verizon

Fios Router
USER GUIDE

Model G3100

CONTENTS

05 / USING NETWORK CONNECTIONS

06 / SETTING PARENTAL CONTROLS

07 / CONFIGURING SECURITY SETTINGS

08 / CONFIGURING ADVANCED SETTINGS

 |

CONTENTS

01/

INTRODUCTION

Verizon Fios Router lets you transmit and distribute digital entertainment and information to multiple devices in your office.

Your Fios Router supports networking using coaxial cables, Ethernet, or Wi-Fi, making it one of the most versatile and powerful routers available.

 |

PACKAGE CONTENTS, SYSTEM REQUIREMENTS AND FEATURES

1.0/ PACKAGE CONTENTS

Your package contains:

- Fios Router
- Power adapter
- Ethernet cable, three meters (white)
- OSS (Open Source Software) insert guide

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 Fios Router features include:

- Support for multiple networking standards, including
  - WAN – Gigabit Ethernet and MoCA 1.1 interfaces
  - LAN – 802.11 a/b/g/n/ac/ax, Gigabit Ethernet and MoCA 2.5 interfaces
- Integrated wired networking with 4-port Ethernet switch and Coax (MoCA)
  - Ethernet supports speeds up to 1000 Mbps

  - MoCA 2.5 LAN enabled to support speeds up to 2500 Mbps over coaxial cable
  - MoCA 1.1 WAN enabled to support speeds up to 100 Mbps over coaxial cable
- One USB 3.0 port
- IoT - Bluetooth and Wi-Fi
- Integrated Wi-Fi networking with 802.11a/b/g/n/ac/ax access point featuring:
  - backward compatible to 802.11a/b/g/n/ac
  - 2.4 GHz 11ax 4x4
  - two 5 GHz 11ax 4x4
- 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
  - Network Protection

 |

FEATURES

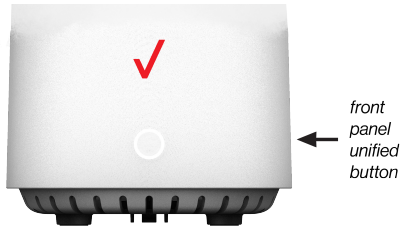
  - Static NAT
  - Port forwarding
  - Port triggering
  - Access control
  - Advanced Wi-Fi protection featuring WPA2 & WPA3 Modes and MAC address filtering
  - Wi-Fi Multimedia (WMM) for Wi-Fi QoS (quality-of-service)
- Compatible with Wi-Fi Mesh system
- Dual-stack network configuration of IPv4 and 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 layer 2/3) 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 My Fios app
- Static routing
- VPN (VPN pass through only)
- IGMP
- Daylight savings time support

1.3/ GETTING TO KNOW YOUR FIOS ROUTER

1.3a/ FRONT PANEL

The front panel's unified button allows quick access to the Wi-Fi Protected Setup (WPS) feature and pairing mode.

The Router Status LED will be solid white when your Fios Router is turned on, connected to the internet, and functioning normally.



Router Status LED

Condition Status	LED Color	Fios Router
Normal	WHITE	Normal operation (solid) Router is booting (fast blink)
	BLUE	Pairing mode (slow blink) Pairing successful (solid)
	GREEN	Wi-Fi has been turned off (solid)
Issue(s)	YELLOW	No internet connection (solid)
	RED	Hardware/System failure detected (solid) Overheating (fast blink) Pairing Failure (slow blink)
Power	OFF	Power off

The WPS button is used to initiate Wi-Fi Protected Setup. This is an easy way to add WPS capable devices to your Wi-Fi network. To activate the WPS function, press and hold the unified button located on the front of your Fios Router for more than two seconds. When WPS is initiated from your router, the Router Status LED slowly flashes blue for up to two minutes, allowing time to complete the

 |

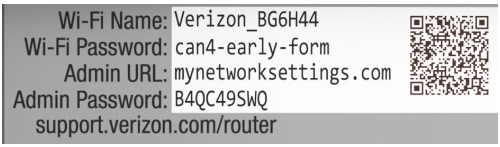
WPS pairing process on your Wi-Fi device (also known as a Wi-Fi client). When a device begins connecting to your router using WPS, the Router Status LED rapidly flashes blue for a few seconds, and turns solid blue and then solid white as the connection completes.

If there is an error during the WPS pairing process, the Router Status LED slowly flashes red for two minutes after the error occurs.

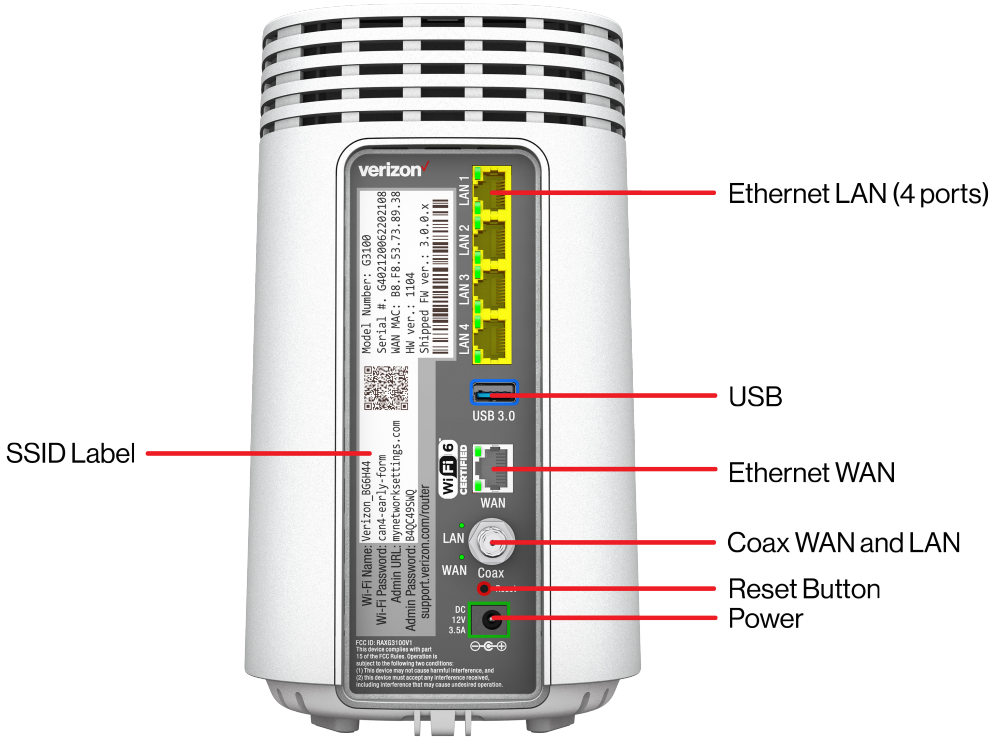
Refer to the “Connecting A Wi-Fi Device Using WPS” for more details. In addition, the unified button also provides a quick view of the operational state of the Fios Router using various colors as indicated in the chart above. Please refer to section 9.0h for details on the rear LEDs.

1.3b/ REAR PANEL

The rear panel of your router has a label that contains important information about your device, including the default settings for the Fios Router’s Wi-Fi name (SSID), Wi-Fi password (WPA2 key), local URL for accessing the router’s administrative pages, and administrator password. The label also contains a QR code that you can scan with your smartphone, tablet, or other 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).



The rear panel has seven ports; F-type coax, Ethernet LAN (four), Ethernet WAN, and USB. The rear panel also includes a DC power jack and a reset button.



 |

GETTING TO KNOW YOUR FIOS ROUTER

- **Ethernet LAN** - connects devices to your Fios Router using Ethernet cables to join the local area network (LAN). The four Ethernet LAN ports are 10/100/1000 Mbps auto-sensing and can be used with either straight-through or crossover Ethernet cables.
- **USB** - provides up to 1000 mA at 5 VDC for attached devices. For example, you could charge a cell phone.
- **Ethernet WAN** - connects your Fios Router to the internet using an Ethernet cable.
- **Coax WAN and LAN** - connects your router to the internet and/or to other MoCA devices using a coaxial cable.

  Warning: The WAN coax port is intended for connection to Verizon Fios only. It must not be connected to any exterior or interior coaxial wires not designated for Verizon Fios.
- **Reset Button** - allows you to reset your router to the factory default settings. To perform a soft reboot, press and hold the button for at least three seconds. To reset your router to the factory default settings, press and hold the button for at least ten seconds.
- **Power** - connects your Fios Router to an electrical wall outlet using the supplied power adapter.

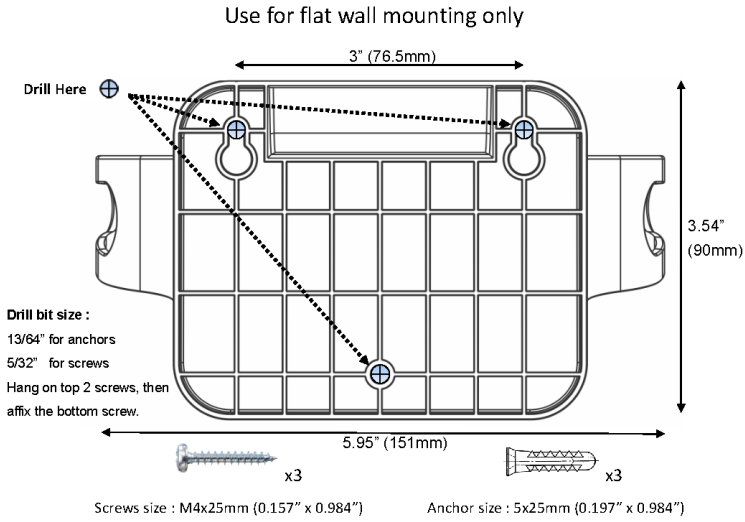
  Warning: The included power adapter is for office use only, supporting voltages from 105-125 voltage in AC. Do not use in environments with greater than 125 voltage in AC.

1.3c/ MOUNTING THE FIOS ROUTER TO A WALL

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

To mount your Fios Router to a wall:

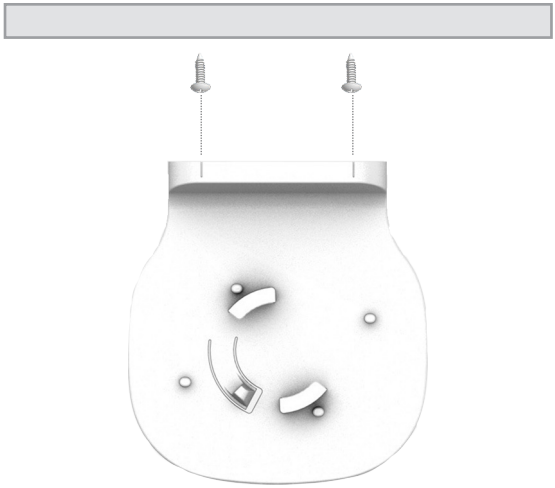
1. You may use the wall-mount template sheet for positioning the Fios Router.
2. Mark the mounting holes using the template sheet as shown below.



 |

GETTING TO KNOW YOUR FIOS ROUTER

3. Drive two screws into the wall. Leave the screws extended about 0.2 inches from the wall.
4. Verify the screws are positioned correctly by placing the wall bracket on the screws. Then remove the wall bracket from the wall.



5. There are two mounting slots located on the bottom of the Fios Router. It allows you to securely attach your router to the wall. Align the slots with the wall mount bracket.

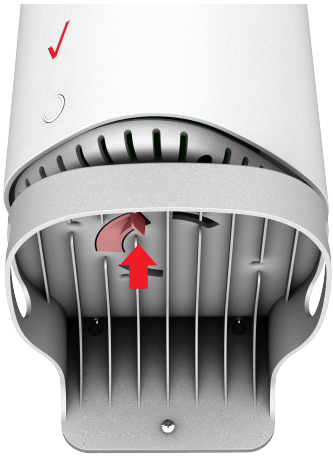
6. Attach the router to the wall mount bracket through an easy twist and lock action.

7. Align the wall mount bracket with the attached router to the screws, then slide the bracket down until it locks in place.

 |

8. To secure the bracket, place one screw into the small hole of the bracket and tighten the screw into your wall.

Note: To release the lock, twist the router counter-clockwise and press down on the small clip on the bottom of the bracket.



02 /

CONNECTING YOUR FIOS ROUTER

Connecting your Fios Router and accessing its web-based User Interface (UI) are both simple procedures.

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

 |

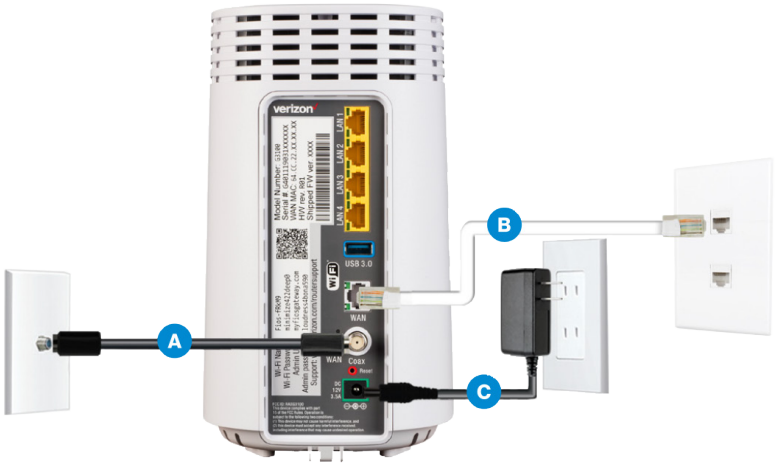
SETTING UP YOUR FIOS ROUTER

2.0/ SETTING UP YOUR FIOS ROUTER

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

2.0a/ INSTALLATION INSTRUCTIONS

1. CONNECT YOUR CABLES
   - A. Connect the coax cable from the coax port on your router to a coax outlet. (Required for Fios TV)
   - B. Connect the Ethernet cable from your router's WAN port to an Ethernet outlet. (Required for internet speeds greater than 100 Mbps)
   - C. Connect the router power cord to an electrical outlet.



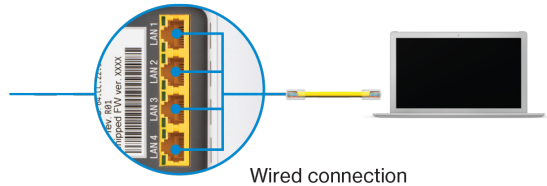
D. Router will take up to 10 minutes to power up completely. Move on when the front light is solid white.

2. CONNECT YOUR DEVICES

Wired or Wi-Fi? Your choice.

Wired

A. Connect the Ethernet cable to any yellow LAN port on your router.



Wired connection

B. Connect the other end to your computer.

Wi-Fi

A. Get the Wi-Fi name and password off the label on your router.

Router label

B. On your device, choose your Wi-Fi name when it appears.

C. Enter the Wi-Fi password exactly as it is on your router label.

 |

SETTING UP YOUR FIOS ROUTER

Wi-Fi Network

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

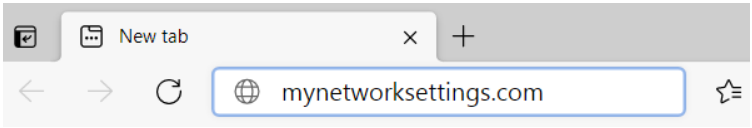
3. **COMPLETE ACTIVATION**

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

2.0b/ CONFIGURE YOUR FIOS ROUTER

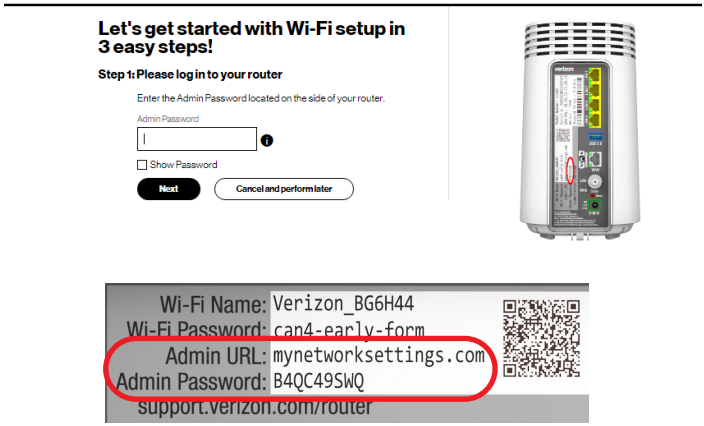
1. Open a web browser on the device connected to your Fios Router network.
2. In the browser address field (URL), enter: mynetworksettings.com, then press the **Enter** key on your keyboard.

   Alternately, you can enter: https://192.168.1.1

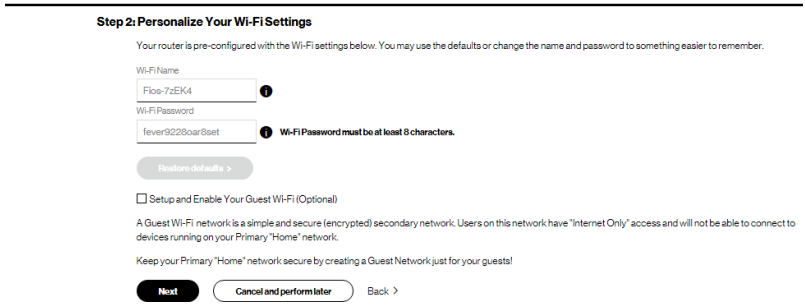


The first time you access your Fios Router, an Easy Setup Wizard displays to help step you through the setup process.

3. On the **Step 1: Please log in to your router** screen, enter the password that is printed next to the Admin password on the label on the rear of your router.



4. Click **Next**. The **Step 2: Personalize Your Wi-Fi Settings** screen displays. Click on the check box next to **Setup and Enable Your Guest Wi-Fi (Optional)** to personalize your Guest Wi-Fi Name and Password.



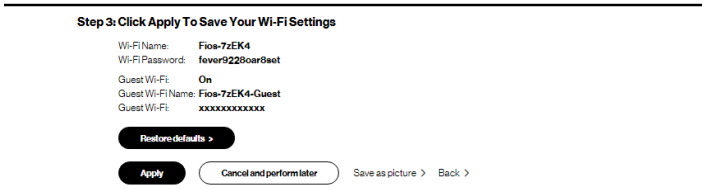
 |

SETTING UP YOUR FIOS ROUTER

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

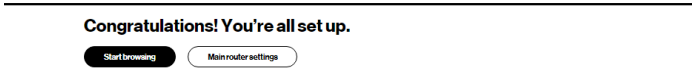
5. Click **Next**. The **Step 3: Click Apply to Save Your Wi-Fi Settings** screen appears. You have an option of saving the Wi-Fi settings as an image on your device by clicking the **Save as picture** button. After you click **Save as picture** to save your Wi-Fi settings as an image, click **Apply** to save the Wi-Fi changes to your Fios Router.

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



The **Congratulations! You're all set up.** screen displays once

your Fios Router verifies the final settings and has successfully connected to the internet and is ready for use. You can click on Main router settings to access the main screen of the Fios Router or click on Start browsing and you will be directed to the Verizon.com website.



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

If your Fios Router fails to connect, follow the troubleshooting steps in the Troubleshooting section of this guide.

2.1/ EXPANDING WI-FI COVERAGE

Connecting Verizon's Fios Extender to the Fios Router allows you to extend Wi-Fi signal range of the Fios Router for eliminating Wi-Fi dead zones on your Wi-Fi network.

 |

EXPANDING WI-FI COVERAGE

2.1a/ WI-FI INSTALLATION

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

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

2.1b/ WIRED INSTALLATION

1. Place the Fios Extender and Fios Router near a coax outlet – ideally in an area with spotty Wi-Fi coverage.
2. Connect the coax cable from the extender to a coax outlet. (If the coax outlet is already in use, you can use the coax splitter included in the shipping box.)
3. Connect the power cord from the extender to an electrical outlet.
4. The light on the extender should turn solid white within a few minutes, indicating the connection is complete.

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

2.2/ COMPUTER NETWORK CONFIGURATION

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

 |

COMPUTER NETWORK CONFIGURATION

2.2a/ CONFIGURING DYNAMIC IP ADDRESSING

To configure a computer to use dynamic IP addressing:

WINDOWS 7/8

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

WINDOWS 10

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

 |

COMPUTER NETWORK CONFIGURATION

MACINTOSH OS X

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

2.2b/ CONNECTING OTHER COMPUTERS AND NETWORK DEVICES

You can connect your Fios Router to other computers or set top boxes using an Ethernet cable, Wi-Fi connection (Wi-Fi), or coaxial cable.

ETHERNET

1. Plug one end of an Ethernet cable into one of the open yellow Ethernet ports on the back of your Fios Router.
2. Plug the other end of the Ethernet cable into an Ethernet port on the computer.

3. Repeat these steps for each computer to be connected to your Fios Router using Ethernet. You can connect up to four.

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 Fios Router creates a secure Wi-Fi network connection.

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

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

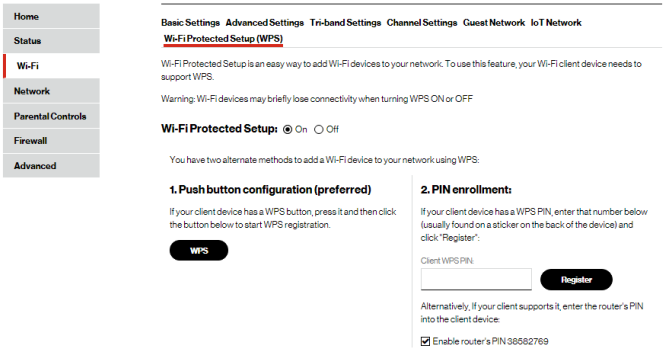
You can easily add Wi-Fi devices to your Wi-Fi network using the WPS option if your Wi-Fi device supports the WPS feature.

To access WPS using the user interface:

1. From the main menu, select **Wi-Fi** settings, then select **Wi-Fi Protected Setup (WPS)**.

 |

COMPUTER NETWORK CONFIGURATION



2. Enable the protected setup by moving the selector to **On**.
3. Use one of the following methods:
   - If your Wi-Fi client device has a WPS button, press the unified button on your Router for more than two seconds, then click the WPS button on your Wi-Fi device (client) 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 **Client WPS PIN** field. The **Client WPS PIN** field is located in the section **2 - PIN enrollment** on the user interface.
   - Click **Register**.
   - Alternatively, you can enter the Router's PIN shown on this screen into the WPS user interface of your device, if this PIN mode is supported by your Wi-Fi device.

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

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

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

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

CONNECTING A WI-FI DEVICE USING A PASSWORD

1. Verify each device that you are connecting with Wi-Fi has built-in Wi-Fi or an external Wi-Fi adapter.
2. Open the device's Wi-Fi settings application.
3. Select your Fios Router's Wi-Fi network name (SSID) from the device's list of discovered Wi-Fi networks.

 |

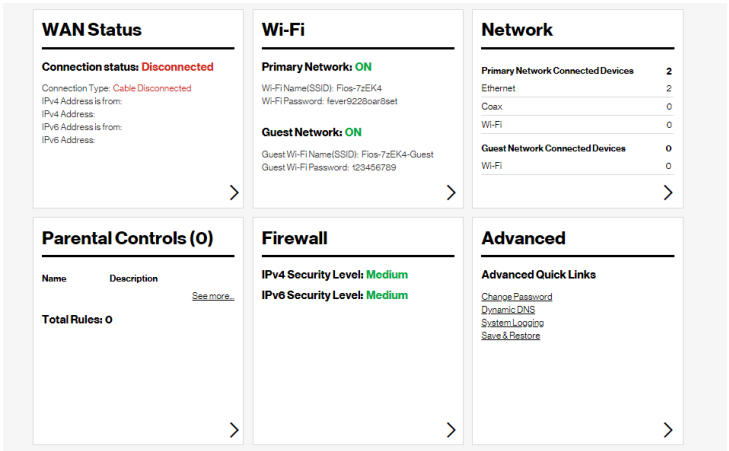
4. When prompted, enter your Fios Router's Wi-Fi password (WPA2 or WPA3 key) into the device's Wi-Fi settings. Your Router's default Wi-Fi network name and password are located on the sticker on the rear panel of your Fios Router.
5. Verify the changes were implemented by using the device's web browser to access a site on the internet.
6. Repeat these steps for every device that you are connecting with Wi-Fi to your router.

COAX

1. Verify all coax devices are turned off.
2. Disconnect any adapter currently connected to the coaxial wall jack in the room where your router is located.
3. Connect one end of the coaxial cable to the coaxial wall jack and the other end to the coax port on your network device.
4. Power up the network device.

2.3/ MAIN SCREEN

When you log into your router, the dashboard main page displays the main navigation menu of connection status, Wi-Fi settings, network settings, parental control, firewall security level, and advanced quick links.



2.3a/ Menu

The main menu contains the following configuration options and chapters:

- Status - this chapter
- Wi-Fi - Chapter 3
- Network - Chapter 4 and Chapter 5
- Parental Controls - Chapter 6
- Firewall - Chapter 7
- Advanced - Chapter 8

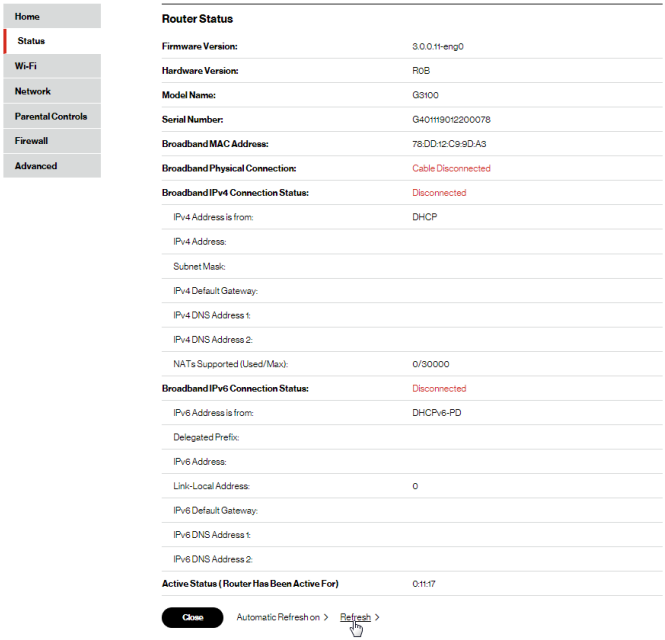
 |

MAIN SCREEN

2.3b/ STATUS

Router Status

This section displays firmware and hardware version numbers, and the status of your router's local network (LAN) and internet connection (WAN).



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.

 |

OVERVIEW

3.0/ OVERVIEW

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

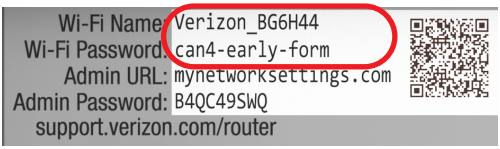
802.11b has a maximum data rate of 11 Mbps, 802.11a and 802.11g have a maximum data rate of 54 Mbps, 802.11n has a maximum data rate of 450 Mbps, 802.11ac has a maximum data rate of 3.12 Gbps, and 802.11ax has a maximum data rate of 4.8 Gbps.

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

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

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

Your router integrates multiple layers of security. These include Wi-Fi Protected Access (WPA/WPA2), and firewall.



3.1/ WI-FI STATUS

Use the Wi-Fi status feature to view the status of your router's Wi-Fi network.

To view the status:

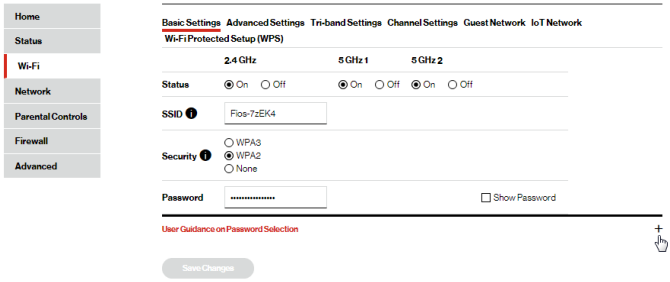
1. Access the dashboard main page. You can quickly view your router's Wi-Fi status in the **Wi-Fi** column.
2. In the **Wi-Fi** column for **Primary Network** and **Guest Network**, the following information displays:
   - **ON/OFF** - displays whether the Wi-Fi radio is active. When the radio is not enabled, no Wi-Fi devices will be able to connect to the office network.
   - **Wi-Fi Name (SSID)** - displays the SSID (Service Set Identifier) shared among all devices on a Wi-Fi network. The SSID is the network name. All devices must use the same SSID.
   - **Wi-Fi Password** - displays the Pre-Shared Key of the Wi-Fi security.

 |

BASIC SETTINGS

3.2/ BASIC SETTINGS

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

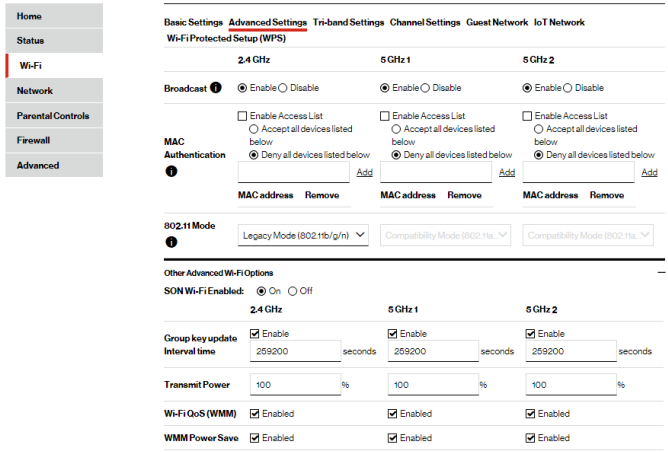


To configure the basic security radio, SSID and security settings:

1. Select Wi-Fi from the left pane, and then click **Basic Settings**.
2. To activate the Wi-Fi radio, click the **On** radio button.
3. If desired, enter a new name for the Wi-Fi network in the SSID field or leave the default name that displays automatically.
4. To activate the Wi-Fi security, click the **WPA2** or **WPA3** radio button.
5. Enter the PSK (Pre-Shared Key) password.
6. Click **Save Changes** to save the changes.

3.3/ ADVANCED SETTINGS

You can change your advanced Wi-Fi security settings, such as disable your SSID broadcast to secure your Wi-Fi traffic; stop your Fios Router from broadcasting your SSID; set Wi-Fi MAC authentication to limit access to specific Wi-Fi devices; and change the Wi-Fi mode to limit or allow access to your Wi-Fi network based on the type of technology as well as other advanced Wi-Fi options.



 |

ADVANCED SETTINGS

3.3a/ BROADCAST

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

1. Select **Wi-Fi** from the left pane, and then click **Advanced Settings**.
2. To enable SSID broadcasting, click the **Enable** radio button. SSID broadcast is enabled by default. The SSID of the Wi-Fi network will be broadcast to all Wi-Fi devices.

   To disable SSID broadcasting, click the **Disable** radio button. 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.
3. When all changes are complete, click **Save Changes** to save the changes.

3.3b/ MAC AUTHENTICATION

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

To set Wi-Fi MAC authentication:

1. To enable access control, select the **Enable Access List** check box.

2. Select either:
    - **Accept all devices listed below** – allows only 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.

    - **Deny all devices listed below** – denies access to the listed devices. All other 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, then click the **Add** button.
4. Repeat step 2 and step 3 to add additional devices, as needed.
5. To remove a specific device's MAC address, click the **Remove** button next to the specific MAC address.
6. When all changes are complete, click **Save Changes** to save the changes.

 |

ADVANCED SETTINGS

3.3c/ 802.11 MODE

From the 802.11 Mode page, you can limit the Wi-Fi access to your network by selecting the 2.4 GHz and 5 GHz Wi-Fi communication standard (mode) best suited or compatible with the devices you allow access to your Wi-Fi network.

Select the Wi-Fi mode as follows:

- Compatibility – This is the default mode setting on 5 GHz, providing a good balance of performance and interoperability with existing Wi-Fi devices. 802.11a,n,ac and ax devices can connect.
- Legacy – This is the default mode setting on 2.4 GHz, providing broad connection support for old and new Wi-Fi devices. Only 802.11b,g and n devices can connect.
- 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.
- When all changes are complete, click **Save Changes** to save the changes.

3.3d/ OTHER ADVANCED WI-FI OPTIONS

You can view additional Wi-Fi options.

Comment: Recommend leaving defaults as is unless otherwise directed.

View the following options:

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.

- SON Wi-Fi Enabled - allows for smart roaming to provide reliable Wi-Fi network with full signal strength in all areas.
- Group key update – to update the WPA shared key, click the **Enable** checkbox.
- Interval time – time interval used to update the WPA shared key (used to generate the group key).
- Transmit Power – adjusts the power of the Wi-Fi signal.
- 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.

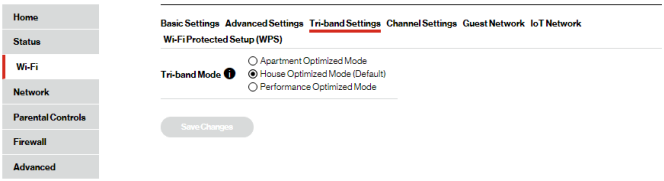
Important: WMM (Wi-Fi Multimedia) QoS and Power Save require a Wi-Fi client device which also supports WMM.

 |

TRI-BAND SETTINGS

3.4/ TRI-BAND SETTINGS

Using Fios Router's Tri-band network management, you can control network congestion and accommodate multiple devices with one 2.4 GHz and two 5 GHz frequency bands on your Wi-Fi network.



To configure the Tri-band mode:

1. Select **Wi-Fi** from the left pane, and then click **Tri-band Settings**.
2. Select the Tri-band mode as follows:
   - **Apartment Optimized Mode** – Provides the 2.4 GHz frequency band and the single 5 GHz frequency band which gets the best channel score. This is recommended for homes with many neighboring Wi-Fi networks.
   - **House Optimized Mode** –
   - This is the default mode setting, providing the 2.4 GHz and two 5 GHz bands. If no Fios Extender connects to the Fios Router over Wi-Fi, then both 5 GHz bands are available to connect to your devices. If the Fios Extender connects to the Fios Router over Wi-Fi, then the 2nd 5 GHz band is only available to connect the router to Fios Extenders. This is recommended for homes with few neighboring Wi-Fi networks.

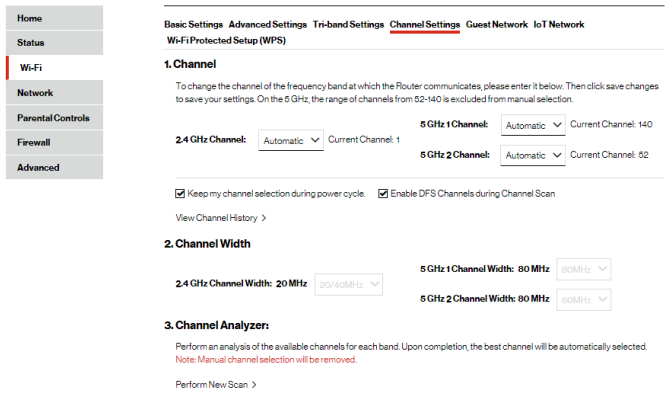
- **Performance Mode** – Enables the 2.4 GHz and two 5GHz bands to connect to your devices, on the router and any connected Fios Extenders. Fios Extenders are unable to connect to the Fios Router over a Wi-Fi connection. This is recommended for the need of high speed and low latency network.

Note: The Fios Router automatically steers Wi-Fi clients to the most appropriate frequency band.

3. When all changes are complete, click **Save Changes** to save the changes.

3.5/ CHANNEL SETTINGS

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



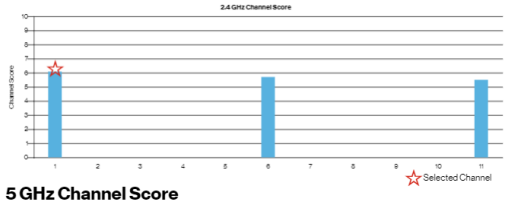
 |

CHANNEL SETTINGS

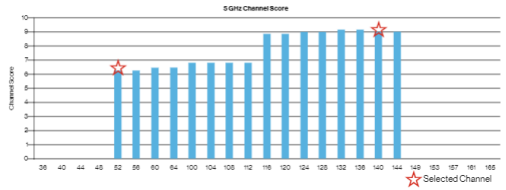
4. Channel Score:

The router scans all available channels for a number of factors, such as the number of nearby Wi-Fi access points, their signal strength, and the interference these may cause. The router then uses these to rank and select the best available channel on each band at the time.

2.4 GHz Channel Score



5 GHz Channel Score

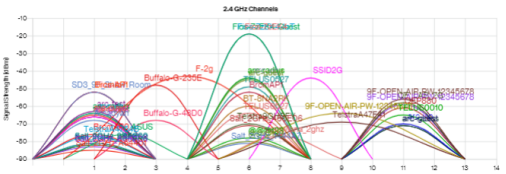


Results from scan performed: Wait for NTP server to synchronize

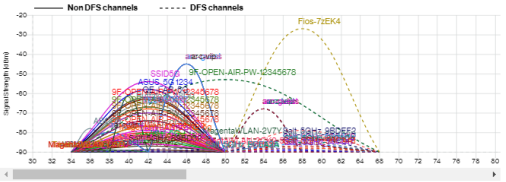
5. Channel Analysis:

The router scans all available channels for Access Points which are broadcasting on a channel(s) and their signal strength. Below is the most recent scan report.

2.4 GHz Channel



5 GHz Channel



Results from scan performed: Wait for NTP server to synchronize

On the **Channel Settings** page for either 2.4 GHz or 5 GHz, the following information displays:

- **Channel** - this is the radio channel used by the Wi-Fi router and its clients to communicate with each other. The channel must be the same on the router and all of its Wi-Fi clients.
  - Select the channel you want the Wi-Fi radio to use to communicate, or accept the default **Automatic** channel selection. Then the router will automatically assign itself a radio channel.
  - Select the **Keep my channel selection during power cycle** check box to save your channel selection when your Fios Router is rebooted.
  - DFS Channels are enabled by default during channel scans. To disable DFS scan uncheck the DFS option.

  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.
- **Channel Width** - displays the Wi-Fi channel currently in use on each band. Default setting is "**Auto**", users can select from available non-DFS channels. On 5 GHz, the DFS channels range from 52-144.

 |

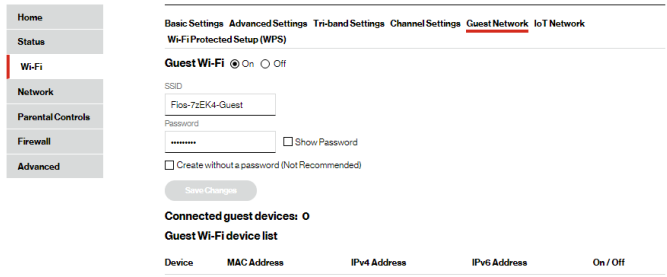
- **Channel Analyzer** - displays the analysis of channel availability.

  Click **Perform New Scan** to perform channel availability scan for the Fios Router accommodating the best radio channel and providing the best Wi-Fi performance.
- **Channel Score** - scans and displays a network congestion score of one to ten in each Wi-Fi channel. It can be used to determine which channels to use or to avoid. Higher score indicates less congestion in a channel.
- **Channel Analysis** - scans and displays channel bandwidth and signal strength of available APs.

3.6/ GUEST NETWORK

The **Guest Network** is designed to provide internet connectivity to your guests but restricts access to your primary network and shared files. The primary network and the guest network are separated from each other through firewalls. You create one Guest Wi-Fi SSID and one password, and use it for all guests. **Guest Wi-Fi** can be managed using either the Fios Router's web interface, or via the Verizon MyFios app. The guest network SSID does not change when you make a change to your primary network SSID.

The Fios Router 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 "Fios-ABCDE" then the default SSID for Guest Wi-Fi is "Fios-ABCDE-Guest".



3.6a/ GUEST WI-FI

To enable Guest Wi-Fi:

1. From the main menu, select **Wi-Fi**, then select **Guest Network**.
2. Click the **On** radio button and enter a valid **SSID** and **Password**.
3. Press **Save Changes** to save the changes.

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

3.6b/ GUEST WI-FI DEVICES

The devices on the **Guest Network** can be viewed on the **Guest Wi-Fi device list**. If the admin toggles the button next to a device to **Off**, that device will be blocked from accessing the internet.

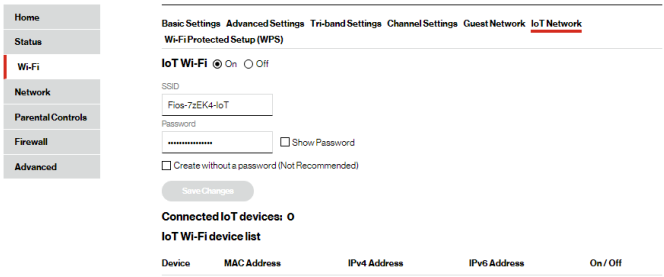
 |

IOT NETWORK

3.7/ IOT NETWORK

The router supports connection of multiple IoT devices on a separate WiFi 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 unrestricted.

The Fios Router 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 "Fios-ABCDE" then the default SSID for IoT Wi-Fi is "Fios-ABCDE-IoT".



To enable IoT Wi-Fi link:

1. Select **Wi-Fi** from the left pane, and then click **IoT Network**.
2. Click the **On** radio button and create an SSID and password.
3. Press **Save Changes** to save the changes.

The connected IoT devices can be viewed on the **IoT Wi-Fi device list**. If the admin toggles the button next to a device to **Off**, that device will be blocked from accessing your Wi-Fi network.

3.8/ 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 Fios Router creates a secure Wi-Fi network connection.

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

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

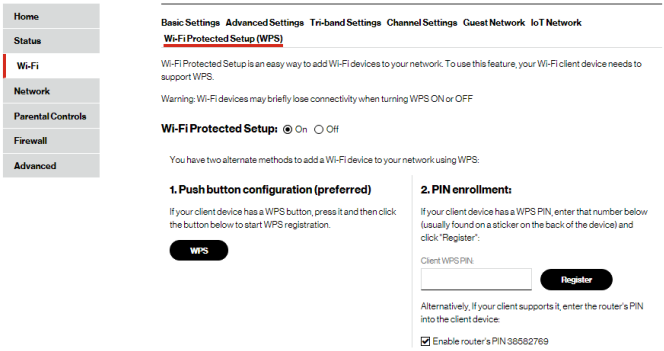
You can easily add Wi-Fi devices to your Wi-Fi network using the WPS option if your Wi-Fi device supports the WPS feature.

 |

WI-FI PROTECTED SETUP (WPS)

To access WPS using the user interface:

1. From the main menu, select **Wi-Fi** settings, then select **Wi-Fi Protected Setup (WPS)**.



2. Enable the protected setup by moving the selector to **On**.
3. Use one of the following methods:
   - If your Wi-Fi client device has a WPS button, press the unified button on your router for more than two seconds, then click the WPS button on your Wi-Fi device (client) 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 **Client WPS PIN** field. The **Client WPS PIN** field is located in the section **2 - PIN enrollment** on the user interface.
   - Click **Register**.

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

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

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

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

 |

04 /

CONFIGURING NETWORK SETTINGS

You can configure the basic network settings for your Fios Router's network.

 |

ACCESSING NETWORK SETTINGS

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

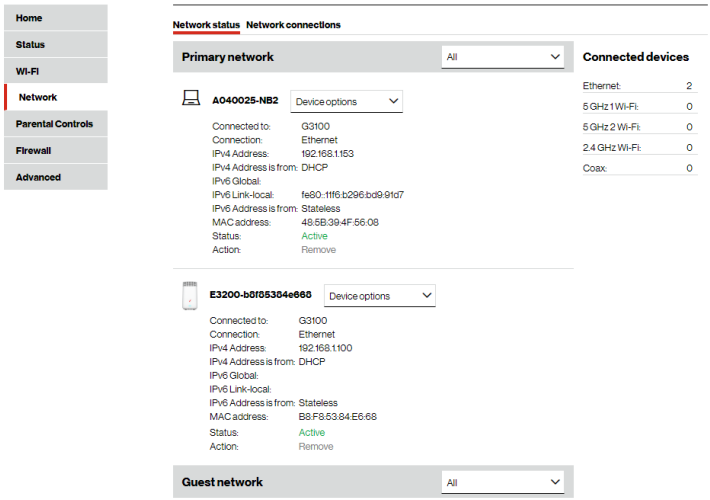
4.0/ ACCESSING NETWORK SETTINGS

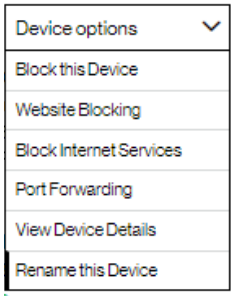
The **Network** section allows you to view and manage your network connections and devices. You can block websites and internet services, set port forwarding, view device details, and rename devices.

4.0a/ NETWORK STATUS

To view your network connections:

Select **Network** from the left pane, and then click **Network status**.



- To view and edit the details of a specific network connected device, click the hyperlinked name from the **Device options** drop-down menu.
- To filter the network connected device, click the drop down menu 

and select one of the options.
- To remove all inactive network connections, click the **Refresh Host** option at the bottom of the list.

The following sections detail the types of network connection settings that you can view and configure.

4.1/ USING NETWORK SETTINGS

You can access and configure common network parameters:

- **Block this Device/Un-Block this Device** - Click this option to quickly enable/disable a device from having internet access.
- **Website Blocking** - To block specific websites, click Website Blocking. The Parental Controls page displays.

 |

For additional information about blocking websites, refer to Chapter 6 Setting Parental Controls.

- **Block Internet Services** - Internet services blocking prevents a device on your network from accessing specific services, such as receiving email or downloading files from FTP sites. Block Internet services by locating the device, then clicking Block Internet Services. The Access Control page displays. For additional information on blocking internet services, refer to the Access Control section in Chapter 7 Configuring Security Settings.
- **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 video conferencing, voice, and chat, to access servers in the local network. To access the Port Forwarding page, click Port Forwarding.

  For additional information, refer to the Port Forwarding section in Chapter 7 Configuring Security Settings.
- **View Device Details** - Click View Device Details to display the Device Information page and view the selected device's information, such as IP Address, MAC address, Network Connection, Lease Type, Port Forwarding Services, as well as the **Ping Test** option.

- **Rename this Device** - To change the name of a specific device, click Rename this Device. The Rename Device page displays. If desired, enter the new device name and/or select a different icon. Click **Apply** to save changes. The Network status page will open with the new name and icon displayed.

 |

05/

USING NETWORK CONNECTIONS

Your Fios Router supports various local area network (LAN) and wide area network (WAN), or internet connections using Ethernet or coaxial cables.

You can configure aspects of the network and internet connections as well as create new connections.

 |

ACCESSING NETWORK CONNECTIONS

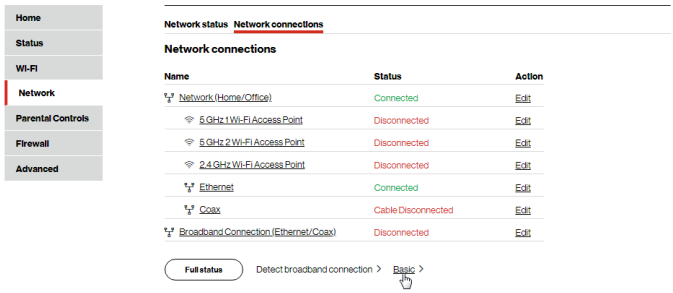
Caution: The settings described in this chapter should only be configured by experienced network technicians. Changes could adversely affect the operation of your router and your local network.

5.0/ ACCESSING NETWORK CONNECTIONS

You can access your network connections and view the connections by connection type.

To access the network connections:

1. Select **Network**, then select **Network Connections**.
2. To display all connection entries, click the **Advanced** button.



3. 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.

5.1/ 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.

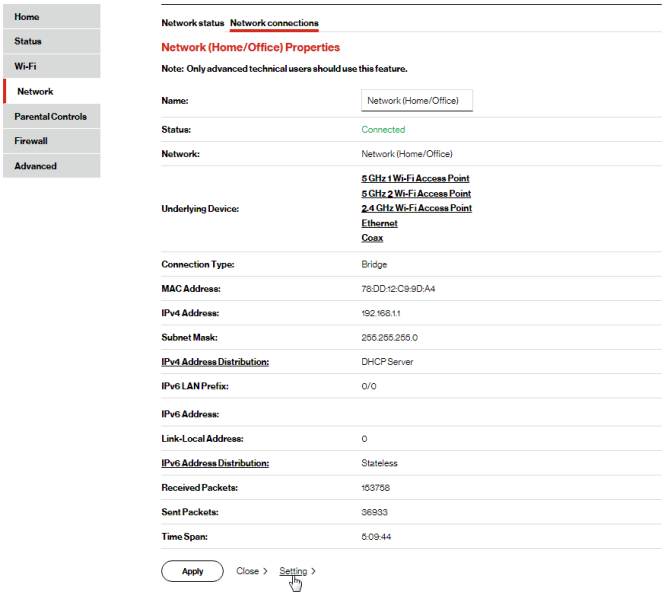
Note: When a network connection is disabled, the underlying devices formerly connected to it will not be able to obtain a new DHCP address from that Fios Router network interface.

To view the connection:

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

 |

NETWORK (HOME/OFFICE) CONNECTION

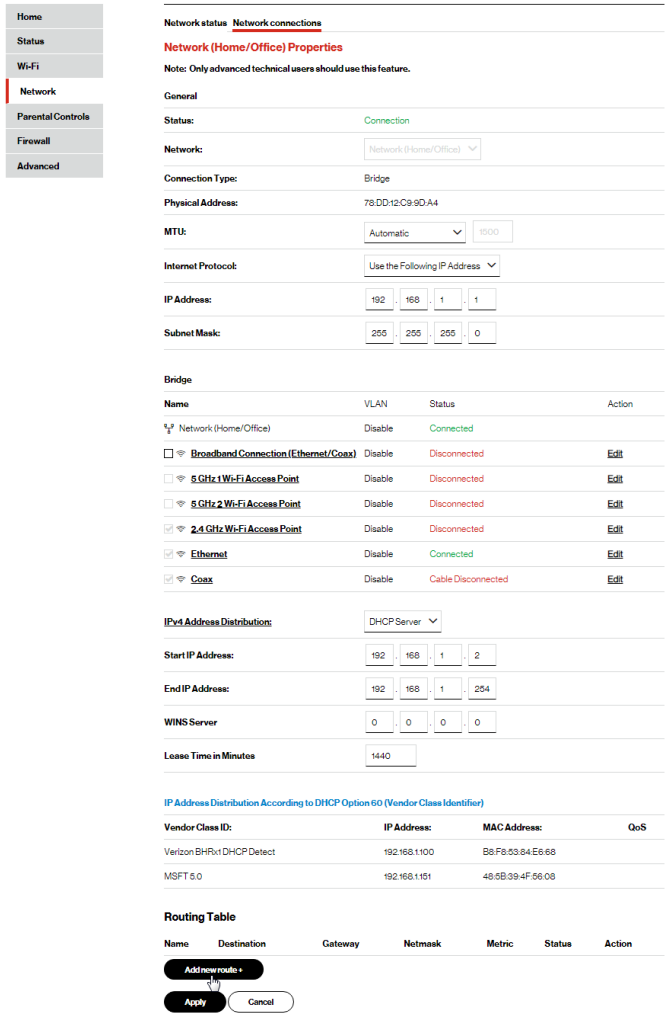


2. To rename a network connection, enter the new network name in the **Name** field.
3. Click **Apply** to save the changes.

5.1a/ CONFIGURING THE HOME/OFFICE NETWORK

To configure the network connection:

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



2. Configure the following sections, as needed.

 |

NETWORK (HOME/OFFICE) CONNECTION

GENERAL

In the General section, verify the following 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 - 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.
- Internet Protocol

  In the Internet Protocol section, specify one of the following:
  - No IPv4 Address: the connection has no IP address. This is useful if the connection operates under a bridge.
  - Obtain an IPv4 Address Automatically: the network connection is required by Verizon to obtain an IP address automatically. The server assigning the IP

address also assigns a subnet mask address, which can be overridden by entering another subnet mask address.

– **Use the Following IP Address**: the network connection uses a permanent or static **IP address** and **Subnet Mask** address, provided by Verizon or experienced network technician.

BRIDGE

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

Caution: Do not change these settings unless specifically instructed to by Verizon. Changes could adversely affect the operation of your Fios Router 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.

 |

NETWORK (HOME/OFFICE) CONNECTION

IP ADDRESS DISTRIBUTION

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

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 Fios Router, configure the network devices as DHCP Clients. There are 2 basic options in this section: **Disabled** and **DHCP Server**.

To set up the Fios Router'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 Fios Router will automatically begin assigning IP addresses from. Since your Fios Router's IP address is 192.168.1.1, the default Start IP Address is 192.168.1.2.
    - **End IP Address** – Enter the last IP address in the IP range that the Fios Router will automatically stop the IP address allocation at. The maximum end IP address range that can be entered is 192.168.1.254.

2. If Windows Internet Naming Service (WINS) is being used, enter the **WINS Server** address.
3. In the **Lease Time in Minutes** field, enter the amount of time a network device is allowed to connect to the Fios Router with its currently issued dynamic IP address.
4. Click **Apply** to save changes.

IP ADDRESS DISTRIBUTION ACCORDING TO DHCP OPTION 60 (VENDOR CLASS IDENTIFIER)

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

ROUTING TABLE

You can configure your Fios Router to use static or dynamic routing.

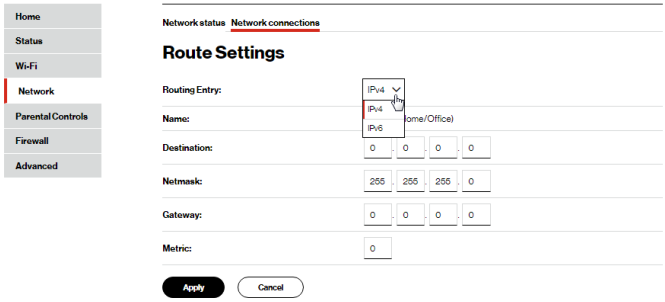
- **Static routing** – specifies a fixed routing path to neighboring destinations based on predetermined metrics.
- **Dynamic routing** – automatically adjusts how packets travel on the network. The path determination is based on network/device reachability and status of network being traveled.

To configure routing:

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

 |

WI-FI ACCESS POINT CONNECTION



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

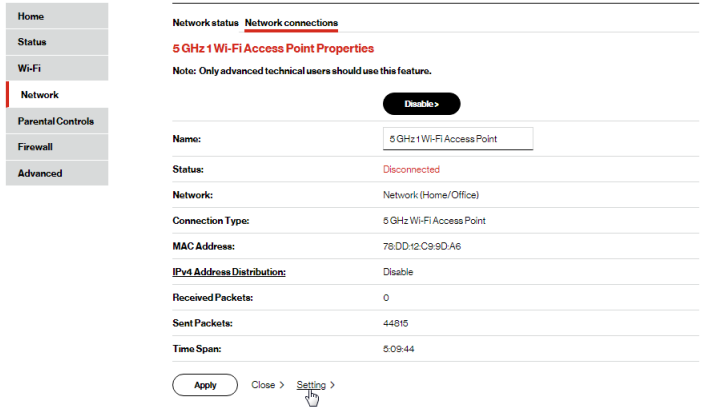
5.2/ WI-FI ACCESS POINT CONNECTION

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

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

To view the connection settings:

1. In the **Network Connections** page, click the **Network (Home/ Office)** connection link.
2. To access the **5.0GHz Wi-Fi Access Point 1 Properties** or **2.4GHz Wi-Fi Access Point 2 Properties** page, click the **5.0GHz Wi-Fi Access Point 1** or **2.4GHz Wi-Fi Access Point 2** link listed under the **Underlying Device** section.



3. To disable the connection, click the **Disable** button.
4. To rename the connection, enter a name in the **Name** field.
5. Click **Apply** to save the changes.
6. Reboot your Fios Router.

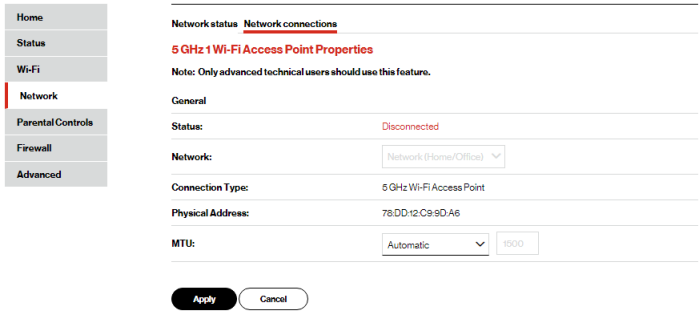
5.2a/ CONFIGURING Wi-Fi ACCESS POINT PROPERTIES

To configure the connection:

1. In the **5.0GHz Wi-Fi Access Point 1 Properties** or **2.4GHz Wi-Fi Access Point 2 Properties** page, click **Setting**. The configuration page displays.

 |

WI-FI ACCESS POINT CONNECTION



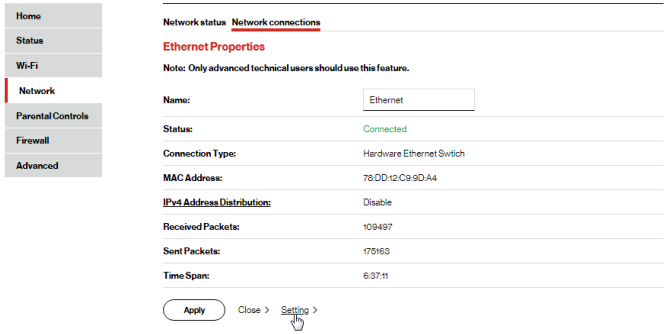
2. Verify the following information:
   - **Status** - displays the connection status of the network.
   - **Network** – displays the type of network connection.
   - **Connection Type** - displays the type of connection interface.
   - **Physical Address** - displays the physical address of the network 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.

5.3/ ETHERNET CONNECTION

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

To view the connection settings:

1. In the **Network Connections** page, click the **Network (Home/ Office)** connection link.
2. Next, to access the **Ethernet Properties** page, click the **Ethernet** link listed under the **Underlying Device** section.



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

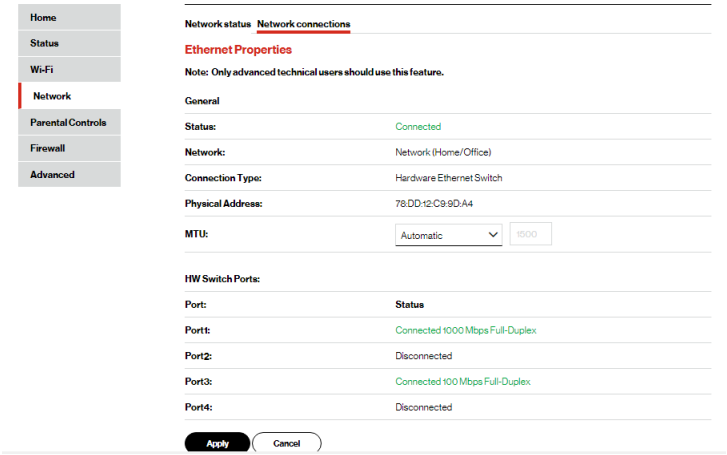
 |

ETHERNET CONNECTION

5.3a/ CONFIGURING ETHERNET PROPERTIES

To configure the connection:

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



2. Configure the following settings, as needed.

GENERAL

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.

5.4/ BROADBAND CONNECTION (ETHERNET/COAX)

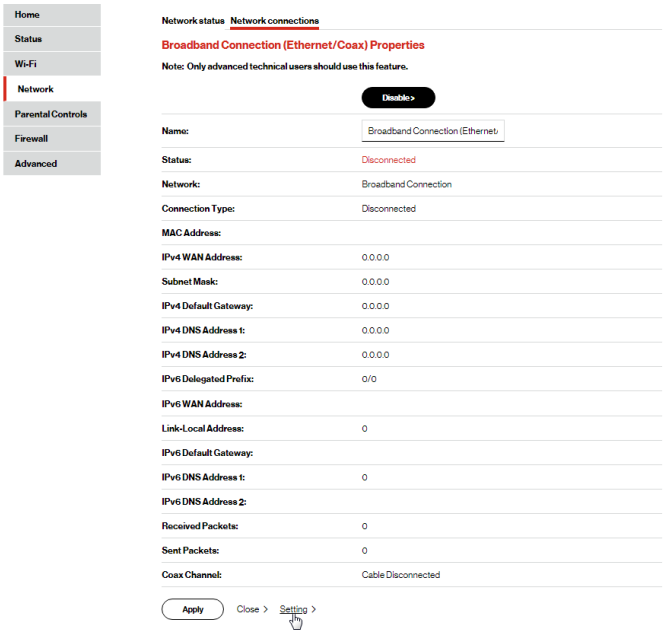
You can view the properties of your broadband connection (your connection to the internet). This connection may be via either Ethernet or Coaxial cable.

To view the connection settings:

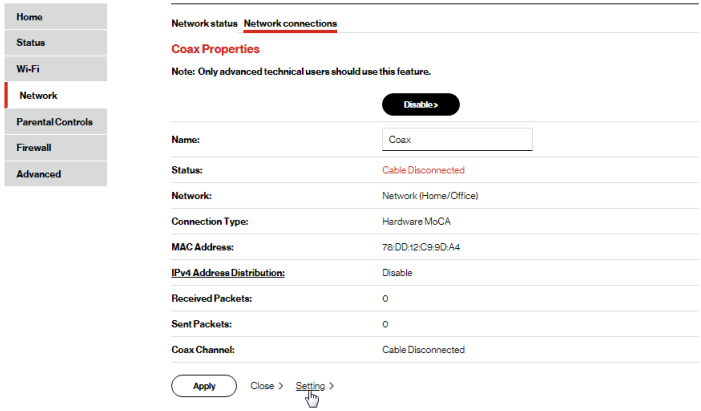
1. In the **Network Connections** page, click the **Broadband Connection (Ethernet/Coax)** or **Coax** link.

 |

BROADBAND CONNECTION (ETHERNET/COAX)



Coax Properties



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

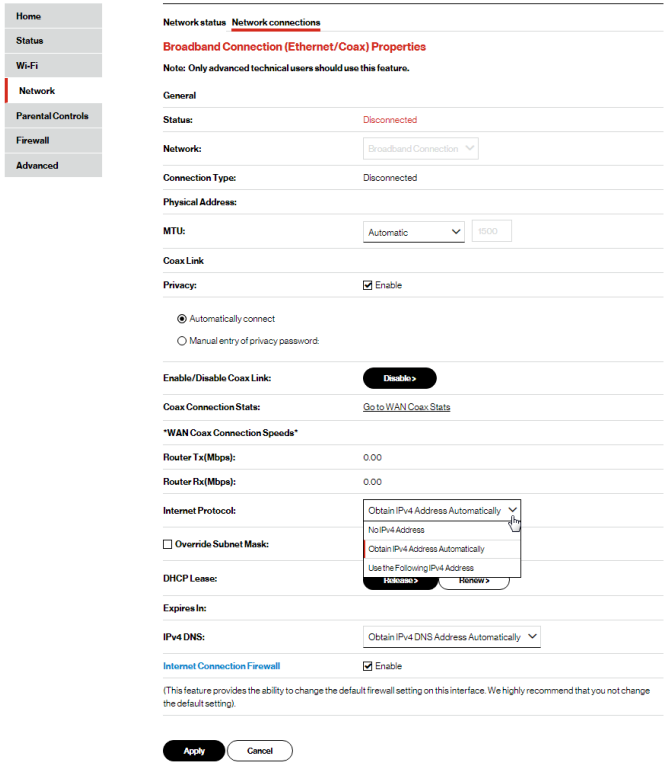
5.4a/ CONFIGURING THE ETHERNET/COAX CONNECTION

To configure the connection:

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

 |

BROADBAND CONNECTION (ETHERNET/COAX)



2. Configure the following settings, as needed.

GENERAL

Verify the following 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**: 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.

COAX LINK

- **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 **Password** field.
- To enable or disable the Coax link, click **Disable** or **Enable**.
- To view the devices connected using the coaxial cable, click the **Go to WAN Coax Status** link.
- In the **Internet Protocol** section, specify one of the following:
  - **No IPv4 Address**: the connection has no IP address. This is useful if the connection operates under a bridge.

 |

  - **Obtain an IPv4 Address Automatically**: the network connection is required by Verizon to obtain an IP address automatically. The server assigning the IP address also assigns a subnet mask address, which can be overridden by entering another subnet mask address.
  - **Use the Following IP Address**: the network connection uses a permanent or static **IP address** and **Subnet Mask** address, provided by Verizon or experienced network technician.
- To override the subnet mask, select the **Override Subnet Mask** check box, then enter the new subnet mask.
- Click **Release/Renew** in the **DHCP Lease** field to drop/get an IP address from the DHCP server.
- In the **Expires In** field, enter the amount of time a network device is allowed to connect to the Fios Router with its currently issued dynamic IP address.
- **IPv4 DNS -** selects **Obtain IPv4 DNS Address Dynamically** for using Dynamic DNS. Each time the public IP address changes, the DNS database is automatically updated with the new IPv4 address. In this way, even though the IP address changes often, the domain name remains constant and accessible.
- **Internet Connection Firewall -** allows you to enable or disable the firewall configuration on this interface.

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

06/

SETTING PARENTAL CONTROLS

The abundance of harmful information on the internet poses a serious challenge for employers who ask “How can I regulate what my employee does on the internet?”

With that question in mind, your Fios Router’s Parental Controls were designed to allow control of internet access on all locally networked devices.

 |

ACTIVATING PARENTAL CONTROLS

6.0/ ACTIVATING PARENTAL CONTROLS

You can create a basic access policy for any computer or device on your Fios Router network. Parental controls limit internet access to specific websites based on a schedule that you create.

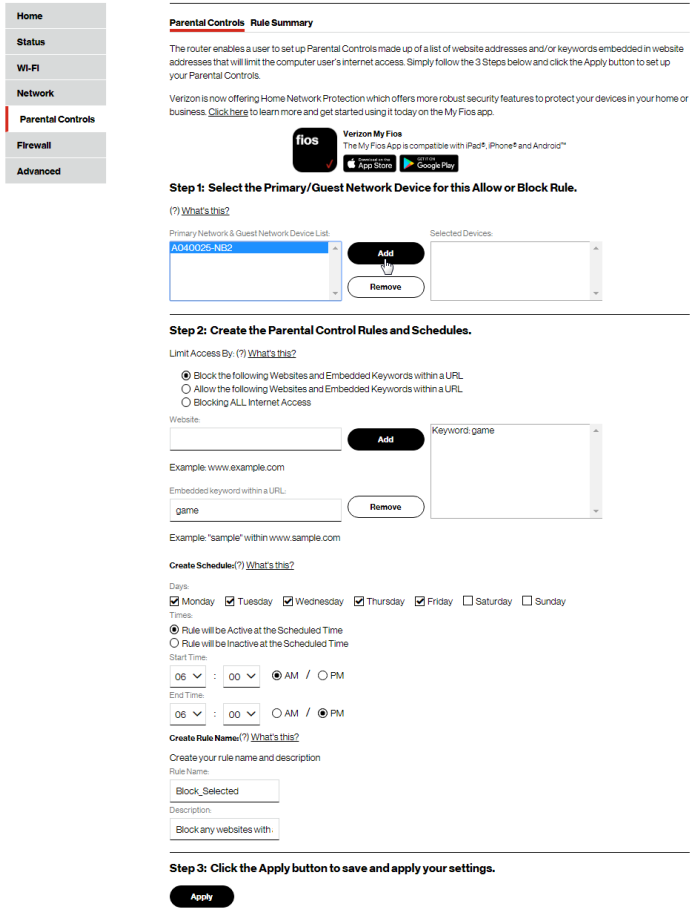
Access can be limited on specific websites or keywords embedded in a website. For example, you can block access to the 'www.anysite.com' as well as block any website that has the word 'any' in its site name.

To limit computer access:

1. Select **Parental Controls**.
2. In Step 1 (optional), select the computers or device where you are limiting access in the **Primary Network & Guest Network Device List** box, then click **Add**. The devices display in the **Selected Devices** section.
3. To remove a device from the **Selected Devices** list box, select the device, then click **Remove**. The device displays in the **Primary Network & Guest Network Device List** list box.
4. In Step 2, click one of the following options in the **Limit Access By** section:
    - **Block the following Websites and Embedded Keywords within a URL** – blocks the specified websites and websites with names containing the specified keyword.
    - **Allow the following Websites and Embedded Keywords within a URL** – allows the specified websites and websites with names containing the specified keyword.

- **Block ALL Internet Access** – blocks the access to all internet websites.

5. Enter the name of the **Website** or **Embedded keyword within a URL**, then click **Add**.



 |

RULE SUMMARY

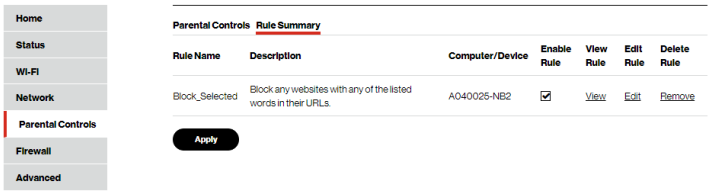
6. To remove a website or keyword, select the word, then click **Remove**.
7. Create a schedule by selecting the days of the week when the rule will be active or inactive.
8. Set the time when the rule will be active or inactive, then specify the start time and end time.
9. Create a rule name and description.
10. Click **Apply** to save changes.

*NEW! The **Verizon My Fios** app provides robust security to protect your office networks. Click the **Click here** link to download the My Fios app for using the My Fios app on the iOS or Android OS.*

6.1/ RULE SUMMARY

You can view the rules created for your Fios Router.

To view the rule summary, select **Rule Summary**. The Rule Summary page opens with the rule name, description, and computer or device displayed.



You can enable, view, edit, or delete the rule; refer to Scheduler Rules for additional setting details.

07/

CONFIGURING SECURITY SETTINGS

Your Fios Router'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.

 |

FIREWALL

This chapter covers the following security features:

- Firewall - select the security level for the firewall.
- Access Control - restrict access from the local network to the internet.
- Port Forwarding - enable access from the internet to specified services provided by computers on the local network.
- Port Triggering - define port triggering entries to dynamically open the firewall for some protocols or ports.
- DMZ Host - allows a single device on your primary network to be fully exposed to the internet for special purposes such as an email server.
- Static NAT - allow multiple static NAT IP addresses to be designated to devices on the network.
- IPv6 Pinhole - provide access tunnel to a service on a host for a particular application.

7.0/ FIREWALL

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

The firewall provides both the security and flexibility that office users seek. It provides a managed, professional level of network security while enabling the safe use of interactive applications, such as 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 Fios Router or rejected and barred from passing through your Fios Router, 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 accessing a website on the internet, a request is sent to the internet for this site. When the request reaches your Fios Router, the firewall identifies the request type and origin, such as HTTP and a specific computer in the local network. Unless your Fios Router is configured to block requests of this type from this computer, the firewall allows this type of request to pass to the internet.

 |

FIREWALL

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

7.0a/ SETTING FIREWALL CONFIGURATION

You can select a maximum, typical, or minimum security level to block, limit, 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
Maximum	Blocked	Limited
Typical	Blocked	Unrestricted
Minimum	Unrestricted	Unrestricted

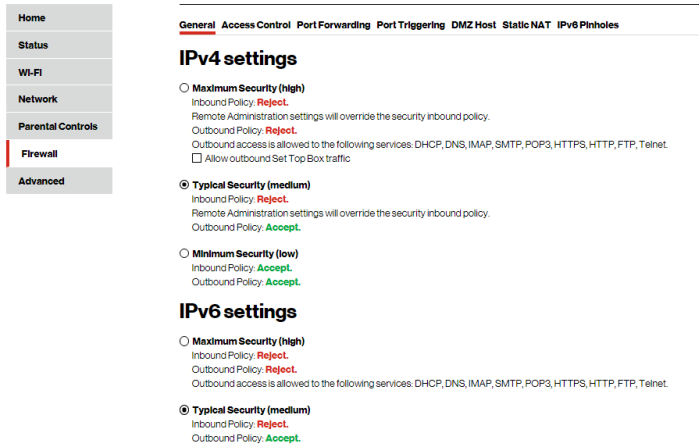
The request access is defined as:

- 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

7.0b/ SPECIFYING GENERAL SETTINGS FOR IPV4 OR IPV6

To set your firewall configuration:

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



2. Select a security level by clicking one of the radio buttons. Using the **Minimum 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** to save changes.

 |

ACCESS CONTROL

7.1/ ACCESS CONTROL

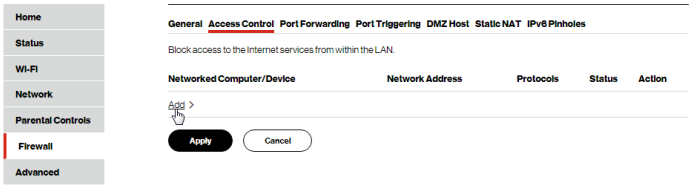
You can block individual computers on your local network from accessing specific services on the internet. For example, you could block one computer from accessing the internet, then block a second computer from transferring files using FTP as well as prohibit the computer from receiving incoming email.

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

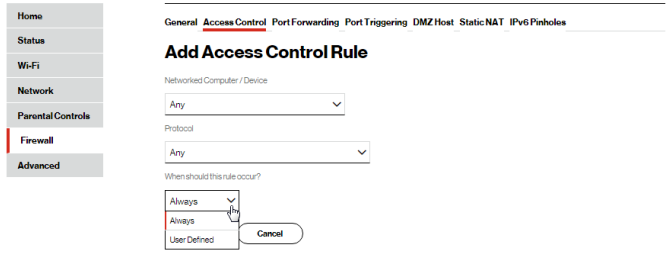
7.1a/ ALLOW OR RESTRICT SERVICES

To allow or restrict services:

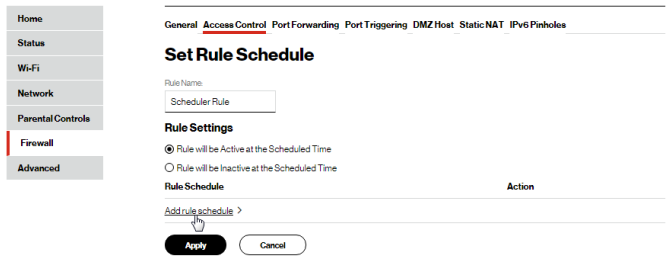
1. From the Firewall page, select **Access Control**. The Access Control page opens with the Allows and Blocked sections displayed. The Allowed section only displays when the firewall is set to maximum security.



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



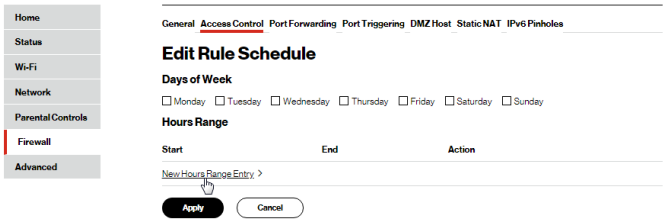
3. To apply the rule to:
   - Networked Computer/Device - select **Any**.
   - Specific devices only - select **User Defined**.
4. In the Protocol field, select the internet protocol to be allowed or blocked. If the service is not included in the list, select **User Defined**. The **Edit Service** page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



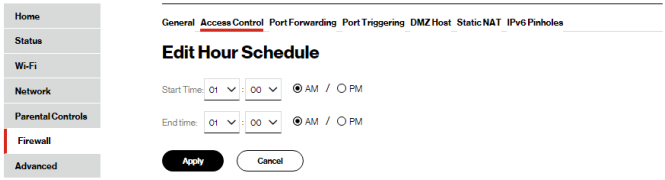
6. Then click **Add rule schedule** to specify the days of the week when the rule will be active.

 |

ACCESS CONTROL



7. Click **New Hours Range Entry** and set the start time and end time when the rule will be active.



8. Click **Apply** to save changes.
9. Click **Apply** again to save all changes.
10. The Access Control page displays a summary of the new access control rule.

7.1b/ DISABLE ACCESS CONTROL

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

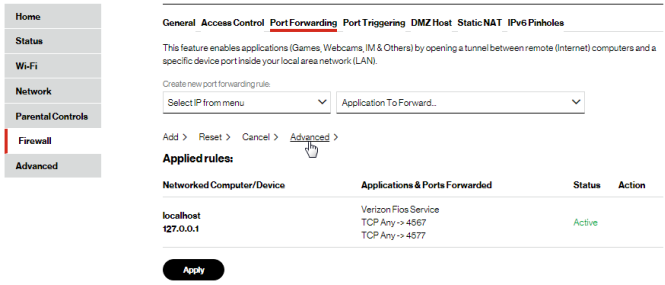
- To disable an access control, clear the check box next to the service name.
- To reinstate the restriction, select the check box next to the service name.
- To remove an access restriction, select the service and click **Remove**. The service is removed from the Access Control table.

7.2/ 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 video conferencing and voice, 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 **Firewall** page, select **Port Forwarding**. The **Port Forwarding** page opens with the current rules displayed.



 |

PORT FORWARDING

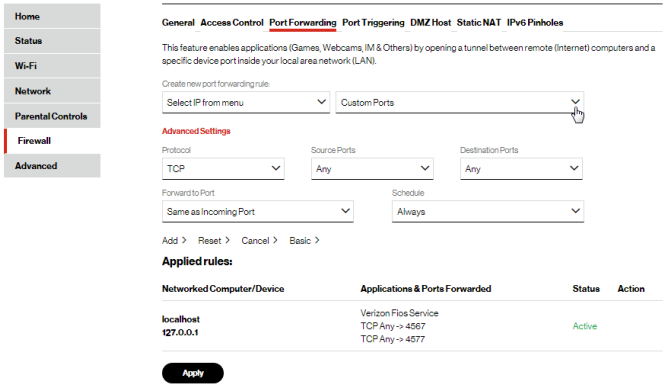
2. To create a new rule, select the IP address in the **Select IP from menu** drop down.
3. Select the application in the **Application To Forward** drop down.
4. Click **Add**. The rule displays in the **Applied Rules** section.
5. Click **Apply** to save changes.

7.2a/ ADVANCED PORT FORWARDING RULES

You can configure advanced port forwarding rules.

To configure the rules:

1. In the **Port Forwarding** page, select **Advanced**.



2. If needed, to select a port to forward communication to, select an option in the **Custom Ports** drop down.

3. If a single port or range of ports is selected, text boxes display. Select the **Protocol** and the port numbers.
4. To schedule the rule, select either **Always** or **User Defined** in the **Schedule** list box.
5. Click **Add**. The rule displays in the **Applied Rules** section.
6. Click **Apply** to save changes.

7.3/ PORT TRIGGERING

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

For example, a web server is accessed using UDP protocol on port 2222. The web server then responds by connecting the user using UDP on port 3333, when a web 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 Fios Router IP, and the connection is not sent back to the host since it is not part of a session.

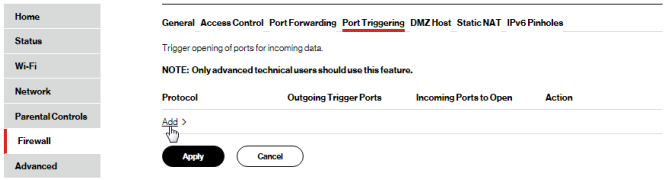
 |

PORT TRIGGERING

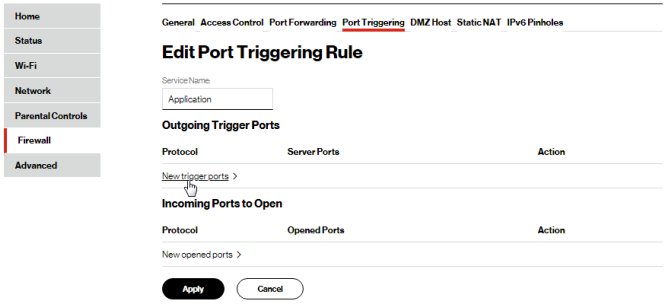
To resolve the conflict, a port triggering entry must be defined, which allows inbound traffic on UDP port 3333 only after a network host generated traffic to UDP port 2222. This results in your Fios Router accepting the inbound traffic from the web server and sending it back to the network host which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

To configure port triggering:

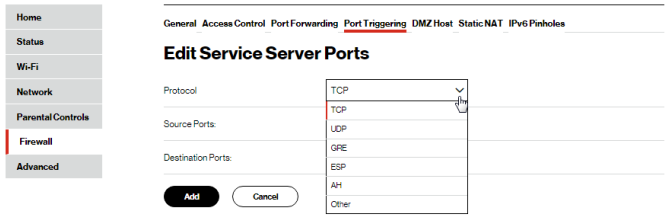
1. Select Port Triggering.



2. To add a service as an active protocol, click **Add**. The **Edit Port Triggering Rule** page displays.



3. Enter the service name then configure its inbound and outbound trigger ports. Click **Add** to save changes.



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

7.4/ DMZ HOST

DMZ Host allows a single device on your primary network to be fully exposed to the internet for special purposes such as an email server.

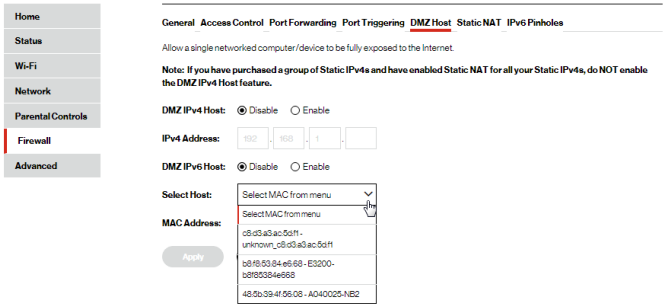
Warning: Enabling DMZ Host is a security risk. When a device on your network is a DMZ Host, it is directly exposed to the internet and loses much of the protection of the firewall. If it is compromised, it can also be used to attack other devices on your primary network.

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

1. From the **Firewall** page, select **DMZ Host**.
2. Select **Enable** for the DMZ Host.
3. Enter the IP address of the device you want to designate as the DMZ Host.
4. Click **Apply**.

 |

STATIC NAT

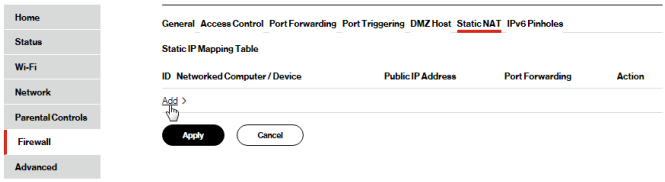


7.5/ STATIC NAT

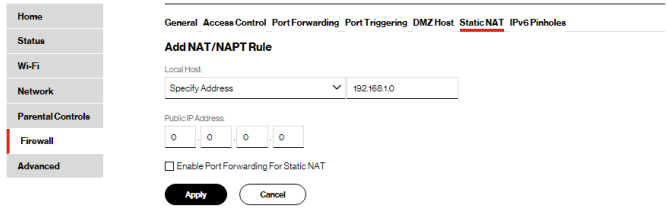
Static NAT allows devices located behind a firewall that is configured with private IP addresses to appear to have public IP addresses to the internet. This allows an internal host, such as a web server, to have an unregistered (private) IP address and still be accessible over the internet.

To configure static NAT:

1. Select **Static NAT**.



2. To create a static NAT, click **Add**. The **Add NAT/NAPT Rule** page displays.



3. Select a source address in the **Specify Address** field or enter an IP address in the text box.
4. Enter the **Public IP Address**.
5. If using port forwarding, select the **Enable Port Forwarding for Static NAT** check box.
6. Click **Apply** to save changes.
7. Repeat these steps to add additional static IP addresses.

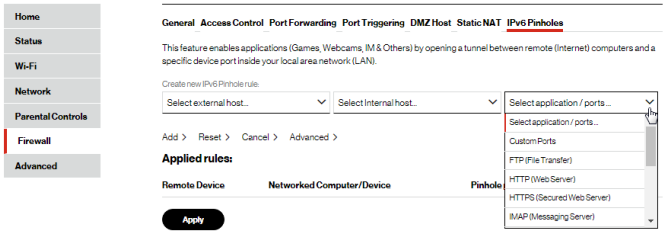
 |

IPV6 PINHOLES

7.6/ IPV6 PINHOLES

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

You can view the Pinhole rules created for your Fios Router. To view the rule summary, select **IPv6 Pinhole**. The screen displays opened pinhole port and its status. It shows the IP addresses of remote device and connected device on your network.



You can enable, view, edit, or delete the rules as shown on the above screen.

08/

CONFIGURING ADVANCED SETTINGS

Advanced settings cover a wide range of sophisticated configurations for your Fios Router's firmware and network.

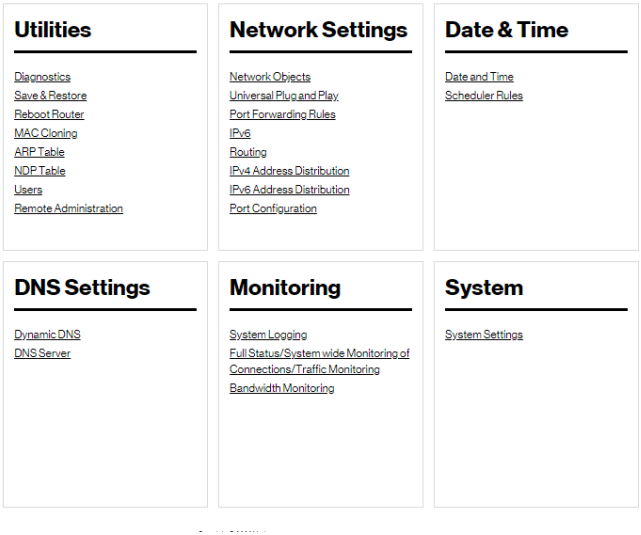
 |

USING ADVANCED SETTINGS

Caution: Many of the settings described in this section should only be configured by experienced network technicians. Changes could adversely affect the operation of your Fios Router and local network.

8.0/ USING ADVANCED SETTINGS

You can access the following settings:



To access the advanced settings:

1. Select **Advanced** from the left pane.
2. Select a topic by clicking the topic name.

8.1/ UTILITIES

You can access the following advanced settings:

- Diagnostics – performs diagnostic tests.
- Save and Restore – resets your Fios Router to its default settings.
- Reboot Router – restarts your Fios Router.
- MAC Cloning – clones the MAC address.
- ARP Table – displays active devices with their IP and MAC addresses.
- NDP (Neighbor Discovery Protocol) Table – displays active devices with their IPv6 and MAC addresses of DHCP connection.
- Users – creates and manages remote users.
- Remote Administration – enable remote configuration of your Fios Router from any internet-accessible computer.

 |

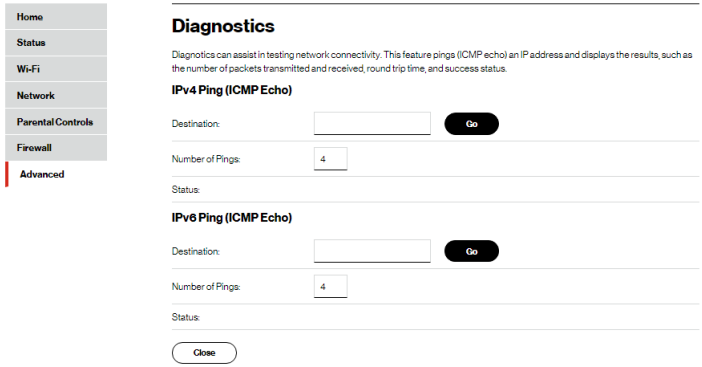
UTILITIES

8.1a/ DIAGNOSTICS

You can use diagnostics to test network connectivity.

To diagnose network connectivity:

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



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

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

3. Click **Close** to exit the session.

8.1b/ SAVE AND RESTORE

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

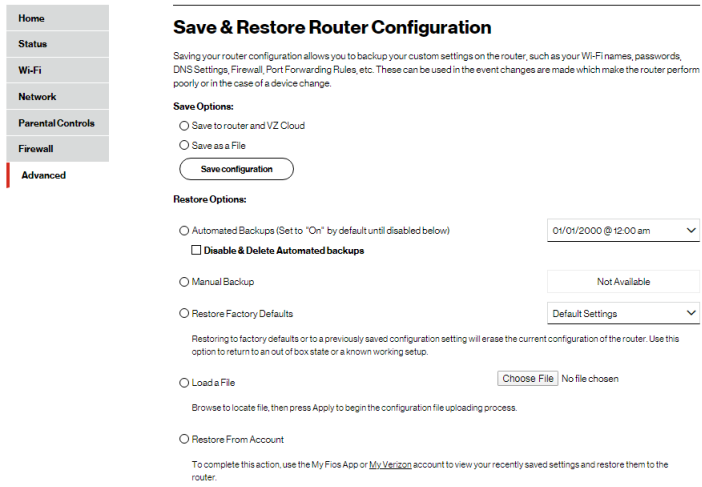
Only configuration files saved on a specific Fios Router can be applied to that Fios Router. You cannot transfer configuration files between Fios Routers.

Warning: Manually editing a configuration file can cause your Fios Router to malfunction or become completely inoperable.

Save Options

To save the configuration file:

1. Select **Save & Restore** in the **Utilities** section.



 |

2. Select **Save to router and VZ Cloud** or **Save as a File** to save the current configuration, then click **Save configuration**.
3. If you select **Save as a File**, the configuration file is saved to you web browser's download folder.

Restore Options

You can restore your configuration settings to your Fios 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 Fios Router 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.

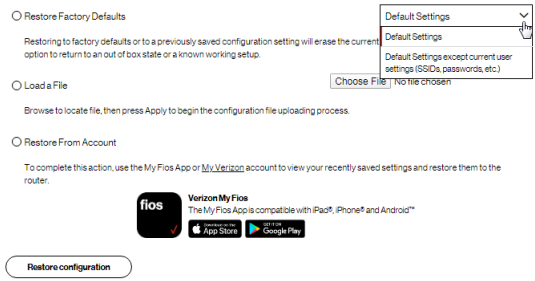
Note: When restoring defaults, the setting and parameters of your Fios Router are restored to their default values. This includes the administrator password. A user-specified password will no longer be valid.

To backup your Fios Router's settings:

1. Select **Save & Restore** in the **Utilities** section.
2. To take a backup of the current settings, click **Automated Backups** or **Manual Backup**. You will be prompted to save a file with the extension ".enc".
3. Click **Backup** to begin the configuration backup process.

To restore your Fios Router's factory default settings:

1. Select **Save & Restore** in the **Utilities** section.
2. Click **Restore Factory Defaults**.



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

To load the configuration file:

1. Select **Save & Restore** in the **Utilities** section.
2. To load a previously saved configuration file, click **Choose File**.

 |

3. Browse to the location of the file, and click **Apply** to begin the configuration uploading process.
4. Accessing the **My Fios** app or the **My Verizon** account also allows you to restore the previously saved settings.
5. Click **Restore configuration** button. Your Fios Router will automatically restart with that configuration.

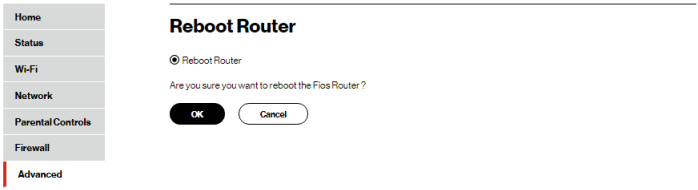
8.1c/ REBOOT FIOS ROUTER

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

You can reboot your Fios Router using the Reboot Router Only feature. Refer to 1.3b/ REAR PANEL for power button options.

To reboot your Fios Router using the user interface:

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



2. To reboot, click **OK**. Your router will reboot. This may take up to a minute.
3. To access your Fios Router user interface, refresh your web browser.

4. After the Router Status LED on the front panel turns solid white, you will automatically be sent to the web browser login page.

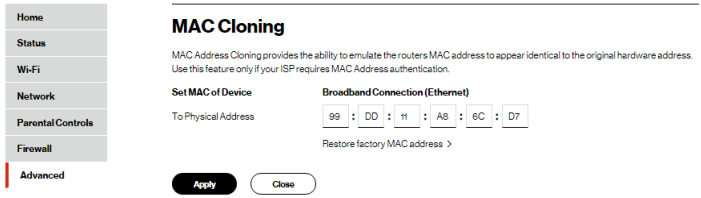
8.1d/ MAC CLONING

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

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

To copy the MAC address of the existing device:

1. Select **MAC Cloning** in the **Utilities** section.



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

 |

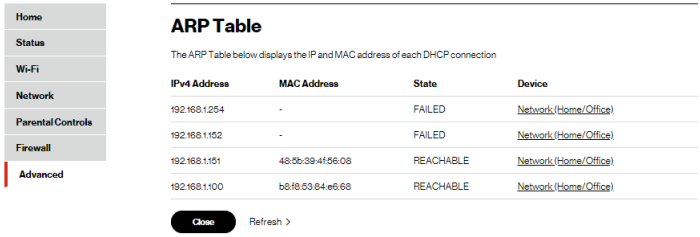
UTILITIES

8.1e/ ARP TABLE

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

To view the IPv4 and MAC addresses:

1. Select **ARP Table** in the **Utilities** section.



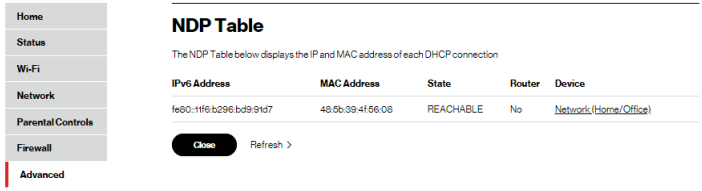
2. Review the IPv4 and MAC address for each device.
3. When complete, click **Close**.

8.1f/ NDP TABLE

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

To view the IPv6 and MAC addresses:

1. Select **NDP** (Neighbor Discovery Protocol) **Table** in the **Utilities** section.



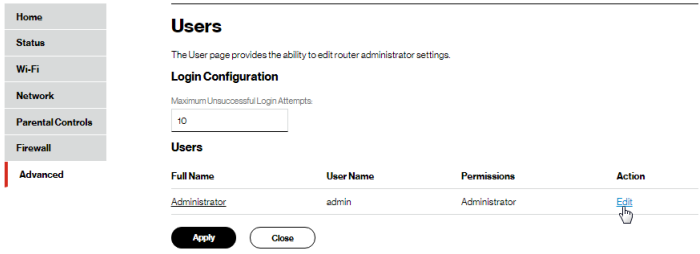
2. Review the IPv6 and MAC address for each device.
3. When complete, click **Close**.

8.1g/ USERS

You can view the users that can currently access your Wi-Fi network. In addition, you can modify their login password and name as well as manage the number of unsuccessful login attempts a user can enter before your Fios Router temporarily denies all further login attempts by that user.

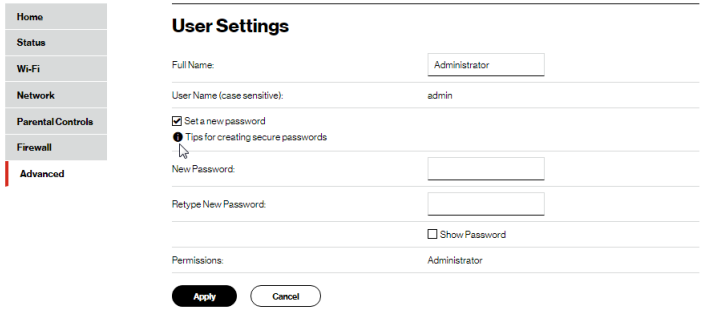
To view users:

1. Select **Users** in the **Utilities** section.



 |

2. In the **Login Configuration** section, enter the maximum number of unsuccessful login attempts.
3. To edit usernames and passwords, click the **Edit** in the **Action** column. The **User Settings** page displays.



4. Edit the username and set a new password, as needed.
5. To add a new user, specify the following parameters:
   - **Full Name** - name of the user.
   - **User Name** – name the user enters to remotely access the office network. This field is case-sensitive.
6. To set a new Password, select the **Set a new password** check box. The **New Password** fields display.
7. Verify the level of access for the user in the **Permissions** field.
8. Click **Apply** to save changes. The **Users** page opens with the user information displayed.
9. Click **Apply** again to save changes and exit.

8.1h/ REMOTE ADMINISTRATION

Caution: Enabling Remote Administration places your Fios Router network at risk from outside attacks.

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

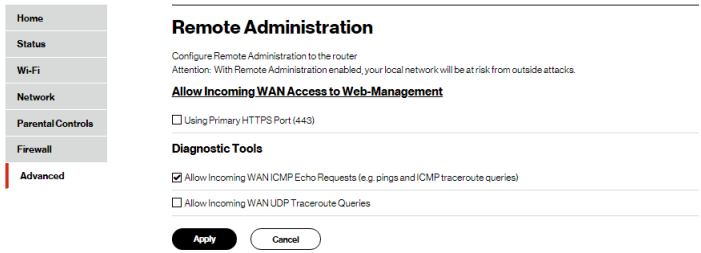
You can allow incoming access to the following:

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

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

To enable remote administration:

1. Select **Remote Administration**.



 |

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

8.2/ NETWORK SETTINGS

You can configure the following network settings:

- **Network Objects** – defines a group, such as a group of computers.
- **Universal Plug and Play (UPnP)** – checks the validity of all UPnP services and rules.
- **Port Forwarding Rules** – displays port forwarding rules.
- **IPv6** – enables IPv6 support.
- **Routing** – manages the routing and IP address distribution rules.
- **IPv4/IPv6 Address Distribution** - adds computers configured as DHCP clients to the network.
- **Port Configuration** – sets up the Ethernet ports as either full- or half-duplex ports, at either 10 Mbps, 100 Mbps, or 1000 Mbps.

8.2a/ NETWORK OBJECTS

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

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

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

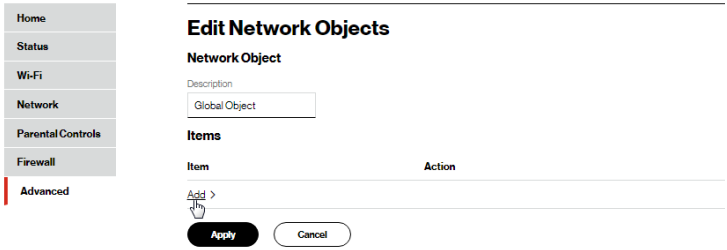
To define a network object:

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

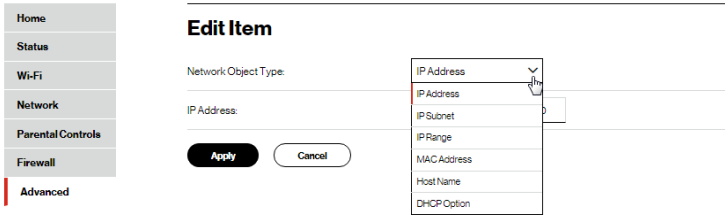
 |

NETWORK SETTINGS

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



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



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

8.2b/ UNIVERSAL PLUG AND PLAY

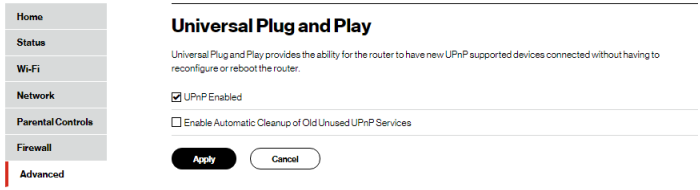
You can use Universal Plug and Play (UPnP) to support new devices without configuring or rebooting your Fios Router.

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. Select **Universal Plug and Play** (UPnP) in the **Network Settings** section.



 |

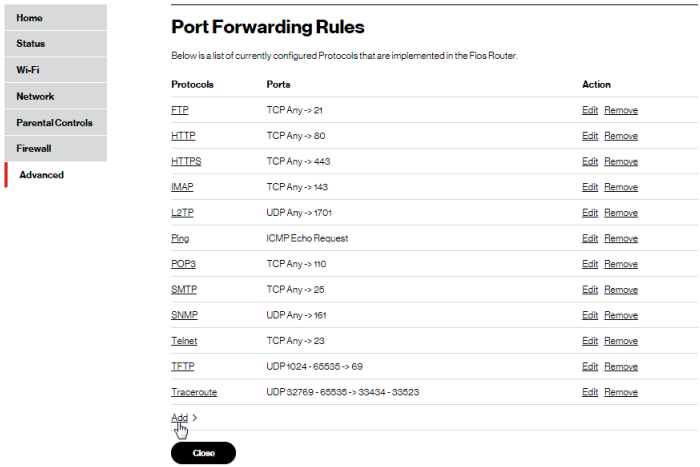
2. To enable UPnP and allow UPnP services to be defined on any network hosts, select the **UPnP Enabled** check box.
3. To enable automatic cleanup of invalid rules, select **Enable Automatic Cleanup of Old Unused UPnP Services** check box.
4. Click **Apply** to save changes.

8.2c/ PORT FORWARDING RULES

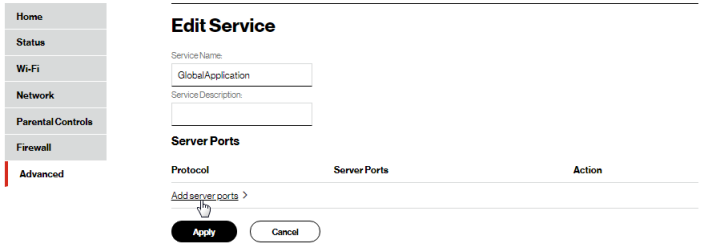
You can view, modify, and delete port forwarding rules.

To access the rules:

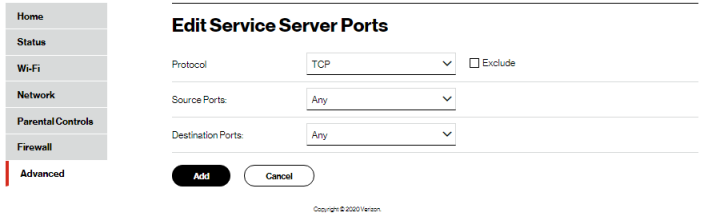
1. Select **Port Forwarding Rules** in the **Network Settings** section.



2. To edit a protocol rule, click the **Edit** icon in the Action column. The **Edit Service** page displays.



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



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

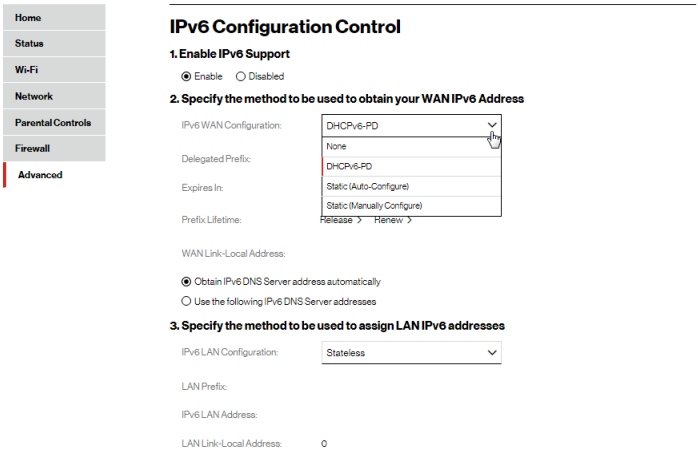
 |

NETWORK SETTINGS

8.2d/ IPv6

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

1. To configure your network to use the IPv6 Internet connection type, select IPv6 from the Advanced page to display the IPv6 service options:



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

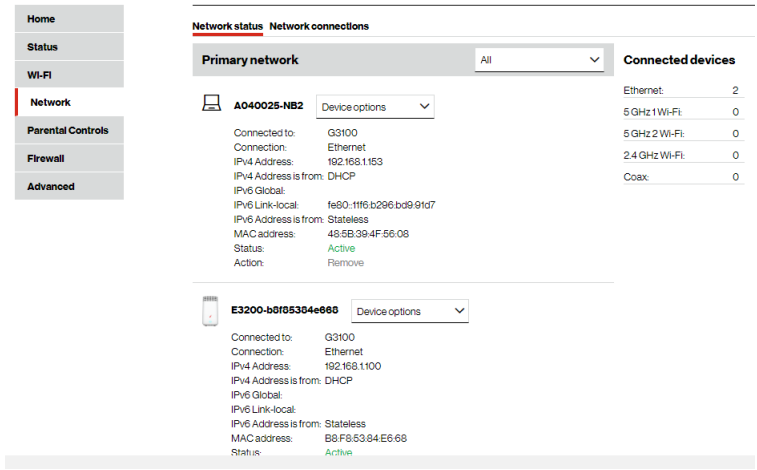
4. Click **Apply** to have changes take effect.

Note: The Internet IPv6 service is required for this feature to work over the internet.

5. To disable the IPv6 service, click on the **Disable** option in the **Enable IPv6 Support** field.
6. Click **Apply** 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** button and the **Status** page on the main menu will reflect the router's new IPv6 address.

You should also see the IPv6 address for all IPv6 supported devices on your local network displayed on the Network/Network Status page.



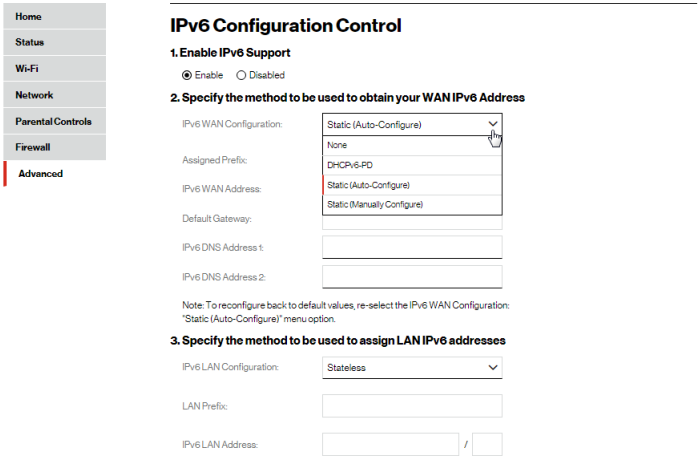
 |

NETWORK SETTINGS

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:

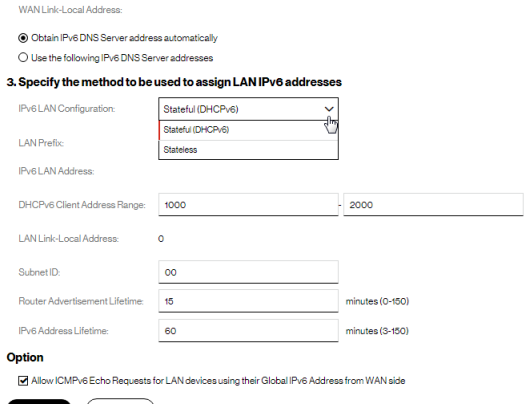


2. Specify the **Static** method to be used to obtain your WAN IPv6 Address by entering:
   - **IPv6 WAN Configuration** (select Static)
   - **Assigned Prefix** (A numeric value between 16 and 128)
   - **IPv6 WAN Address**
   - **Default Gateway**: Fios Router
   - **IPv6** (Primary) **DNS Address 1**
   - **IPv6** (Secondary) **DNS Address 2**

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

Static WAN with LAN IPv6 Stateful Settings

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



2. Specify the **Stateful (DHCPv6)** settings to be used to assign LAN IPv6 addresses by entering the following details:
   - **IPv6 LAN Configuration** (select Stateful from the dropdown list)
   - **LAN Prefix** (automatically populated)
   - **IPv6 LAN Address** (automatically populated)

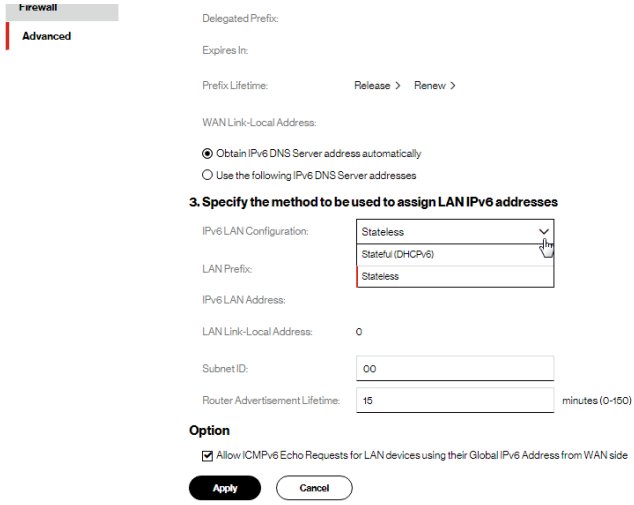
 |

- **DHCPv6 Client Address Range** (start and end)
- **LAN Link Local Address** (automatically populated)
- **Subnet ID** - set the site topology for your internal site
- **Router Advertisement Lifetime** (minutes between 0-150)
- **IPv6 Address Lifetime** (minutes between 3-150)
- **Option: Allow ICMPv6 Echo Request for LAN devices using their Global IPv6 Address from WAN side** - requesting an IPv6 address from any available DHCPv6 servers available on the ISP

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

Static WAN with LAN IPv6 Stateless Settings

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



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

 |

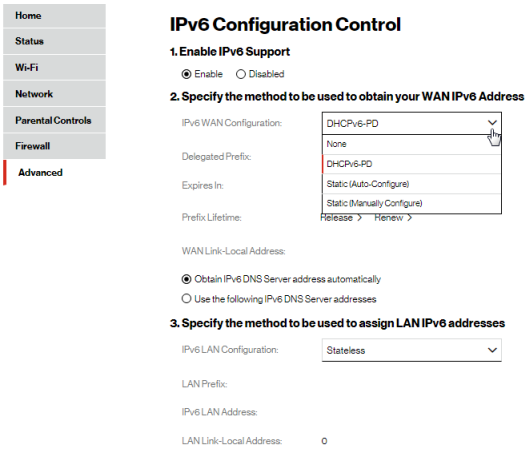
- **Option: Allow ICMPv6 Echo Request for LAN devices using their Global IPv6 Address from WAN side** - requesting an IPv6 address from any available DHCPv6 servers available on the ISP

3. After entering all appropriate IPv6 settings, click **Apply** 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.

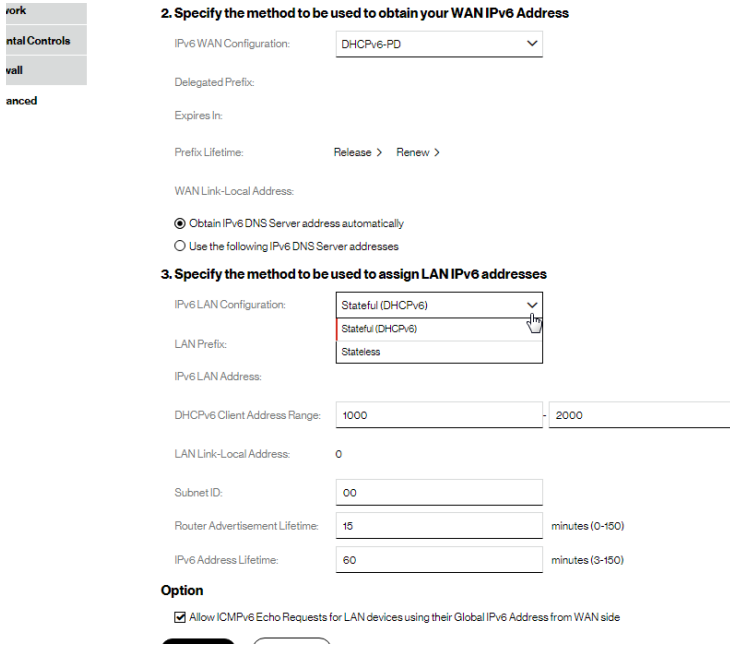
1. To configure IPv6 WAN Stateful (DHCPv6) mode, select the **DHCPv6-PD** option on the **IPv6 Configuration Control** page as shown below:



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** to have changes take effect.

DHCPv6 WAN with LAN IPv6 Stateful (DHCPv6) Settings

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

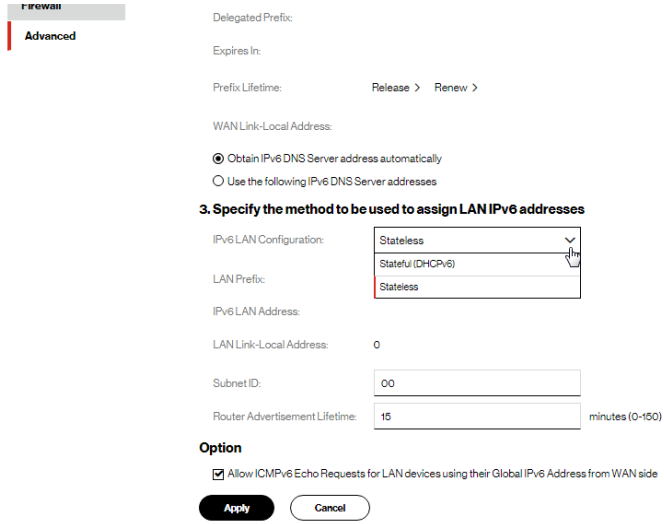


 |

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

DHCPv6 WAN with LAN IPv6 Stateless Settings

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



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

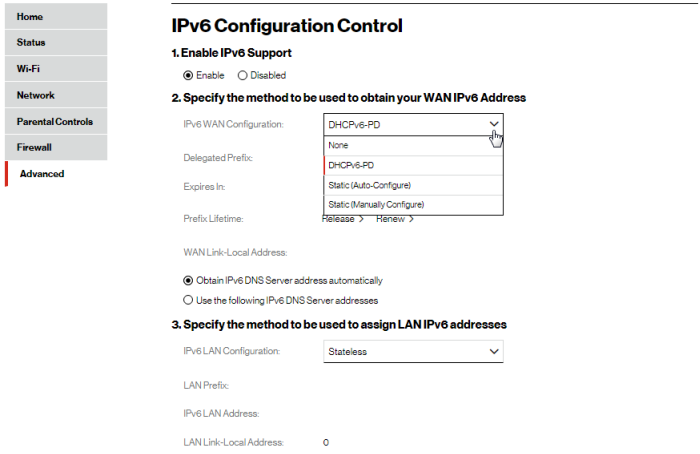
 |

- **Option: Allow ICMPv6 Echo Request for LAN devices using their Global IPv6 Address from WAN side** - requesting an IPv6 address from any available DHCPv6 servers available on the ISP

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

LAN IPv6 Configuration without An IPv6 WAN Connection

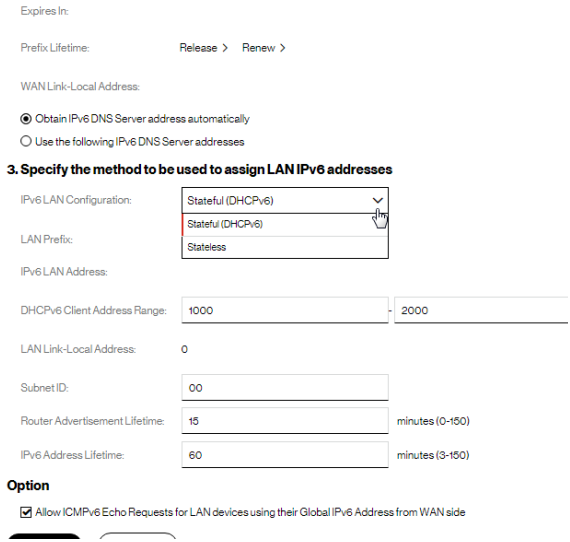
1. To configure IPv6 to use either the IPv6 LAN Stateful or Stateless mode without using an IPv6 Internet WAN connection, select the **None** option on the **IPv6 Configuration Control** page.



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

LAN IPv6 Stateful (DHCPv6) with No WAN Settings

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



2. Specify the **Stateful (DHCPv6)** settings to be used to assign LAN IPv6 addresses by entering the following details:
   - **IPv6 LAN Configuration** (select Stateful from the dropdown list)
   - **LAN Prefix** (automatically populated)
   - **IPv6 LAN Address** (automatically populated)
   - **DHCPv6 Client Address Range** (start and end)

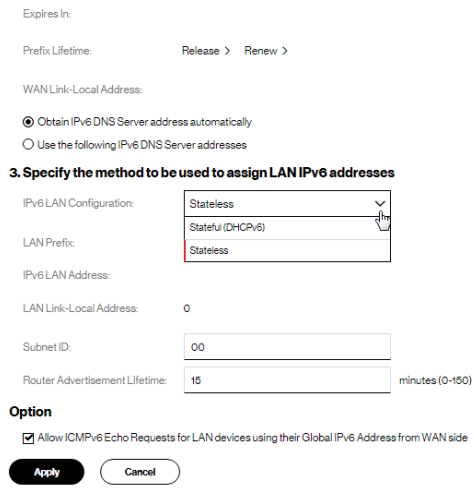
 |

- **LAN Link Local Address** (automatically populated)
- **Subnet ID** - set the site topology for your internal site
- **Router Advertisement Lifetime** (minutes between 0-150)
- **IPv6 Address Lifetime** (minutes between 3-150)
- **Option: Allow ICMPv6 Echo Request for LAN devices using their Global IPv6 Address from WAN side** - requesting an IPv6 address from any available DHCPv6 servers available on the ISP

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

LAN IPv6 Stateless with No WAN Settings

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



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

 |

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

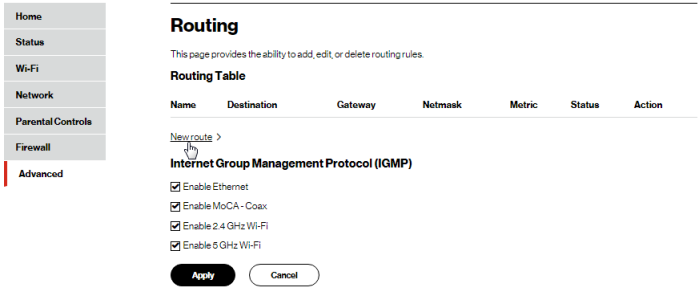
8.2e/ ROUTING SETTINGS

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

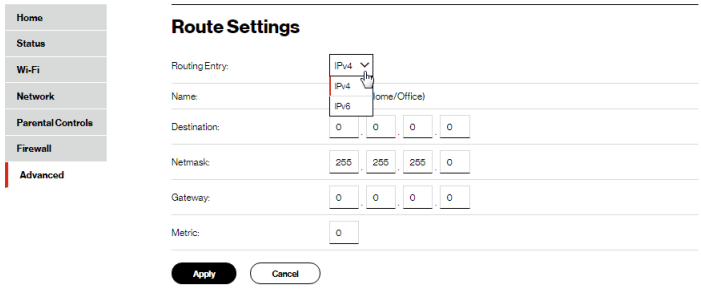
Routing Table

To view the rules:

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



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



3. Specify the following parameters:
   - **Name** – select the network 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 Fios Router.
   - **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** to save changes.

Internet Group Management Protocol (IGMP)

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

 |

To enable this function:

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

8.2f/ 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.

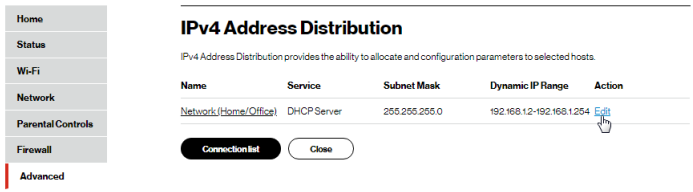
If the host wishes to terminate a lease before its expiration, it sends a release message to the DHCP server. This makes the IP address available for use by other hosts.

The DHCP server performs the following functions:

- Displays a list of all DHCP host devices connected to your Fios Router
- 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:

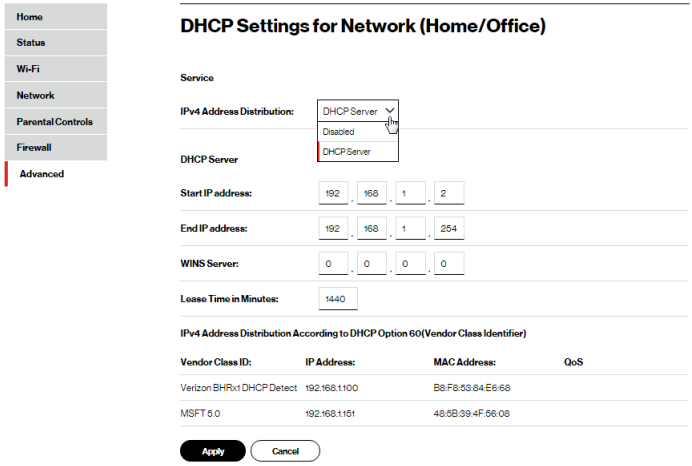
1. Select **IPv4 Address Distribution** in the **Network Settings** section.



 |

NETWORK SETTINGS

2. You can edit the DHCP server settings for a device. On the **IPv4 Address Distribution** page, click the **Edit** icon in the **Action** column. 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.



5. To configure the DHCP server, complete the following fields:
   - **Start IP Address** – enter the first IP address that your Fios Router will automatically begin assigning IP addresses from. Since your Fios Router's default IP address is 192.168.1.1, the default start IP address should be 192.162.1.2.

- **End IP Address** – enter the last IP address that your Fios Router 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 Indentifier)

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

 |

DHCP Connection List

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

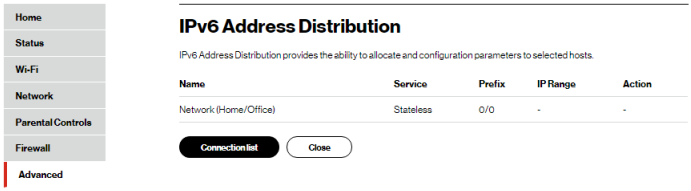
To view a list of computers:

1. On the **IPv4 Address Distribution** page, click **Connection List**.
2. To define a new **Static** Connection with a fixed IP address, click **Add Static Connection**.
3. Enter the host name.
4. Enter the fixed IP address to be assigned.
5. Enter the MAC address of the network interface of the computer used with this DHCP static connection.
6. Click **Apply** to save changes.

8.2g/ IPv6 ADDRESS DISTRIBUTION

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

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



2. You can edit the DHCP server settings for a device. On the **IPv6 Address Distribution** page, click the **Edit** icon in the **Action** column. The DHCP Settings page opens with the device information displayed.
3. To configure the DHCP server complete the following fields:
   - **Start IPv6 Address** – the starting IPv6 address in the consecutive list of addresses that makes up this LAN pool for the DHCPv6 server.
   - **End IPv6 Address** – the ending IPv6 address in the consecutive list of addresses that makes up this LAN pool for the DHCPv6 server.
   - **Lease Time in Minutes** – assigns the amount of time in minutes that each device is assigned an IP address by the DHCP server when it connects to the network.

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

DHCP Connection List

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

 |

To view a list of computers:

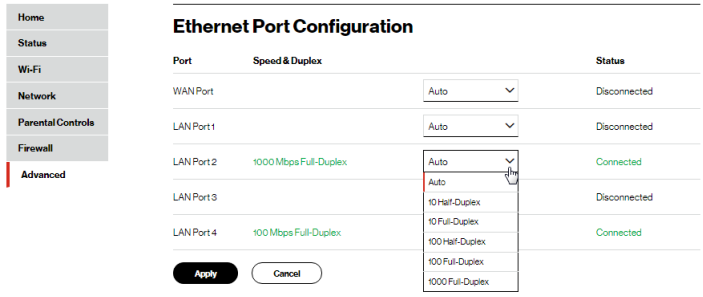
1. On the **IPv6 Address Distribution** page, click **Connection List**.
2. To define a new **Static** Connection with a fixed IP address, click **Add Static Connection**.
3. Enter the host name.
4. Enter the fixed IP address to be assigned.
5. Enter the MAC address of the network interface of the computer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

8.2h/ PORT CONFIGURATION

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

To configure the ports:

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



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

8.3/ DATE AND TIME

You can configure the following settings:

- Date and Time Settings – sets the time zone and enables automatic time updates.
- Scheduler Rules Settings – limits the activation of firewall rules to specific time periods.

8.3a/ DATE AND TIME SETTINGS

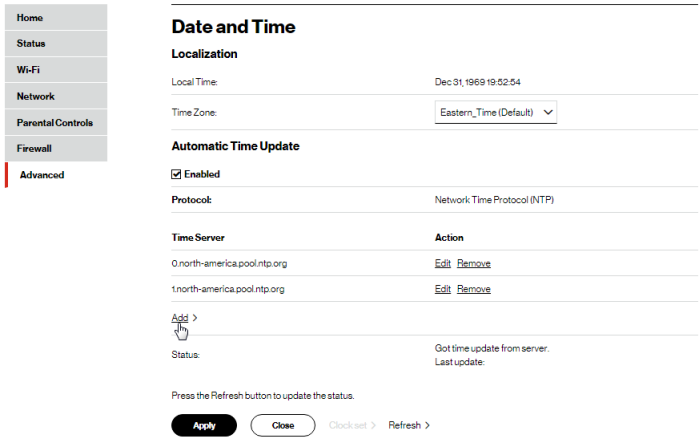
You can set the time zone and enable automatic time updates.

To configure the settings:

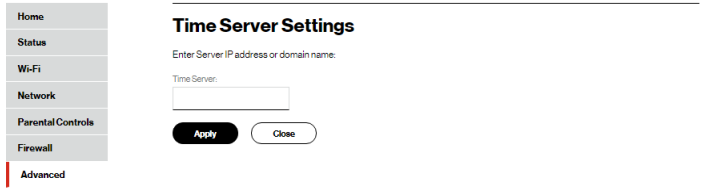
1. Select **Date and Time** in the **Date and Time** section.

 |

DATE AND TIME



2. Select the local time zone. Your Fios Router automatically detects daylight saving times for selected time zone.
3. In the **Automatic Time Update** section, select the **Enabled** checkbox to perform an automatic time update.
4. Define the time server addresses by clicking **Add**. The **Time Server Settings** page displays.



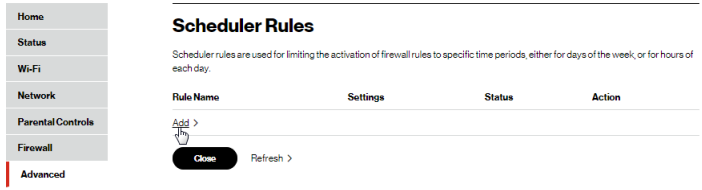
5. Enter the IP address or domain name of the time server, then click **Apply** to save changes.

8.3b/ 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:

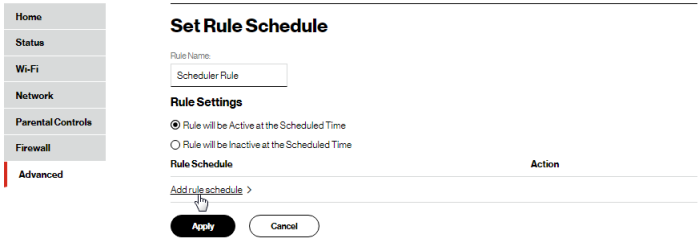
1. Verify that the date and time of your Fios Router is correct.
2. Select **Scheduler Rules** in the **Date and Time** section.



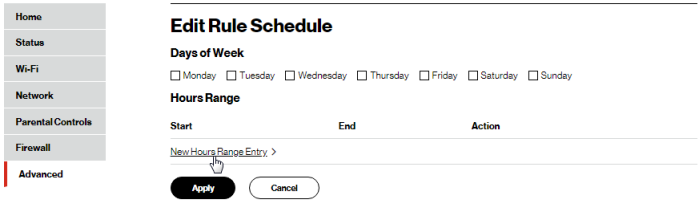
3. Click **Add**. The **Set Rule Schedule** page displays.

 |

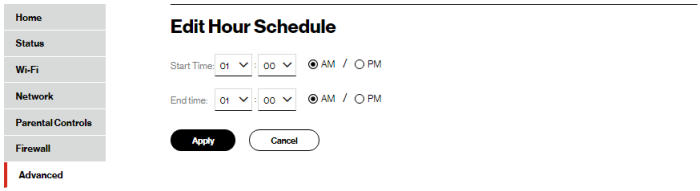
DATE AND TIME



4. Enter the name of the rule.
5. In the **Rule Settings** section, specify if the rule is active at the scheduled time or inactive at the scheduled time.
6. Click the **Add rule schedule**. The **Edit Rule Schedule** page displays.



7. Select the active or inactive days of the week.
8. To define a new active or inactive hourly range, click **New Hours Range Entry**.



9. Enter the start and end time, then click **Apply** to save changes.
10. Click **Apply** again to save the rule schedule.

8.4/ DNS SETTINGS

You can view and manage the DNS server host name and IP address as well as add a new computer. The DNS server does not require configuration.

8.4a/ DYNAMIC DNS

Typically, when connecting to the internet, your router 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.

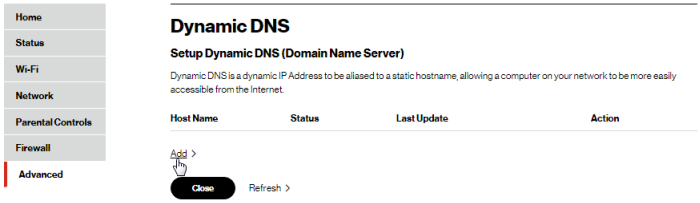
When using Dynamic DNS, each time the public IP address changes, the DNS database is automatically updated with the new IP address. In this way, even though the IP address changes often, the domain name remains constant and accessible.

To set up dynamic DNS:

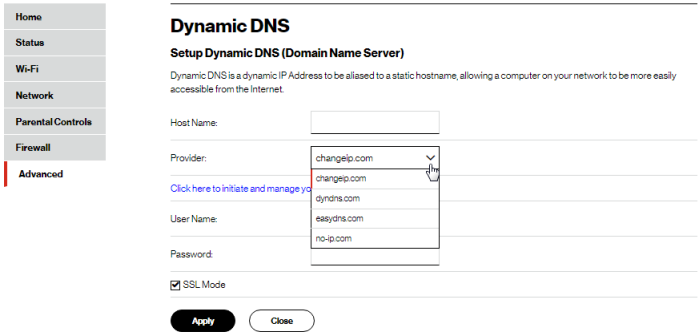
1. Select **Dynamic DNS** in the **DNS** section.

 |

DNS SETTINGS



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.

To edit the host name or IP address:

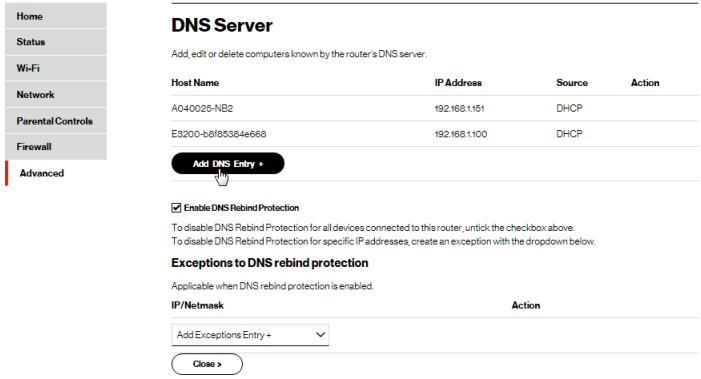
1. In the **Action** column, click the **Edit** icon. The DNS Entry page displays.
2. Edit the settings.
3. Click **Apply** to save the changes.

8.4b/ 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. Select **DNS Server** in the **DNS** section.



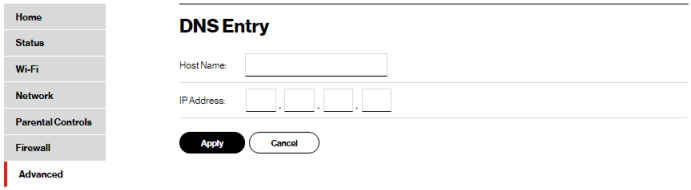
 |

DNS SETTINGS

2. To disable DNS rebind protection, untick the checkbox of **Stop DNS Rebind.**

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

3. To view and add computers stored in the **DNS** table, click **Add DNS Entry**. The **DNS Entry** page displays.



4. In the **Host Name** field, enter the name of the computer, then enter the **IP address** and click **Apply** to save changes.
5. Then the **DNS Server** page displays.
6. To edit the host name or IP address, click the **Edit** icon in the **Action** column. The **DNS Entry** page displays. Edit the host name and/or IP address, then click **Apply** to save changes.
7. To remove a host from the DNS table, click the **Delete** icon in the **Action** column.

8.5/ MONITORING

You can view the details and status of:

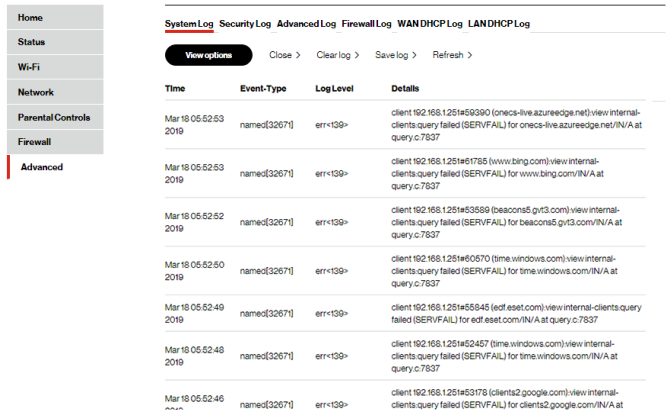
- System Logging
- Full Status/System wide Monitoring of Connections/Traffic Monitoring
- Bandwidth Monitoring

8.5a/ SYSTEM LOGGING

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

To view the system log:

1. In the **Monitoring** section, click the **System Logging** link.



 |

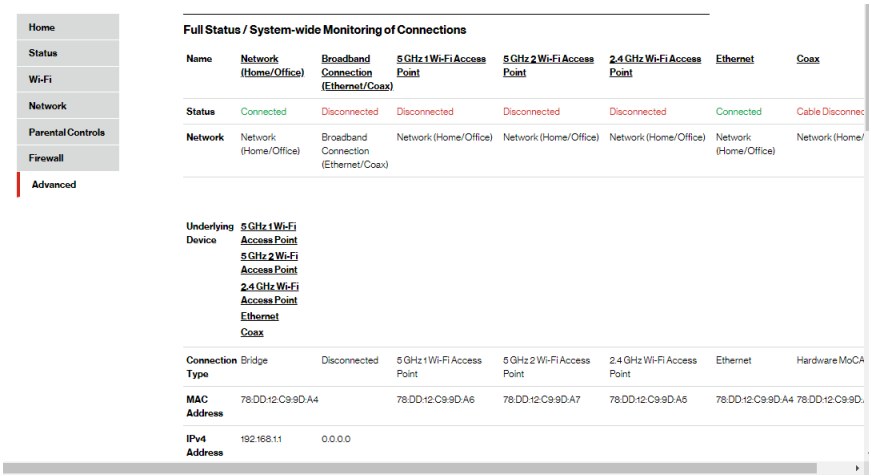
2. To view a specific type of log event such as Security Log, WAN DHCP Log, etc., click the appropriate link in the menu on the top.
3. To update the data, click **Refresh**.

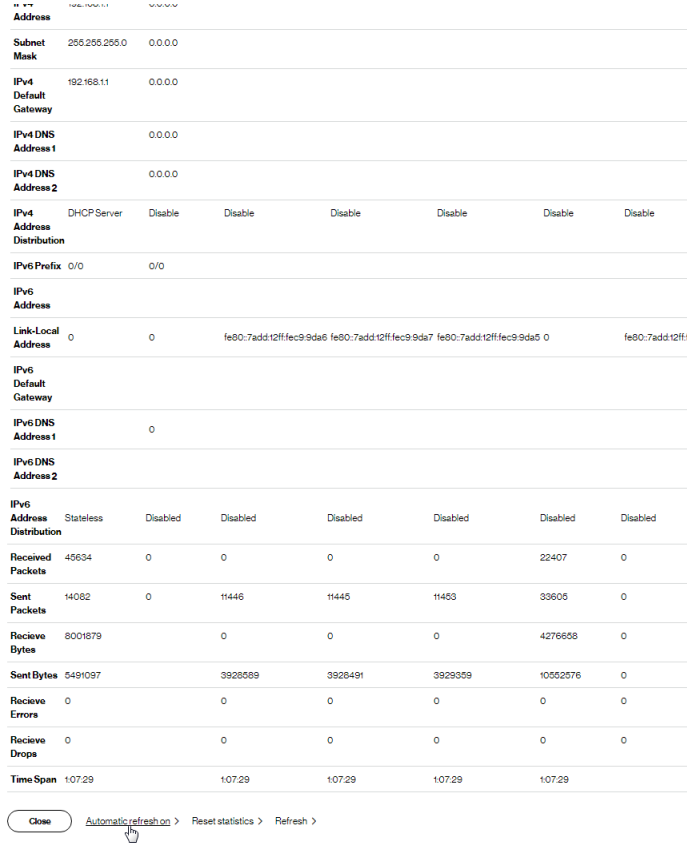
8.5b/ FULL STATUS/SYSTEM WIDE MONITORING OF CONNECTIONS

You can view a summary of the monitored data collected for your Fios Router.

To view your Fios Router's full system status and traffic monitoring data:

1. In the **Monitoring** section, click **Full Status/System wide Monitoring of Connections/Traffic Monitoring**.





Address							
Subnet Mask	255.255.255.0	0.0.0.0					
IPv4 Default Gateway	192.168.1.1	0.0.0.0					
IPv4 DNS Address 1		0.0.0.0					
IPv4 DNS Address 2		0.0.0.0					
IPv4 Address Distribution	DHCP Server	Disable	Disable	Disable	Disable	Disable	Disable
IPv6 Prefix	0/0	0/0					
IPv6 Address							
Link-Local Address	0	0	fe80::7add:12ff:fec9:9da6	fe80::7add:12ff:fec9:9da7	fe80::7add:12ff:fec9:9da5	0	fe80::7add:12ff:f
IPv6 Default Gateway							
IPv6 DNS Address 1		0					
IPv6 DNS Address 2							
IPv6 Address Distribution	Stateless	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Received Packets	45634	0	0	0	0	22407	0
Sent Packets	14082	0	11446	11445	11463	33606	0
Recieve Bytes	8001879		0	0	0	4276658	0
Sent Bytes	5491097		3928589	3928491	3929359	10552576	0
Recieve Errors	0		0	0	0	0	0
Recieve Drops	0		0	0	0	0	0
Time Span	1:07:29		1:07:29	1:07:29	1:07:29	1:07:29	

Close Automatic refresh on > Reset statistics > Refresh >

2. To modify the connection properties, click the individual connection links.
3. To refresh the page, click **Refresh**.
4. To continuously refresh the page, click **Automatic refresh on**.

 |

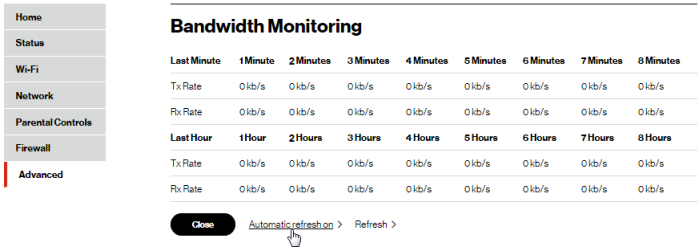
SYSTEM SETTINGS

8.5c/ BANDWIDTH MONITORING

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

To view the bandwidth:

1. In the **Monitoring** section, select **Bandwidth Monitoring**.



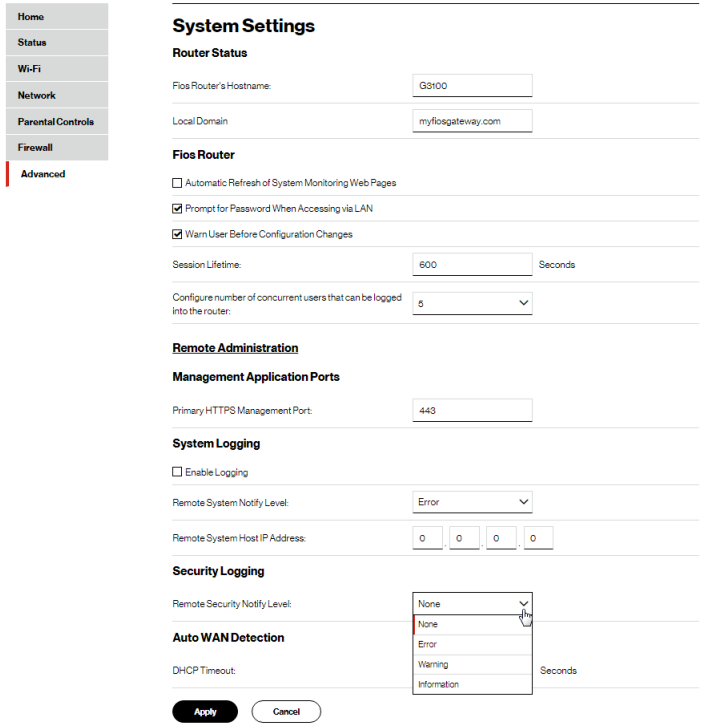
2. To refresh the page, click **Refresh**.
3. To continuously refresh the page, click **Automatic refresh on**.

8.6/ SYSTEM SETTINGS

You can configure various system and management parameters.

To configure system settings:

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



2. In the **Router Status** section, configure the following:
   - **Fios Router's Hostname** – enter the host name or URL address of your Fios Router. Both names are the same.
   - **Local Domain** – view the local domain of the network.
3. In the **Fios 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 Fios Router 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.

4. In the **Session Lifetime** field, specify the length of time required before re-entering a user name and password after your Fios Router has been inactive.
5. In the **Configure number of concurrent users that can be logged into the router** field, select the number of users that can access your Fios Router at the same time.
6. Select **Remote Administration** to configure the remote administration to your Fios Router.
7. In the **Management Application Ports** section, change the primary HTTP management and SSH ports.

   Refer to 8.1h Remote Administration for using this feature.
8. In the **System Logging** section, configure the following system log options:
   - **Enable Logging** – activates system logging.
   - **Remote System Notify Level** – specify the type of information, such as none, error, warning, and information, received for remote system logging.

- **Remote System Host IP Address** – enter the IP address of system log server for Security Logging messages.

9. In the **Security Logging** section, configure the following security logging options:
   - Low Capacity Notification Enabled – activates low capacity notification. This works in conjunction with the Allowed Capacity before Email Notification and System Log Buffer Size.
   - Allowed Capacity before Email Notification – specify the capacity before an email notification is sent.
   - System Log Buffer Size – specify the size of the system log buffer.
10. In the **Auto WAN Detection** section, specify the DHCP timeout.
11. Click **Apply** to save changes.

 |

09/

TROUBLE SHOOTING

This chapter lists solutions for issues that may be encountered while using your Fios Router as well as frequently asked questions.

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

 |

TROUBLESHOOTING TIPS

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

9.0/ TROUBLESHOOTING TIPS

9.0a/ IF YOU ARE UNABLE TO CONNECT TO THE INTERNET:

- The first thing to check is whether your Fios Router is powered on and is connected to the internet. Check the Router Status LED on the front of the Fios Router. Be sure to refer to the "1.3a/ FRONT PANEL" on page 10 to determine status of the Fios Router. Check the WAN cable (Ethernet or coaxial) connecting your Fios Router to the internet to make sure it is properly connected on both ends.
- If the prior tips do not resolve your connection issue, try restarting (rebooting) the router portion of the Fios Router by manually pressing the 'red' reset power button on the rear panel of the Fios Router for 2-4 seconds (the Router Status LED should go off) to begin rebooting your Fios Router. Your Fios Router will begin rebooting and will return to service in 3 - 5 minutes depending on your network connection. Check Router Status LED and if it is solid white, try again to access the internet.

- If rebooting your router does not resolve your connection issue, try power cycling the Fios Router by unplugging the power cable from the adapter or the wall and wait 2 minutes. During the 2 min. wait period, also power cycle the network device (e.g. the computer, tablet, etc.) and then plug the power cable back into the Fios Router. After 3-5 minutes, recheck the Router Status LED and try again to access the internet.

9.0b/ IF YOU ARE UNABLE TO CONNECT TO YOUR FIOS ROUTER USING WI-FI:

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

 |

TROUBLESHOOTING TIPS

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

9.0c/ ACCESSING YOUR FIOS ROUTER IF YOU ARE LOCKED OUT

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

The common ways to lock access to your Fios Router are:

- Scheduler - If a schedule has been created that applies to the computer over the connection being used, your Fios Router 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 Fios Router is denied.

To gain access, restore the default settings to your Fios Router.

9.0d/ RESTORING YOUR FIOS ROUTER'S DEFAULT SETTINGS

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

For additional information regarding the Restore Defaults feature, refer to section 8.1/ Utilities/Save And Restore.

- Using the tip of a ballpoint pen or pencil, press and hold the Reset button on the back of your Fios Router for three seconds.
- Access the UI and navigate to the Advanced Settings page. Select the 8.1b Save and Restore option. After saving your configuration, if desired, click the Restore Factory Defaults radio button. For additional details, refer to the 8.1/ Utilities/Save And Restore section of this guide.

Note: If you reset or reboot your Fios Router, you may also need to disconnect your Fios Router's power supply for a few minutes (3 or more) and then reconnect the power cable. However, in order to provide full synchronization to the coaxial network, disconnecting and reconnecting the power may be required.

9.0e/ LAN CONNECTION FAILURE

To troubleshoot a LAN connection failure:

- Verify your Fios Router is properly installed, LAN connections are correct, and that the Fios Router and communicating network devices are all powered on.

 |

- Confirm that the computer and Fios Router 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 Fios Router.

- Verify the subnet mask address is set to 255.255.255.0.

9.0f/ TIMEOUT ERROR OCCURS WHEN ENTERING THE URL OR IP ADDRESS

Verify the following:

- All computers are working properly.
- IP settings are correct.
- Fios Router is on and connected properly.
- Fios Router 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 Fios Router and restart the Fios Router, wait 1-2 mins. and insert the Ethernet cable again.
- Under limited circumstances you may use a port forwarding configuration on the router, based on the application you are using (refer to the 7.2/ Port Forwarding section or Verizon's support online help for more details).

9.0g/ FRONT UNIFIED BUTTON

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

Condition Status	LED Color	Fios Router
Normal	WHITE	Normal operation (solid) Router is booting. (fast blink)
	BLUE	Pairing mode (slow blink) Pairing successful (solid)
	GREEN	Wi-Fi has been turned off. (solid)
Issue(s)	YELLOW	No internet connection (solid)
	RED	Hardware/System failure detected (solid) Overheating (fast blink) Pairing Failure (slow blink)
Power	OFF	Power off

 |

TROUBLESHOOTING TIPS

9.0h/ REAR LIGHTED INDICATORS

Flash Speed

- Slow flash – Two times per second
- Fast flash – Four times per second

WAN Ethernet

- Unlit – Indicates no Ethernet link
- Solid green – Indicates a network link
- Fast flash green – Indicates network activity. The traffic can be in either direction.

LAN Ethernet – Upper LED

- Unlit – Indicates no 1 Gbps link
- Solid green – Indicates 1 Gbps link
- Fast flash green – Indicates LAN activity. The traffic can be in either direction.

LAN Ethernet – Lower LED

- Unlit – Indicates no 10/100/1000 Mbps link
- Solid green – Indicates 10/100/1000 Mbps link

LAN Coax

- Unlit – Indicates no MoCA network connection to the device
- Solid green – Indicates network link

WAN Coax

- Unlit – Indicates no link to the upstream MoCA device
- Solid green – Indicates network link
- Fast flash green – Indicates LAN activity. The traffic can be in either direction

9.1/ FREQUENTLY ASKED QUESTIONS

9.1a/ I'VE RUN OUT OF ETHERNET PORTS ON MY FIOS ROUTER. HOW DO I ADD MORE COMPUTERS OR DEVICES?

Plugging in an Ethernet hub or switch expands the number of ports on your Fios Router.

- Run a straight-through Ethernet cable from the Uplink port of the new hub to the Fios Router.

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

- Remove an existing device from the yellow Ethernet port on your Fios Router and use that port.

 |

FREQUENTLY ASKED QUESTIONS

9.1b/ HOW DO I CHANGE THE PASSWORD ON MY FIOS ROUTER UI?

To change the password:

1. On the main screen, select **Advanced**, then select **Users** in the **Utilities** section.
2. Click the **Edit** in the **Action** column. The **User Settings** page displays.
3. Edit the user name and set a new password.

9.1c/ IS THE WI-FI OPTION ON BY DEFAULT ON MY FIOS ROUTER?

Yes, your Fios Router's Wi-Fi option is activated out of the box.

9.1d/ 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 panel of your Fios Router.

9.1e/ ARE MY FIOS ROUTER'S ETHERNET PORTS AUTO-SENSING?

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

9.1f/ CAN I USE AN OLDER WI-FI DEVICE TO CONNECT TO MY FIOS ROUTER?

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

9.1g/ CAN MY WI-FI SIGNAL PASS THROUGH FLOORS, WALLS, AND GLASS?

The physical environment surrounding your Fios Router 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.

9.1h/ HOW DO I LOCATE THE IP ADDRESS THAT MY COMPUTER IS USING?

In Windows 7 or Windows 10, click the Windows button and select Control Panel, then click View Network Status and Tasks. In the next window, click Local Area Connection. In the Local Area Network Connection Status window, click Details.

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

 |

FREQUENTLY ASKED QUESTIONS

9.1i/ I USED DHCP TO CONFIGURE MY NETWORK. DO I NEED TO RESTART MY COMPUTER TO REFRESH MY IP ADDRESS?

No. In Windows 7, Windows 10 and OSX, unplug the Ethernet cable or Wi-Fi card, then plug it back in.

9.1j/ I CANNOT ACCESS MY FIOS ROUTER UI. WHAT SHOULD I DO?

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

9.1k/ I HAVE A FTP OR WEB SERVER ON MY NETWORK. HOW CAN I MAKE IT AVAILABLE TO USERS ON THE INTERNET?

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

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

9.1l/ HOW MANY COMPUTERS CAN BE CONNECTED THROUGH MY FIOS ROUTER?

Your Fios Router is capable of 254 connections, but we recommend having no more than 45 connections. As the number of connections increase, the available speed for each computer decreases.

 |

10 /

SPECIFICATIONS

The specifications for your Fios Router are as follows.

This includes standards, cabling types and environmental parameters.

 |

GENERAL SPECIFICATIONS

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

10.0/ GENERAL SPECIFICATIONS

Model Number: G3100

Standards:	IEEE 802.3x, 802.3u
	IEEE 802.11a/b/g/n/ac/ax
IP:	IP versions 4 and 6
MoCA WAN:	975 - 1025 MHz 175 Mbps
MoCA LAN:	1125 – 1675 MHz 2500 Mbps
Speed:	Wired WAN Ethernet: 10/100/1000 Mbps auto-sensing
	Wired LAN Ethernet: 10/100/1000 Mbps auto-sensing
	Cabling Type: Ethernet 10BaseT: UTP/STP Category 3 or 5
	Ethernet 100BaseT: UTP/STP Category 5
	Ethernet 1000BaseT: UTP/STP Category 5e
Firewall:	ICSA certified

10.1/ LED INDICATORS

Front Panel:	Unified Button: Router Status LED
Rear Panel:	WAN Coax, LAN Coax, WAN Ethernet, and LAN Ethernet [4]

10.2/ ENVIRONMENTAL PARAMETERS

DIMENSIONS AND WEIGHT

Fios Router (unit only):

Size: 5.32” wide x 9.27” high x 5.94” deep

Weight: 2.50 lbs / 1.138 kg

Complete System (inc. packaging):

Size: 12.24” wide x 6.26” high x 7.09” deep

Weight: 4.00 lbs ~ 4.05 lbs / 1.81 kg ~ 1.83 kg

Power:	External, 12V, 3.5A
Screws (optional):	PH TP+N: 0.157” x 0.984” Anchor PE: 0.197” x 0.984”
Certifications:	FCC, UL 60950-1

 |

ENVIRONMENTAL PARAMETERS

Operating Temperature:	5° C to 40° C (41° F to 104° F)
Storage Temperature:	-5° C to 50° C (23° F to 122° F)
Operating Humidity:	5% to 85%
Storage Humidity:	5% to 93% (non-condensing)

11 /

NOTICES

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

 |

REGULATORY COMPLIANCE NOTICES

11.0/ REGULATORY COMPLIANCE NOTICES

11.0a/ Class B Equipment

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

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

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.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

RF Exposure:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 32 cm between the radiator & your body.

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

2.4GHz operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

This device is restricted for indoor use.

 |

REGULATORY COMPLIANCE NOTICES

11.0b/ 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.

11.0c/ Alerte de sécurité:

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

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

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

11.0d/ NEBS (Network Equipment Building System) Statement

An external SPD is intended to be used with G3100/E3200.

WARNING: The intra-building ports of the equipment or subassembly is suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port(s) of the equipment or subassembly MUST NOT be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 4 ports as described in GR-1089) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.

 |

REGULATORY COMPLIANCE NOTICES

Caution: The Fios Router must be installed inside the office. The Router is not designed for exterior installation.

11.0e/ GENERAL PUBLIC LICENSE

This product contains certain software that is covered by open source licensing requirements. Copies of the licenses and a downloadable copy of the source code for the open source software that is used in this product are available on the following website:

http://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.

You may also obtain a copy of the source code for the open source software used in this product for a period of three years after your receipt of the product by sending a check for $10, payable to VERIZON, to the address below:

Verizon
One Verizon Way
Basking Ridge, NJ 07920
Attn: Legal, Open Source Requests

Note: 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.