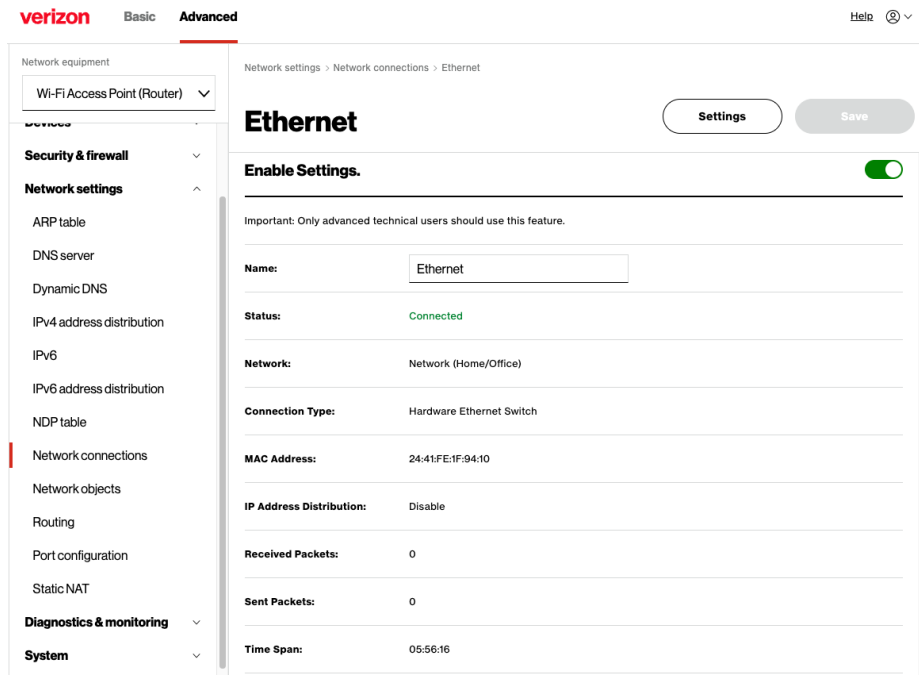
Ethernet Connection

You can view the properties of your Ethernet LAN connection using an Ethernet cable inserted into one of your Wi-Fi Access Point'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.





verizon Basic **Advanced** Help ⓘ

Network equipment
Wi-Fi Access Point (Router) ▼

Security & firewall ▼
Network settings ▲
ARP table
DNS server
Dynamic DNS
IPv4 address distribution
IPv6
IPv6 address distribution
NDP table
Network connections
Network objects
Routing
Port configuration
Static NAT
Diagnostics & monitoring ▼
System ▼

Network settings > Network connections > Ethernet

Ethernet

Settings Save

Enable Settings. ☒

Important: Only advanced technical users should use this feature.

Name: Ethernet

Status: **Connected**

Network: Network (Home/Office)

Connection Type: Hardware Ethernet Switch

MAC Address: 24:41:FE:1F:94:10

IP Address Distribution: Disable

Received Packets: 0

Sent Packets: 0

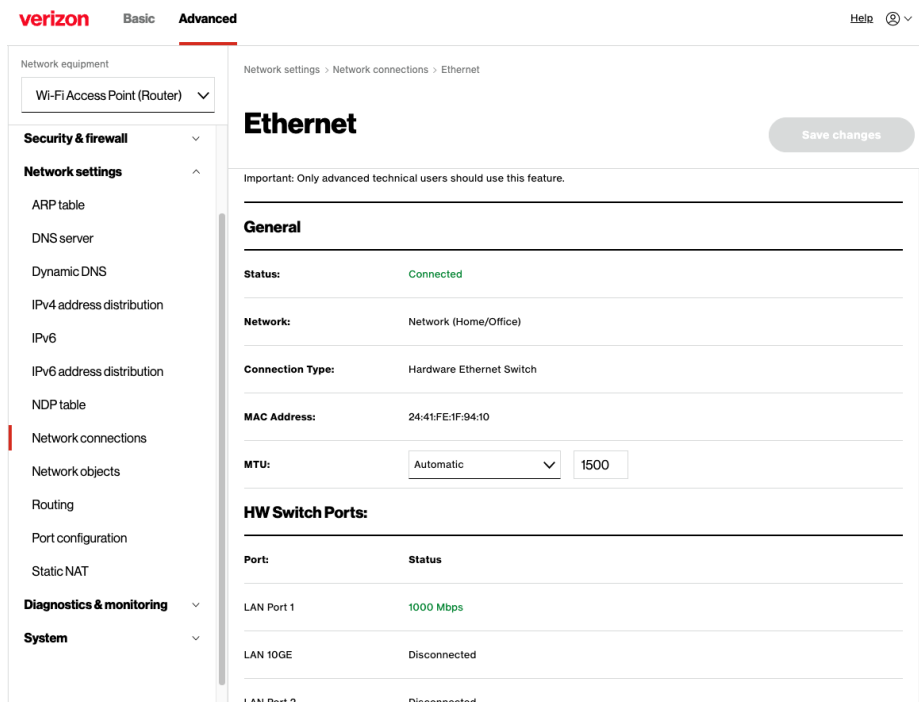
Time Span: 05:56:16

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.



verizon Basic **Advanced** Help ⓘ

Network equipment
Wi-Fi Access Point (Router) ▼

Security & firewall ▼
Network settings ▲
ARP table
DNS server
Dynamic DNS
IPv4 address distribution
IPv6
IPv6 address distribution
NDP table
Network connections
Network objects
Routing
Port configuration
Static NAT
Diagnostics & monitoring ▼
System ▼

Network settings > Network connections > Ethernet

Ethernet

Save changes

Important: Only advanced technical users should use this feature.

General

Status: **Connected**

Network: Network (Home/Office)

Connection Type: Hardware Ethernet Switch

MAC Address: 24:41:FE:1F:94:10

MTU: Automatic ▼ 1500

HW Switch Ports:

Port	Status
LAN Port 1	1000 Mbps
LAN 10GE	Disconnected
LAN Port 2	Disconnected

2. Verify the following information:
 - Status - displays the connection status of the network.
 - Network - displays the type 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.

Coax

The screenshot shows the Verizon network settings interface. On the left is a sidebar with a menu including: Network equipment, Wi-Fi Access Point (Router), Home, Wi-Fi, Devices, Security & firewall, Network settings (highlighted), ARP table, DNS server, Dynamic DNS, IPv4 address distribution, IPv6, IPv6 address distribution, NDP table, Network connections (highlighted with a red bar), Network objects, Routing, Port configuration, Static NAT, Diagnostics & monitoring, and System. The main content area is titled 'Coax' and has tabs for 'Settings' and 'Save'. Under 'Enable Settings', there is a green toggle switch. Below this is a note: 'Important: Only advanced technical users should use this feature.' The configuration fields are as follows:

Name:	Coax
Status:	Cable Disconnected
Network:	Network (Home/Office)
Connection Type:	Hardware MoCA
MAC Address:	DC:4B:A1C9:82:70
IP Address Distribution:	Disable
Received Packets:	0
Sent Packets:	0
Time Span:	00:00:00

To view the connection settings:

1. In the Network Connections page, click the Coax link.
2. From the connection's Enable Settings page, to enable or disable the connection, move the selector to on or off.
3. To rename the network connection, enter the new name in the Name field.
4. Click Save to apply changes.

Configuring Coax Properties

To configure the connection:

1. In the Coax page, click Settings. The configuration page displays.



2. Configure the following General settings, as needed.

- 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: sets the MTU (Maximum Transmission Unit at 1500).

3. Configure the following Coax Link settings, as needed.

- Privacy - to set Privacy, select the Enabled check box. This causes all devices connected to the coaxial cable to use the same password. This is recommended. To set the password, enter the Coax Link password in the Manual entry of privacy password field.
- To enable or disable the Coax link, click Enable or Disable.
- To view the devices connected using the coaxial cable, click the Go to LAN Coax Status link.

4. Click Apply to save changes.

Broadband Connection (Ethernet)

You can view the properties of your broadband connection (your connection to the internet). This connection may be via Ethernet cable.

To view the connection settings:

1. In the Network Connections page, click the Broadband Connection (Ethernet) link.



verizon

Basic

Advanced

Help ⓘ

Network equipment

Wi-Fi Access Point (Router) ▼

Security & firewall

Network settings

ARP table

DNS server

Dynamic DNS

IPv4 address distribution

IPv6

IPv6 address distribution

NDP table

Network connections

Network objects

Routing

Port configuration

Static NAT

Diagnostics & monitoring

Network settings > Network connections > Broadband Connection

Broadband Connection

Settings

Save

Enable Settings.

Important: Only advanced technical users should use this feature.

Name:

Broadband Connection

Status:

Connected

Network:

Broadband Connection

Connection Type:

Ethernet

MAC Address:

24:41:FE:1F:94:10

IPv4 WAN Address:

10.76.216.149

Subnet Mask:

255.255.255.0

Default Gateway:

10.76.216.1

IPv4 DNS Address 1:

208.52.253.24

IPv4 DNS Address 2:

208.52.253.88

IP Address Distribution:

DHCP

IPv6 WAN Address:

2001:d0:226:57:1

IPv6 Link Local Address:

fe80::2641:feff:fe1f:9410

IPv6 Default Gateway:

fe80::2ef8:9bff:fe90:2abf

IPv6 DNS Address 1:

IPv6 DNS Address 2:

Received Packets:

196632

Sent Packets:

18274

Time Span:

05:56:16

Configuring Broadband Connection

To configure the connection:

1. In the Broadband Connection (Ethernet) Properties page, click Settings. The configuration page displays.



verizon Basic **Advanced** Help

Network equipment
Wi-Fi Access Point (Router)

Security & firewall
Network settings
ARP table
DNS server
Dynamic DNS
IPv4 address distribution
IPv6
IPv6 address distribution
NDP table
Network connections

Network settings > Network connections > Broadband Connection

Broadband Connection

Save changes

General

Status: Connected

Network: Broadband Connection

Connection Type: Ethernet

MAC Address: 24:41:FE:1F:94:10

MTU: Automatic 1500

WAN IP Address

Internet Protocol: Obtain IPv4 Address Automatically

☐ **Override Subnet Mask:** 0 0 0 0

DHCP Lease: Release Renew

Expires In: 259 minutes

IPv4 DNS: Obtain IPv4 DNS Address Automatically

Internet Connection Firewall: ☒ Enable

This feature provides the ability to change the default firewall setting on this interface. We highly recommend that you do not change the default setting.

2. Configure the following General settings, as needed.

- 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: 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.

5.1i Network objects

Network objects define a group, such as a group of computers, on your Wi-Fi Access Point 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.

You can simultaneously apply website filtering to multiple computers by defining them as a single network object. Website filtering can then be simultaneously applied to all the computers.

To define a network object:

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



Network equipment

Wi-Fi Access Point (Router)

Security & firewall

Network settings

ARP table

DNS server

Dynamic DNS

IPv4 address distribution

IPv6

IPv6 address distribution

NDP table

Network connections

Network objects

Routing

Port configuration

Network settings > Network objects

Network objects

A Network Object is a set of host name, IP addresses, or MAC addresses. Security rules can be applied to a distinct LAN subnet using Network Objects

Create an Object

Object name: Global Object

Object type: Select

Add

Object list

Object name	Object type	Status	Actions
Global Object	IP Address	Active	Edit Remove

3. To define a network object, enter a name for the network object in the Objects Name field.
4. Select and configure the type of network object as IP Address, IP Subnet, IP Range, MAC Address, Host Name, or DHCP Option, and click Add.
5. The network object displays in the Objects List section.
6. Repeat the above steps to create additional network objects.
7. When complete, click Apply Changes to save changes.

5.1j 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.

Network equipment

Wi-Fi Access Point (Router)

Network settings

ARP table

DNS server

Dynamic DNS

IPv4 address distribution

IPv6

IPv6 address distribution

NDP table

Network connections

Network objects

Routing

Port configuration

Network settings > Port configuration

Port configuration

Apply changes

Port	Service	Status
WAN Port	Auto	Disconnected
LAN 10GE	Auto	Disconnected
LAN Port 1	Auto	Disconnected
LAN Port 2	Full-Duplex 2,500 Mbps	Connected

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.



5.1k 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.

Network equipment: Wi-Fi Access Point (Router)

Network settings > Routing

Routing

This page provides the ability to add, edit or delete routing rules.

Routing table

Name	Destination	Gateway	Netmask	Metric	Status	Action
Network (Home/Office)	1.1.1.1	1.1.1.1	255.0.0.0	1	Failed	Edit Remove

[New route](#)

Internet Group Management Protocol (IGMP)

- ☒ Enable Ethernet
- ☒ Enable MoCA - Coax
- ☒ Enable 2.4 GHz Wi-Fi
- ☒ Enable 5 GHz Wi-Fi
- ☒ Enable 6 GHz Wi-Fi

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

Network equipment: Wi-Fi Access Point (Router)

Network settings > Routing > Route settings

Route settings

Routing entry: IPv4

Name: IPv4

Destination: 0 0 0 0

Netmask: 0 0 0 0

Gateway: 0 0 0 0

Metric: 0

[Apply](#)

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 Wi-Fi Access Point.
 - 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/MLD (Multicast Listener Discovery)-based forwarding is managed by IGMP, which handles a single upstream interface and multiple downstream interfaces. This functionality allows the system to send IGMP host messages on behalf of hosts that are discovered via standard IGMP interfaces. Furthermore, IGMP snooping enables an Ethernet switch to monitor the IGMP communication between hosts and routers, while the IGMP querier sends 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.

5.1 Static NAT

Static NAT allows devices located behind a firewall that is configured with private IP addresses to appear to have public IP addresses to the internet. This allows an internal host, such as a web server, to have an unregistered (private) IP address and still be accessible over the internet.

To configure static NAT:

1. From the Advanced menu, select Network Settings and then click Static NAT.

verizon Basic Advanced Help ⓘ

Network equipment

Wi-Fi Access Point (Router) ▼

ARP table

DNS server

Dynamic DNS

IPv4 address distribution

IPv6

IPv6 address distribution

NDP table

Network connections

Network objects

Routing

Port configuration

Static NAT

Network settings > Static NAT

Static NAT

Apply changes

Trigger opening of ports for incoming data.

Create rule

Device: Select ▼

Public IP address: 0 0 0 0

☐ Enable port forward

☐ Add another entry Add

Rules list

ID	Network Device	Public IP address	Port forward
1	192.168.1.2	1.1.1.1	

2. To create a static NAT, select a source address in the Local Host field.
3. Enter the Public IP Address.
4. If using port forwarding, select the Enable port forward check box.
5. Click Add. The rule displays in the Rules List section.
6. Click Apply changes to save changes.
7. Repeat these steps to add additional static IP addresses.



5.2 Diagnostics & monitoring

5.2a Bandwidth monitoring

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

To view the bandwidth:

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

The screenshot shows the Verizon Advanced settings interface. At the top, there are tabs for 'Basic' and 'Advanced', with 'Advanced' selected. Below the tabs is a 'Network equipment' dropdown menu set to 'Wi-Fi Access Point (Router)'. On the left, a sidebar lists various settings: Home, Wi-Fi, Devices, Security & firewall, Network settings, and Diagnostics & monitoring. The 'Diagnostics & monitoring' section is expanded, showing 'Bandwidth monitoring' as the selected option. The main content area is titled 'Bandwidth monitoring' and includes an 'Auto-refresh' toggle (which is turned on) and a 'Refresh' button. Below this, there are tabs for 'WAN' and 'LAN', with 'WAN' selected. A table displays bandwidth usage for the selected network. The table has columns for 'Usage', '1hr', '12hr', '24hr', '1Week', and '1Month'. The 'Usage' column lists 'Upload' and 'Download' usage, all of which are currently at '0 bytes'.

Usage	1hr	12hr	24hr	1Week	1Month
Upload	0 bytes	0 bytes	0 bytes	0 bytes	0 bytes
Download	0 bytes	0 bytes	0 bytes	0 bytes	0 bytes

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.



verizon Basic **Advanced** Help ⓘ

Network equipment
Wi-Fi Access Point (Router) ▼

Home

Wi-Fi ▼

Devices ▼

Security & firewall ▼

Network settings ▼

Diagnostics & monitoring ▲

Bandwidth monitoring

Diagnostics

Speed test

System logging

System-wide connections

Backhaul logging

System ▼

Diagnostics & Monitoring > Diagnostics

Diagnostics

How it works

Diagnostics can assist in testing network connectivity. This feature pings (ICMP echo) an IP address and displays the results, such as the number of packets transmitted and received, round trip time and success status.

IPv4 Ping (ICMP Echo)

Destination

Number of pings

Status

IPv6 Ping (ICMP Echo)

Destination

Number of pings

Status

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.

5.2c System logging

System logging provides a view of the most recent activity of your Wi-Fi Access Point. In addition, you can view additional logs, such as the security, firewall, WAN link and LAN DHCP.

To view the system log:

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

verizon Basic **Advanced** Help ⓘ

Network equipment
Wi-Fi Access Point (Router) ▼

Home

Wi-Fi ▼

Devices ▼

Security & firewall ▼

Network settings ▼

Diagnostics & monitoring ▲

Bandwidth monitoring

Diagnostics

Speed test

System logging

Diagnostics & monitoring > System logging > System log

System logging

System log Security log Advanced log Firewall log WAN DHCP log LAN DHCP log Wi-Fi log Migration log

Time	Event type	Log level	Details
Clear			

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



verizon

Basic

Advanced

Help ⓘ

Network equipment

Wi-Fi Access Point (Router) ▼

Home

Wi-Fi

Devices

Security & firewall

Network settings

Diagnostics & monitoring

Bandwidth monitoring

Diagnostics

Speed test

System logging

System-wide connections

Backhaul logging

System

Diagnostics & monitoring > System logging > System log

System log

Security log

Advanced log

Firewall log

WAN DHCP log

LAN DHCP log

Wi-Fi log

Migration log

System logging

Logging view options

Past day

Past week

Custom range

Start Date

Start Time

03/06/25

2:00 pm ▼

End Date

End Time

03/06/25

2:00 pm ▼

Cancel

Save

3. Select your preferred logging time.
4. Click Apply to save changes.
5. To view a specific type of log event such as Security Log, WAN 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 Wi-Fi Access Point.

To view your Wi-Fi Access Point's full system status and traffic monitoring data:

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

verizon

Basic

Advanced

Help ⓘ

Network equipment

Wi-Fi Access Point (Router) ▼

Home

Wi-Fi

Devices

Security & firewall

Network settings

Diagnostics & monitoring

Bandwidth monitoring

Diagnostics

Speed test

System logging

System-wide connections

Diagnostics & Monitoring > System-wide Connections

System-wide Connections

Auto-refresh 

Name	Network (Home/Office)	Broadband Connection	6 GHz Wi-Fi Access Point	5 GHz Wi-Fi Access
Status	Connected	Connected	Disconnected	Disconnected
Underlying Device	Network (Home/Office)	Broadband Connection	Network (Home/Office)	Network (Home/Office)
Connection Type	6 GHz Wi-Fi Access Point 5 GHz Wi-Fi Access Point 2.4 GHz Wi-Fi Access Point Ethernet	Ethernet	6 GHz Wi-Fi Access Point	5 GHz Wi-Fi Access I
MAC Address	24:41:FE:1F:94:11	24:41:FE:1F:94:10	24:41:FE:1F:94:18	26:41:FE:1F:96:16
IPv4 Address	192.168.1.1	10.76.216.149	--	--



Subnet Mask	255.255.255.0	255.255.255.0	--	--
IPv4 Default Gateway	192.168.1.1	10.76.216.1	--	--
IPv4 DNS Address 1	192.168.1.1	208.52.253.24	--	--
IPv4 DNS Address 2	--	208.52.253.88	--	--
IPv4 Address Distrtn.	DHCP Server	DHCP	Disable	Disable
IPv6 Prefix	--	--	--	--
IPv6 Address	--	2001:df0:226:57:1	--	--
IPv6 Link-Local Address	fe80::2641:feff:fe1f:9411	fe80::2641:feff:fe1f:9410	--	--
IPv6 Default Gateway	--	fe80::2ef8:9bff:fe90:2abf	--	--
IPv6 DNS Address 1	--	--	--	--
IPv6 DNS Address 2	--	--	--	--
IPv6 Address Distrtn.	Stateless	DHCP	Disable	Disable
Rec'd Packets	32540	196632	0	0
Sent Packets	45021	18274	0	0
Rec'd Bytes	30220545	23550368	0	0
Sent'd Bytes	49944067	1894198	0	0
Rec'd Errors	0	0	0	0
Rec'd Drops	0	0	0	0
Time Span	05:56:16	05:56:16	05:55:28	05:55:25

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.



Network equipment

Wi-Fi Access Point (Router) ▼

Home

Wi-Fi ▼

Devices ▼

Security & firewall ▼

Network settings ▼

Diagnostics & monitoring > Backhaul logging

Backhaul logging

Fios Extender **Wi-Fi Access Point (Extender)**

Time	Date	Backhaul type	Connection rate	MAC address	Location
07:29 am	02 / 19 / 24	Ethernet	1000 Mbps	A8:A2:37:6B:EA:88	

RefreshClearSave

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 Wi-Fi Access Point'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 Wi-Fi Access Point's local network (LAN) and internet connection (WAN), firmware and hardware version numbers, MAC Address, IP settings of Wi-Fi Access Point and extender(s) (if connected).

verizon Basic Advanced

Help ⓘ

Network equipment

Wi-Fi Access Point (Router) ▼

Home

Wi-Fi ▼

Devices ▼

Security & firewall ▼

Network settings ▼

Diagnostics & monitoring ▼

System ▲

System status

Date & time

Factory reset

LED brightness

Open source software

Quick setup wizard

Reboot internet equipment

System > System status

System status

Auto-refresh ☒ Refresh

Broadband IPv4

Status
Connected

IPv4 address is from:
DHCP

IPv4 address
10.76.216.149

Subnet mask
255.255.255.0

IPv4 default gateway
10.76.216.1

IPv4 DNS address 1
208.52.253.24

IPv4 DNS address 2
208.52.253.88

NATs supported (used / max)
47/30000

Broadband IPv6

Status
Connected

IPv6 address is from:
DHCPv6-PD

Delegated prefix

IPv6 address
2001:df0:226:57:1

Link-local address
fe80::2641:feff:fe1f:9410

IPv6 default gateway
fe80::2ef8:9bff:fe90:2abf

IPv6 DNS address 1

IPv6 DNS address 2

Router	
Firmware version	4.1.6.26d
Hardware version	0.0.3
Wi-Fi chipset version	WLAN.WBE.1.3.1-00130-QCAHKSWPL_SILICONZ.1.85203.1.88734.1
Model name	CHR30A-R
Serial number	ACY44200101
LAN IPv4 address	192.168.1.1
Broadband MAC address	24:41:FE:1F:94:10
Broadband physical connection	Ethernet
Router has been active for	0 day(s) 6 hours 4 minutes 24 seconds
LED status	Normal Operation

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.

verizon Basic Advanced Help ⓘ

Network equipment
Wi-Fi Access Point (Router) ▼

Home
Wi-Fi ▼
Devices ▼
Security & firewall ▼
Network settings ▼
Diagnostics & monitoring ▼
System ▲
System status
Date & time
Factory reset
LED brightness
Open source software
Quick setup wizard
Reboot internet equipment

System > Date & time

Date & time

Refresh

Use the Refresh button to Refresh the status

Localization

Local time: Mar 06, 2025 02:56:58pm Edit

Time zone: Eastern Time (Default) ▼

Automatic time update

Enable ☒

Protocol: Network Time Protocol (NTP)

Time server

Apply

cpe-ntp1.verizon.com
cpe-ntp2.verizon.com
cpe-ntp3.verizon.com

Last updated: Mar 06, 2025 02:56:58pm

3. Select the local time zone. Your Wi-Fi Access Point automatically detects daylight saving times for the selected time zone.
4. In the Automatic Time Update section, select the Enable check box to perform an automatic time update.
5. Enter the IP address or domain name of the Time Server, then click Apply to save changes.
6. 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 Wi-Fi Access Point.

Only configuration files saved on a specific Wi-Fi Access Point can be applied to that Wi-Fi Access Point. You cannot transfer configuration files between routers.

Warning: Manually editing a configuration file can cause your Wi-Fi Access Point to malfunction or become completely inoperable.

Restore Options

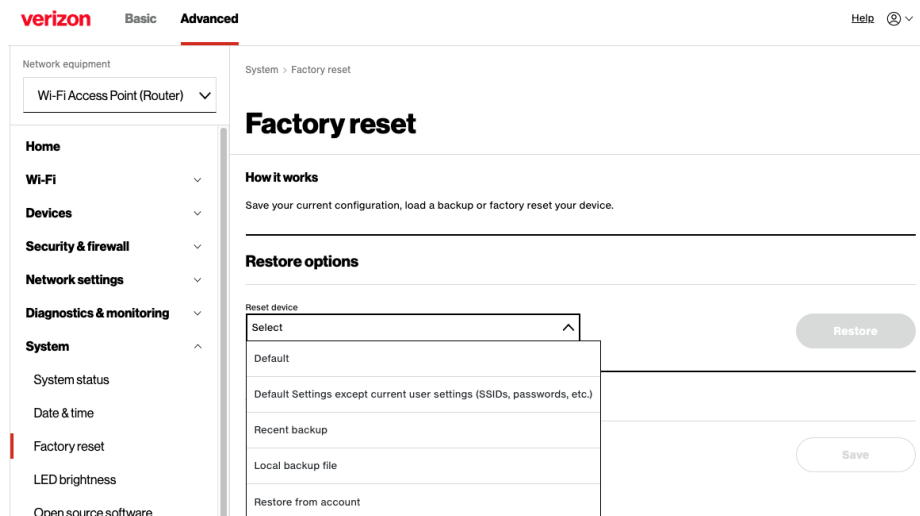
You can restore your configuration settings to your router factory default settings. Restoring the default settings erases the current configuration, including user defined settings and network connections. All connected DHCP clients must request new IP addresses. Your Wi-Fi Access Point must restart.

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 Wi-Fi Access Point are restored to their default values. This includes the administrator password. A user-specified password will no longer be valid.

To restore your Wi-Fi Access Point's factory default settings:

1. Click Factory Reset in the System section.
2. Select Default Settings or Default Settings except current user settings.
 - 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 the Restore button. The factory default settings are applied and your Wi-Fi Access Point 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 Recent backup or Load a backup file then click choose file.



3. Browse to the location of the file, and click the Restore button to begin the configuration uploading process.
4. Accessing the Verizon Home app, My Verizon app, or the My Verizon account also allows you to restore the previously saved settings. Select Restore from Verizon Home app, My Verizon app, or My Verizon account to restore the saved settings to the Wi-Fi Access Point.
5. Click the Restore button. Your Wi-Fi Access Point will automatically restart with that configuration.

Save Options

To save the configuration file:

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

The screenshot shows the Verizon configuration interface for a Wi-Fi Access Point (Router). The top navigation bar includes the Verizon logo, 'Basic' and 'Advanced' tabs, and a 'Help' link. The left sidebar lists various settings categories: Home, Wi-Fi, Devices, Security & firewall, Network settings, Diagnostics & monitoring, System, System status, Date & time, Factory reset (highlighted), LED brightness, Open source software, and Quick setup wizard. The main content area is titled 'System > Factory reset' and 'Factory reset'. It includes a 'How it works' section, a 'Restore options' section with a 'Reset device' dropdown menu and a 'Restore' button, and a 'Save options' section with a 'Saved configurations' dropdown menu and a 'Save' button. The 'Saved configurations' dropdown is open, showing options: 'Router and Verizon account' and 'Backup file'.

3. Select Router and Verizon account or Backup file to save the current configuration, then click Save button.
4. If you select Backup file, the configuration file is saved to your web browser's download folder.
5. Click the Save button to begin the configuration backup process.

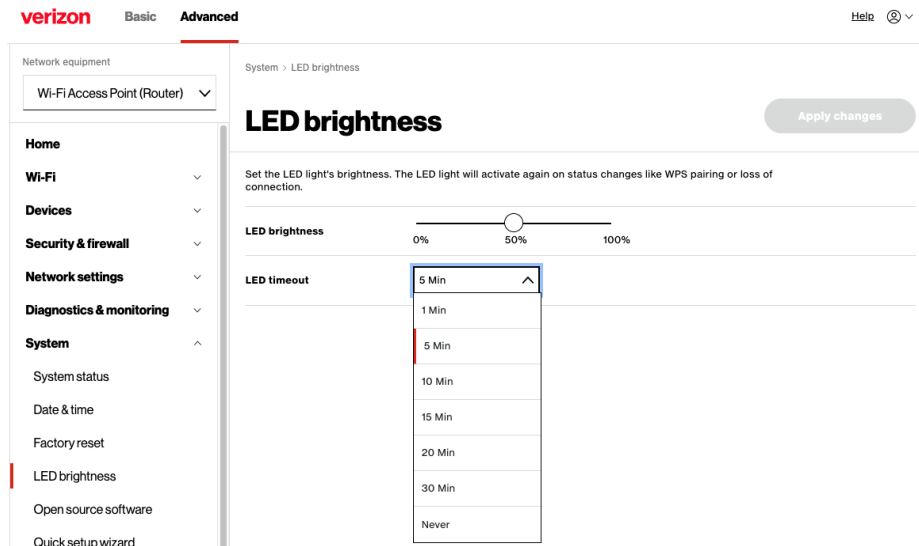
5.3d LED brightness

The Wi-Fi Access Point 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.

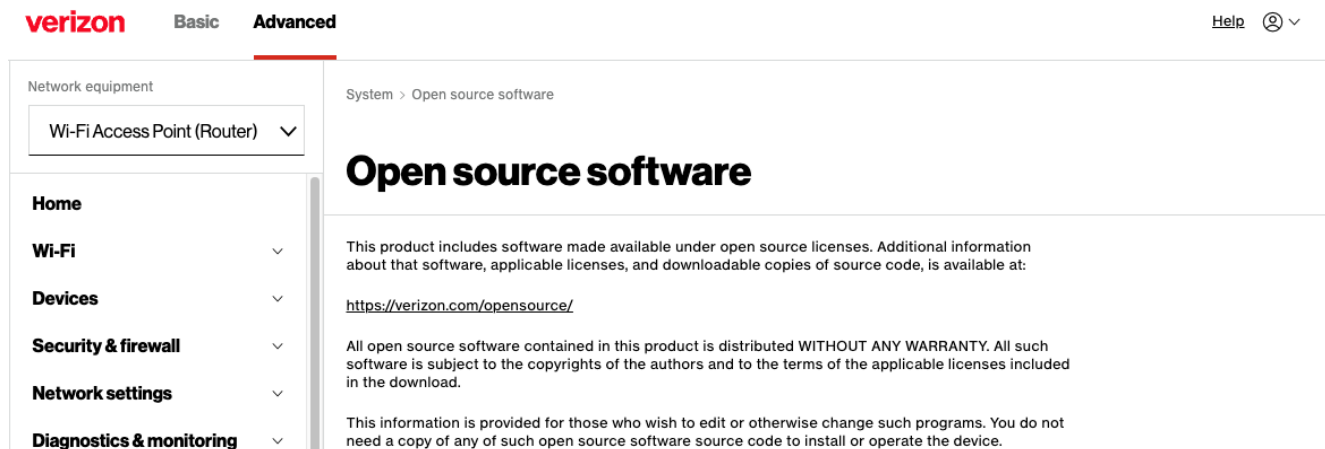




2. Slide the bar to adjust the brightness of the LED.
3. Select your preferred timeout period (in minutes) from the dropdown list for the LED dimming setting.
The Status LED will automatically turn off after the timeout period.
4. Click Apply Changes to save changes.

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

5.3e Open source software



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

5.3f Reboot internet equipment

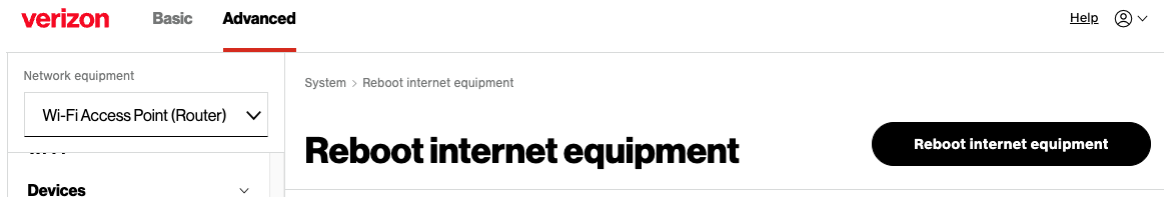
Warning: Only select Reboot internet equipment if instructed to do so by Verizon support.

You can reboot your Wi-Fi Access Point using the Reboot internet equipment feature. Refer to 1.3b Rear Panel for factory reset function.

To reboot your Wi-Fi Access Point using the user interface:



1. Select Reboot internet equipment in the System section.



2. To reboot, click Reboot Device. Your Wi-Fi Access Point will reboot. This may take a minute or more.
3. To access your Wi-Fi Access Point's 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 Wi-Fi Access Point's network at risk from outside attacks.

You can access and control your Wi-Fi Access Point not only from within the local network, but also from the internet using Remote Administration.

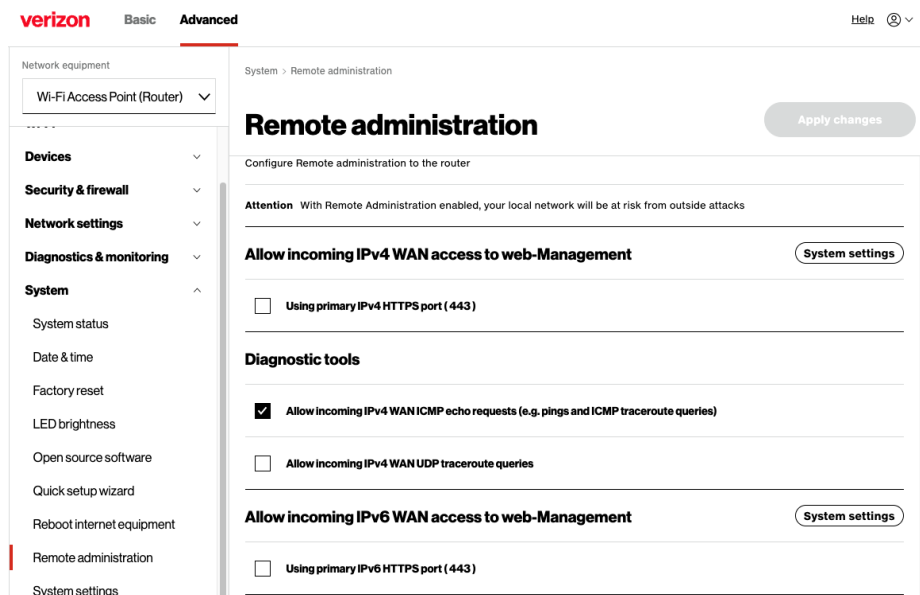
You can allow incoming access to the following:

- Allow Incoming WAN Access to Web-Management - used to obtain access to your Wi-Fi Access Point'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 support.

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 the 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 System settings interface. The left sidebar has a 'System' section expanded, with 'System settings' highlighted. The main content area is titled 'System settings' and includes an 'Apply changes' button. The settings are organized into several sections:

- Router's status:**
 - Router's hostname: CHR30A
 - Local domain: mynetworksettings.com
 - Location: Other (dropdown)
- User settings:**
 - User name: Admin
 - Set new password: (input field) minimum 8 characters
 - Retype new password: (input field)
 - Unsuccessful login attempts: 10 (dropdown) maximum attempts
- Router:**
 - ☐ Automatic refresh of system monitoring web pages
 - ☒ Prompt for password when accessing via LAN
 - ☒ Warn user before configuration changes
 - Session lifetime: 600 seconds
 - Number of concurrent sessions that can be logged into the Router: 10 (dropdown)
- Remote administration:**
 - Primary HTTPS management port: 443
 - System logging: ☐ Disabled
 - Remote system notify level: None (dropdown)
 - Remote security notify level: None (dropdown)

2. In the Router Status section, configure the following:
 - Router's Hostname - enter the host name of your Wi-Fi Access Point.
 - Local Domain - view the local domain of the network.
 - Location - select your current location of the Router from the dropdown list.



3. In the User Settings section, you can view the administration user that can currently access your network. In addition, you can modify the login password and manage the number of unsuccessful login attempts the administration user can enter before your Wi-Fi Access Point 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 Wi-Fi Access Point 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 Wi-Fi Access Point has been active.
 - In the Number of concurrent sessions that can be logged into the router field, select the number of users that can access your Wi-Fi Access Point at the same time.
5. In the Remote Administration section, configure the following:
 - Enter the Primary HTTP Management Port.
Refer to section 5.3g Remote Administration for this feature.
 - In the System Logging section move the selector to on to activate system logging.
 - 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 network security logging.
 - In the DHCP Timeout section, specify the DHCP timeout.
6. Click Apply Changes to save the changes.

06 Troubleshooting

This chapter lists solutions for issues that may be encountered while using your Wi-Fi Access Point as well as frequently asked questions.

Although the majority of the Wi-Fi Access Point'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.

Note: The advanced settings should only be configured by experienced network technicians to avoid adversely affecting the operation of your Wi-Fi Access Point 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 Wi-Fi Access Point is powered on and is connected to the internet. Check the Status LED on the front of the Wi-Fi Access Point. Be sure to refer to section 1.3a "Front panel" to determine the status of the Wi-Fi Access Point.
- If the prior tips do not resolve your connection issue, try power cycling the Wi-Fi Access Point by unplugging the power cord from the power supply and wait 2 minutes. During the 2 minute wait period,



also power cycle the network device (e.g. the computer, tablet, etc.) and then plug the power cable back into the Wi-Fi Access Point. After 3 - 5 minutes, recheck the Status LED and try again to access the internet.

- If rebooting your Wi-Fi Access Point does not resolve your connection issue, try resetting the Wi-Fi Access Point back to its factory default state. Press the reset button on the rear panel of the Wi-Fi Access Point for 3+ seconds (the Status LED should go off) to begin resetting your Wi-Fi Access Point. The Wi-Fi Access Point will return to service in 3-5 minutes depending on your network connection. Try to access the internet once the Status LED is solid white.

6.0b If you are unable to connect to your Wi-Fi Access Point using Wi-Fi

- Be sure your Wi-Fi device is within range of your Wi-Fi Access Point; move it closer to see if your connection improves.
- Check your 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 Wi-Fi Access Point.
- Be sure you are connecting to the correct Wi-Fi network; check to be sure you are using your Wi-Fi Access Point's SSID. In some cases, if using a Wi-Fi password, you may need to enter the Wi-Fi password into your device again to be sure your device accepts the password.
- Check to be sure you are running the latest software for your device.
- Try turning your device's Wi-Fi off and on, and try to connect.
- If you have made any changes in your network settings and turning your device's Wi-Fi off and on does not help, try to restart your 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 connect to your Wi-Fi Access Point, you may need to try connecting to the Wi-Fi with another device. If the issue goes away with a different device, then the issue is likely with the prior device's individual network configuration.

6.0c Accessing your Wi-Fi Access Point if you are locked out

- If your Wi-Fi Access Point connection is lost while making configuration changes, a setting that locks access to your Wi-Fi Access Point's UI may have inadvertently been activated.
- Common ways to lock access to your Wi-Fi Access Point are:
 - Scheduler - If a schedule has been created that applies to the computer over the connection being used, your Wi-Fi Access Point 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 Wi-Fi Access Point is denied.
- To regain access, restore the default settings to your Wi-Fi Access Point

6.0d Restoring your Wi-Fi Access Point's default settings

- There are two ways to restore your Wi-Fi Access Point's default settings. It is important to note that after performing either procedure, all previously saved settings on your Wi-Fi Access Point will be lost.
- Using the tip of a paperclip or similar object, press and hold the Reset button on the rear of your Wi-Fi Access Point for over three seconds.
- Access the UI and navigate to the Advanced page. Select Factory reset under System. Save your existing configuration if desired. Select one of the restore options and click the Restore radio button.
- For additional information regarding the Restore Defaults feature, refer to section 5.3c Factory Reset/Restore Options.



Note: If you reset or reboot your Wi-Fi Access Point, you may also need to disconnect your Wi-Fi Access Point's power supply for a few minutes (3 or more) and then reconnect the power cable.

6.0e LAN connection failure

- Verify your Wi-Fi Access Point is properly installed, LAN connections are correct, and that the Wi-Fi Access Point and communicating network devices are all powered on.
- Confirm that the computer and Wi-Fi Access Point 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 Wi-Fi Access Point.
- 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
 - Wi-Fi Access Point is on and connected properly
 - Wi-Fi Access Point 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 the Wi-Fi Access Point and restart the Wi-Fi Access Point, wait 1-2 minutes 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).

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
Installation mode (5G Home customer)	Passing signal	Solid white
	LTE coverage only / No signal	Solid red
Regular usage	Setup complete	50% bright white
	No Signal	Solid red
	Wi-Fi disabled by user	Solid green



Pairing	WPS pairing	Hard blink blue
Other	Factory reset Firmware error	Fast blink yellow Soft blink red

6.0h Rear lighted indicators

Ethernet port mode	Status LED	Left LED	Right LED
Wired LAN connection	Ethernet >= 100M* Link	Off	Solid white
	Ethernet >= 100M* Activity	Off	Blinking white
Threshold level can be decided based on port capability	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 Wi-Fi Access Point. How do I connect more computers or devices?

- Plugging in an Ethernet hub or switch expands the number of ports to connect more devices.
 - Run a straight-through Ethernet cable from the Uplink port of the hub to the Wi-Fi Access Point.
 - Use a crossover cable if there is no Uplink port/switch on your hub, to connect to the Wi-Fi Access Point.
- Remove an existing device from the Ethernet port on your Wi-Fi Access Point and use that port.

6.1b How do I change my Wi-Fi Access Point's password through the UI?

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

6.1c Is the Wi-Fi option on by default on my Wi-Fi Access Point?

- Yes, your Wi-Fi Access Point'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 rear of your Wi-Fi Access Point.

6.1e Are my Wi-Fi Access Point's Ethernet ports auto-sensing?

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

6.1f Can I connect an older Wi-Fi device to my Wi-Fi Access Point?

- Yes, your Wi-Fi Access Point can interface with 802.11b, g, n, ac, ax, or be devices. Your Wi-Fi Access Point also can be set up 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 Wi-Fi Access Point 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.

6.1h How do I locate the IP address that my computer is using?

- In Windows 8, Windows 10, or Windows 11 click the Windows button and select Settings, then click Network & Internet and Status. Click the Properties button 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 Wi-Fi Access Point UI:
 - From the Basic menu, select Devices from the left pane.
 - 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 OS X, unplug the Ethernet cable or Wi-Fi card, then plug it back in.

6.1j I cannot access my Wi-Fi Access Point UI. What should I do?

- If you cannot access the UI, verify the computer connected to your Wi-Fi Access Point 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 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.
- 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.

6.1l How many computers can be connected through my Wi-Fi Access Point?

- Your Wi-Fi Access Point 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

The specifications for your Wi-Fi Access Point are as follows.

This includes standards, cabling types and environmental parameters.



7.0 General specifications

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

Model number	CHR30A
Standards	IEEE 802.3x, 802.3u, 802.3ab, 802.3bz, 802.3an IEEE 802.11a/b/g/n/ac/ax/be
IP	IP versions 4 and 6
Speed (wired)	10GE WAN Ethernet: 100 Mbps, 1/2.5/5/10 Gbps auto-sensing 10GE LAN Ethernet: 100 Mbps, 1/2.5/5/10 Gbps auto-sensing 2.5GE LAN Ethernet: 10/100 Mbps, 1/2.5 Gbps auto sensing
Speed (wireless)	2.4 GHz - IEEE 802.11b/g/n: maximum up to 600 Mbps IEEE 802.11ax: maximum up to 1.1 Gbps 5 GHz - IEEE 802.11a/n/ac: maximum up to 2.2 Gbps IEEE 802.11ax: maximum up to 2.4 Gbps 6 GHz - IEEE 802.11ax: maximum up to 4.8 Gbps MLO enabled - IEEE 802.11be: maximum up to 46 Gbps
Cabling type	Ethernet 100BaseT: UTP/STP Category 5 Ethernet 1000BaseT: UTP/STP Category 5e Ethernet 2.5/5/10GBaseT: UTP/STP Category 6a
Firewall	ICSA



7.1 LED indicators

Front panel	Status LED
Rear panel	WAN Ethernet and LAN Ethernet [3]

7.2 Environmental parameters

Wi-Fi Access Point (unit only)	Size: 5.1" wide x 5.1" deep x 8.6" height Weight: 3.20 lbs / 1.45 kg
Complete system (including packaging)	Size: 5.9" wide x 11.2" deep x 7.1" height Weight: 4.85 lbs / 2.20 kg
Power	External 12V, 5A
Mounting bracket (wired)	Size: 3.97" wide x 6.6" deep x 6.86" height Weight: 0.39 lbs / 175 g
Screws (optional)	PH TP+N: 0.157" x 0.984" PE Anchor: 0.236" x 0.984"
Certifications	FCC, UL 62368, WFA
Operating temperature	41°F to 104°F (5°C to 40°C)
Storage temperature	23°F to 122°F (-5°C to 50°C)
Operating humidity	5% to 85%
Storage humidity	5% to 93% (non-condensing)

08 Notices

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



8.0 Regulatory compliance notices

8.0a Class B equipment

FCC interference statement

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 or more 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.

The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet.

Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

Radio frequency exposure statement

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 31cm 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.

8.0c Alerte de sécurité

7. Le circuit de distribution par câble considéré est le circuit TNV-1.
8. 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).
9. 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 CHR30A

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 metalically 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 metalically to OSP wiring.

Caution: The Wi-Fi Access Point must be installed inside the home or office. 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/>

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

