fios by verizon

Fios-G2100

USER GUIDE

Model Fios-G2100

CONTENTS

05/
CONFIGURING MY NETWORK SETTINGS

06/
USING NETWORK CONNECTIONS

07/
CONFIGURING SECURITY SETTINGS

08/
SETTING PARENTAL CONTROLS

CONTENTS

11/ TROUBLESHOOTING

12/ SPECIFICATIONS

13/ NOTICES

01/

INTRODUCTION

The Verizon Fios-G2100 lets you transmit and distribute digital entertainment and information to multiple devices in your home/office.

Your Fios-G2100 supports networking using fiber cable, Ethernet, or Wi-Fi, making it one of the most versatile and powerful routers available.

 |

PACKAGE CONTENTS, SYSTEM REQUIREMENTS AND FEATURES

1.0/ PACKAGE CONTENT

Your package contains:

- Fios-G2100
- Power adapter
- LAN Ethernet cable
- Phone Cable
- Quick Start 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 Fiber interfaces
  - LAN – 802.11 b/g/n/ac and Gigabit Ethernet interfaces
  - ONT – Network connectivity to service provider

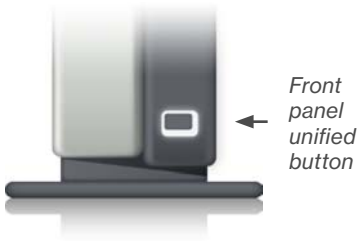
- Integrated wired networking with 4-port Ethernet switch and Fiber
  - Ethernet supports speeds up to 1000 Mbps
  - Fiber enabled to support speeds up to 2 Gbps - downlink and 1.25 Gbps - uplink
- Integrated wireless networking with 802.11b/g/n/ac access point featuring:
  - Enabled 802.11b capable speeds (based on device)
  - Enabled 802.11g capable speeds (based on device)
  - Enabled 802.11n capable speeds (based on device)
  - Enabled 802.11ac capable speeds (based on device)
- 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
  - Event logging

 |

  - MAC address filtering
  - Static NAT
  - Port forwarding
  - Port triggering
  - Access control
  - Advanced wireless protection featuring WPA2/WPA Mixed Mode and MAC address filtering

- Options, including:
  - DHCP server
  - WAN interface auto-detection
  - Dynamic DNS
  - DNS server
  - LAN IP and WAN IP address selection
  - MAC address cloning
  - IPv6 support
  - 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
  - Remote management and secured remote management using HTTPS
  - 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 handset paging/paring mode.

Router Lights

Condition Status	LED Color	BHR5
Normal	WHITE	Normal Operation (solid) Router is booting (fast blink) ONT is booting (slow blink)
	BLUE	Pairing Mode (slow blink) Paging Mode (fast blink)
	GREY	Wi-Fi has been turned off
Issue(s)	YELLOW	No internet Connection (slow blink)
	RED	Hardware/System Failure detected (solid) Overheating (fast blink)
Mode Changed	GREEN	Device is set to Router only mode (ONT/DECT disabled)
	OFF	Device is set to ONT only mode (Router off) or Fiber cable is not connected, dirty or possibly damaged.

 |

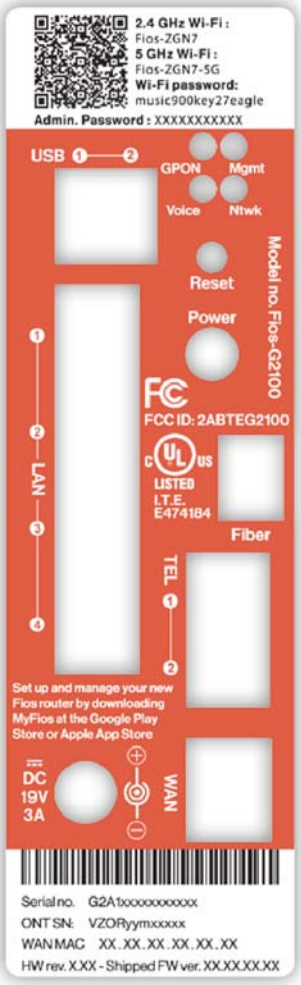
GETTING TO KNOW YOUR FIOS ROUTER

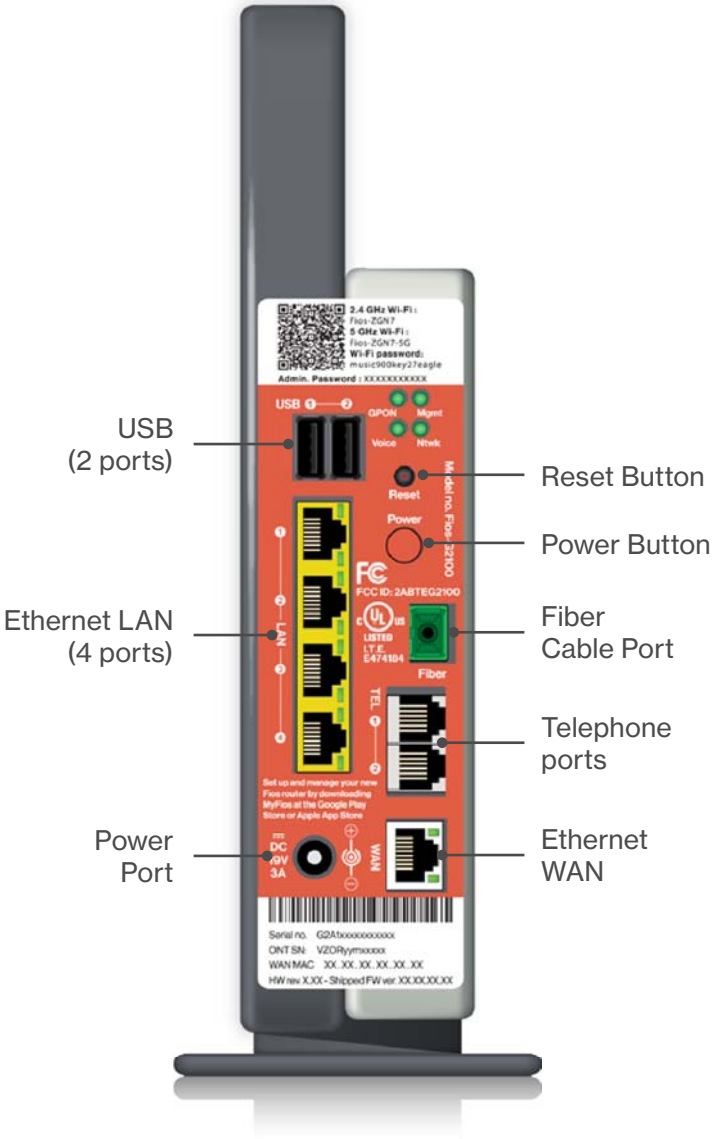
Refer to the ‘Connecting a Wi-Fi device using WPS’ and ‘Voice’ sections for more details. In addition, the Unified Button also provides a quick view of the operational state of the Fios Router using various colors as indicated in the chart above. Please refer to section 11.0h for details on the rear LEDs.

1.3b/ REAR PANEL

The rear panel of your Fios Router has a label that contains important information about your device, including the default settings for the Fios Router’s wireless network name (ESSID), wireless password (WPA2 key), local URL for accessing the Fios Router’s administrative pages, and Fios Router 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 of your Fios Router has 10 ports; Fiber and Ethernet WAN, Ethernet LAN [4], Telephone [2] and USB [2]. The rear panel also includes a DC power jack and a reset button.





GETTING TO KNOW YOUR FIOS ROUTER

- **USB** - provides up to 500 mA at 5 VDC for attached devices. For example, you could charge a cell phone. In the future, with a firmware upgrade, the USB host functionality may be available for other devices, such as external storage and cameras. Firmware updates are performed automatically by Verizon.
- **Reset Button**
  - Factory Reset Router - Press and Hold 3-10 seconds
  - Factory Reset ONT - Press and Hold 10-20 seconds
  - Factory Reset both ONT and Router - Press and Hold for greater than 20 seconds
- **Power Button** - Press the power button for 2-4 seconds to toggle the router functionality On/off. Press and hold the power button for more than 30 seconds to power off the entire unit.
- **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.
- **Ethernet WAN** - connects your Fios Router to the Internet using an Ethernet cable.
- **Fiber WAN** - connects your Fios Router to the Service Provider network using the fiber cable provided.

  Laser Warning: An invisible laser light may be present at the fiber optic cable when the cable is removed from the connector. Avoid direct exposure to the laser beam.

Warning: The WAN Fiber Port is intended for connection to Verizon Fios only. It must not be connected to any cables/wires not designated for Verizon Fios.

- **Telephone Ports** - connects a traditional phone to your Fios Router.
- **Power** - connects your Fios Router to an electrical wall outlet using the supplied power adapter.

  Warning: The included power adapter is for home use only, supporting voltages from 100-240Vac. Do not use in environments with greater than 240Vac.

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/fiosaccessories*.

If you are replacing an existing Verizon wall mounted router, you do not need to remove the mounting screws from the wall. The existing mounting screws will fit the new bracket.

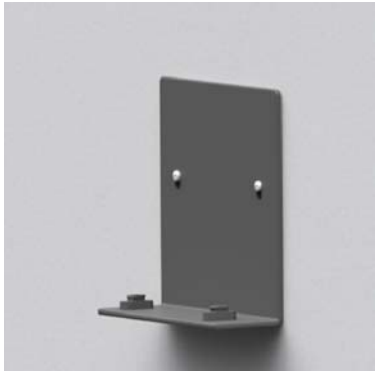
To mount your Fios Router to a wall:

1. Remove the foot by sliding the foot towards the back of the Fios Router and pull the foot from the holes. You may need to wiggle the foot slightly.

 |

GETTING TO KNOW YOUR FIOS ROUTER

2. You may use the wall mount bracket as a template for positioning the Fios Router.
3. Mark the mounting holes, then remove the wall mount bracket from the wall.
4. Drill holes for the screw anchors.



5. Insert the screw anchors in the holes in the wall, then insert the screws into the screw anchors and tighten the screws. Leave screws extended about 0.2 inches from the wall.
6. Verify the screws are positioned correctly by placing the wall bracket on the screws. Remove the wall bracket from the wall.

7. Place the Fios Router on the wall bracket and slide the Fios Router forward until it locks in place.
8. Slide the wall mount bracket with the attached Fios Router on the screws, then slide the bracket down until it locks in place.

02/

CONNECTING YOUR FIOS ROUTER

 |

SETTING UP YOUR FIOS ROUTER

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

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

2.0/ SETTING UP YOUR FIOS ROUTER

There are three basic steps to setting up your Fios Router:

Step 1: Connect your Fios Router to the Internet

Step 2: Connect your network device to your Fios Router

Step 3: Configure your Fios Router

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

2.0a/ STEP 1 - CONNECT YOUR FIOS ROUTER

1. Remove your Fios Router, cables, and power adapter from the box.
2. Locate your Fios WAN Port. This would be the wall jack installed previously by Verizon. Note the type of jack may be either Ethernet or fiber.
3. If connecting the WAN using Fiber, use the green fiber cable and plug one end into the green fiber WAN port on the back of your Fios Router. Plug the other end of the cable into the fiber wall jack.
4. Plug the power cord into the power port on the back of your Fios Router and then into a power outlet.

 |

SETTING UP YOUR FIOS ROUTER

Warning: An invisible laser light may be present at the fiber optic cable when the cable is removed from the connector. Avoid direct exposure to the laser beam.

Important: Before proceeding to section 2.0b, please check the status of the rear LEDs (refer to section 11.0h). Please wait until the Unified Button light on the front of the Fios Router stops flashing and is solid white. If the light turns red, check the steps in the Troubleshooting section of this user guide.

2.0b/ STEP 2 - CONNECT THE DEVICE TO YOUR FIOS ROUTER

If connecting a device using Ethernet (preferred for initial setup):

- Plug one end of the Ethernet cable into one of the four yellow Ethernet ports in the back of your Fios Router. Alternatively, you can use your own Ethernet cable of any color to connect from the yellow Ethernet ports on the back of your Fios Router to your device with an Ethernet connector.
- Plug the other end of the yellow Ethernet cable into the Ethernet port of your network device.

If connecting a wireless device:

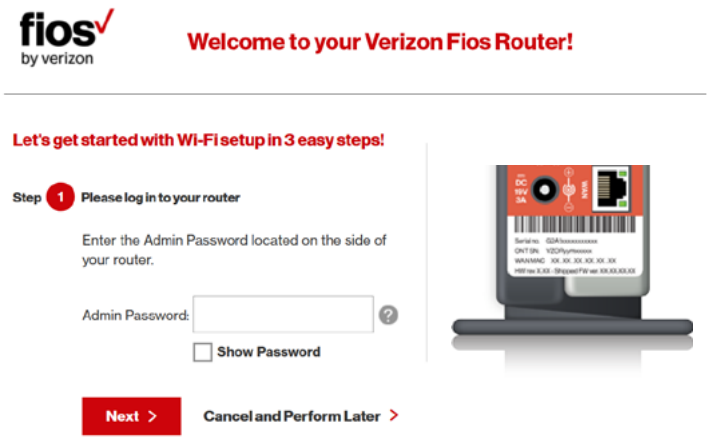
- Access the Wi-Fi setting on your wireless device, then select your new Fios Router using the wireless network name (ESSID) shown on the sticker located on the rear of your Fios Router.
- Enter the wireless password (WPA2 key) also shown on the sticker.

2.0c/ STEP 3 - 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: **myfiosgateway.com**, then press the **Enter** key on your keyboard.

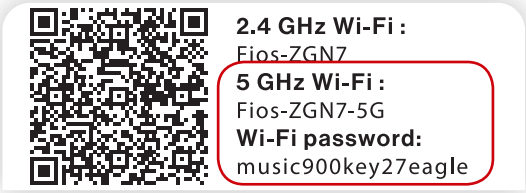
   Alternately, you can enter: **https://192.168.1.1**

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

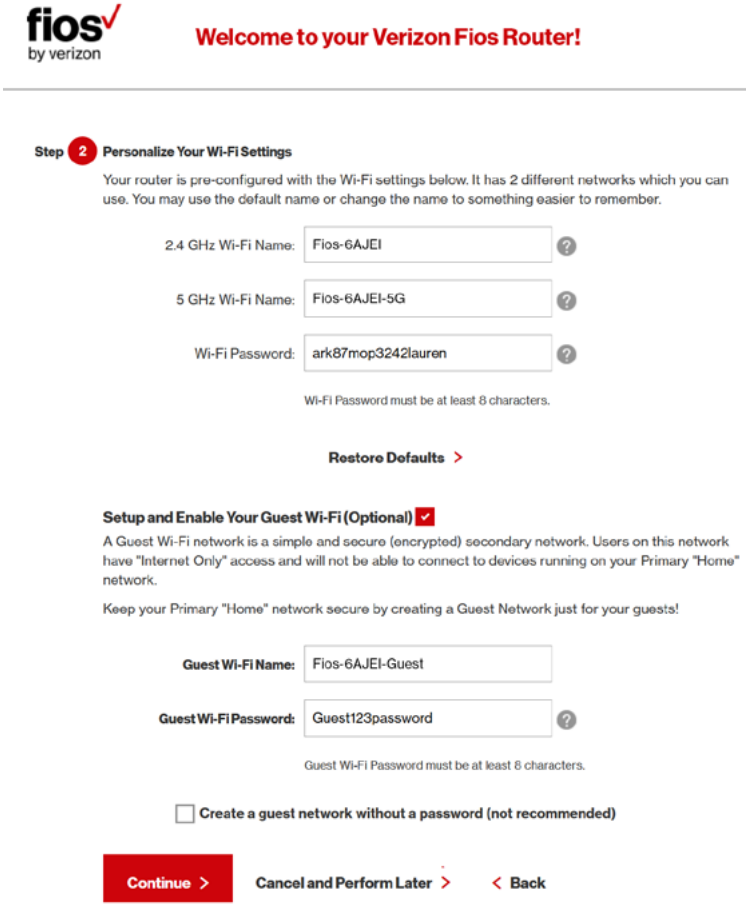


SETTING UP YOUR FIOS ROUTER

3. In the **Admin Password** field, enter the password that is printed next to the Administrator Password on the label on the rear of your Fios Router.



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

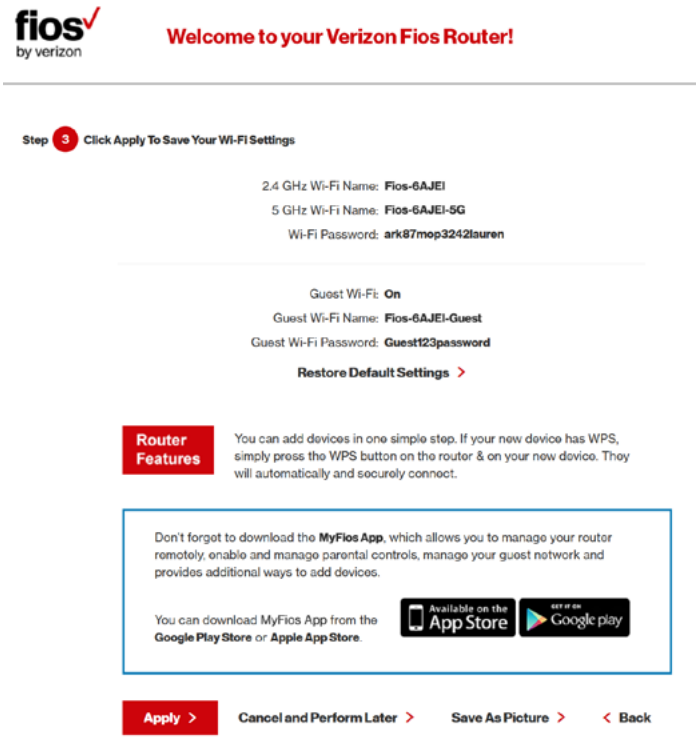


For your protection, your Fios Router is pre-set at the factory to use WPA2 (Wi-Fi Protected Access) encryption for your wireless network. This is the best setting for most users and provides maximum security.

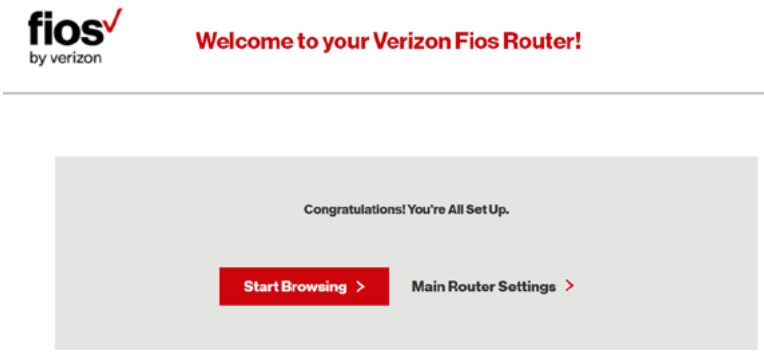
SETTING UP YOUR FIOS ROUTER AND COMPUTER NETWORK CONFIGURATION

5. Click **Continue**. The 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/ COMPUTER NETWORK CONFIGURATION

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

 |

COMPUTER NETWORK CONFIGURATION

2.1a/ 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 step 1 to 7. However for step 3, select **Internet Protocol Version 6 (TCP/IPv6)** in the Properties option (refer to IPv6 section for Fios Router 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.

2.1b/ CONNECTING OTHER COMPUTERS & NETWORK DEVICES

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

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 wireless network connection. Instead of manually entering passwords or multiple keys on each wireless client, such as a laptop, printer, or external hard drive, your Fios Router creates a secure wireless network.

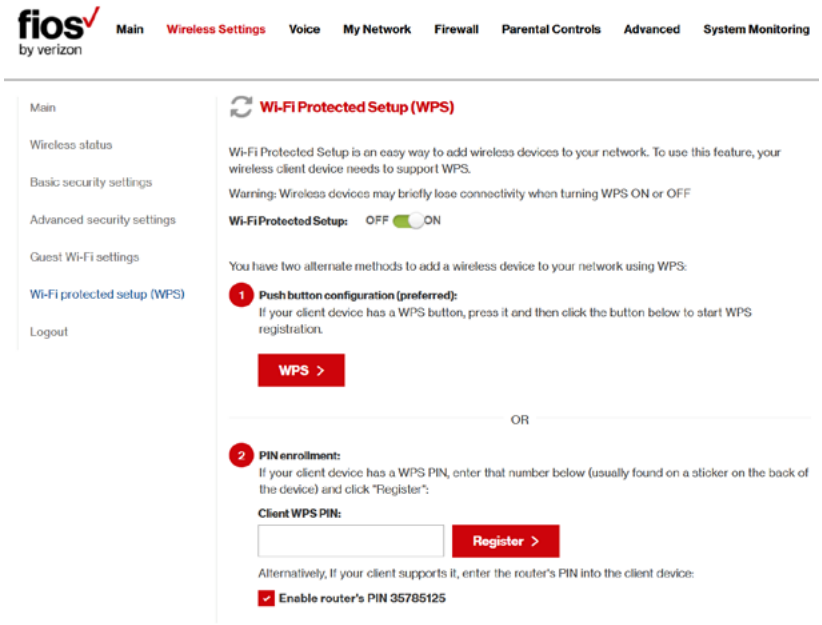
In most cases, this only requires the pressing of two buttons – one on your Fios Router and one on the wireless client. This could be either a built-in button or one on a compatible wireless adapter/card, or a virtual button in software. Once completed, this allows wireless clients to join your wireless 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 15 seconds or use the GUI and press the on-screen button.

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

To access WPS using the user interface:

1. From the Main menu, select **Wireless 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 wireless client device has a WPS button, press the Unified Button on the front panel of your Fios Router for 2-5 seconds, then click the WPS button on your wireless 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 **B - PIN Enrollment** on the user interface.

Click **Register**.

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

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

   When the Unified Button on your Fios Router is pressed, the Unified Button light on the front of your Fios Router begins flashing blue. The flashing continues until WPS pairing to the client device completes successfully. At this time, the Wireless light turns solid white.

   If WPS fails to establish a connection to a wireless client device within two minutes, the Wireless light on your Fios 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.

CONNECTING A WI-FI DEVICE USING A PASSWORD

1. Verify each device that you are connecting wirelessly (using Wi-Fi) has a built-in wireless or external wireless adapter.

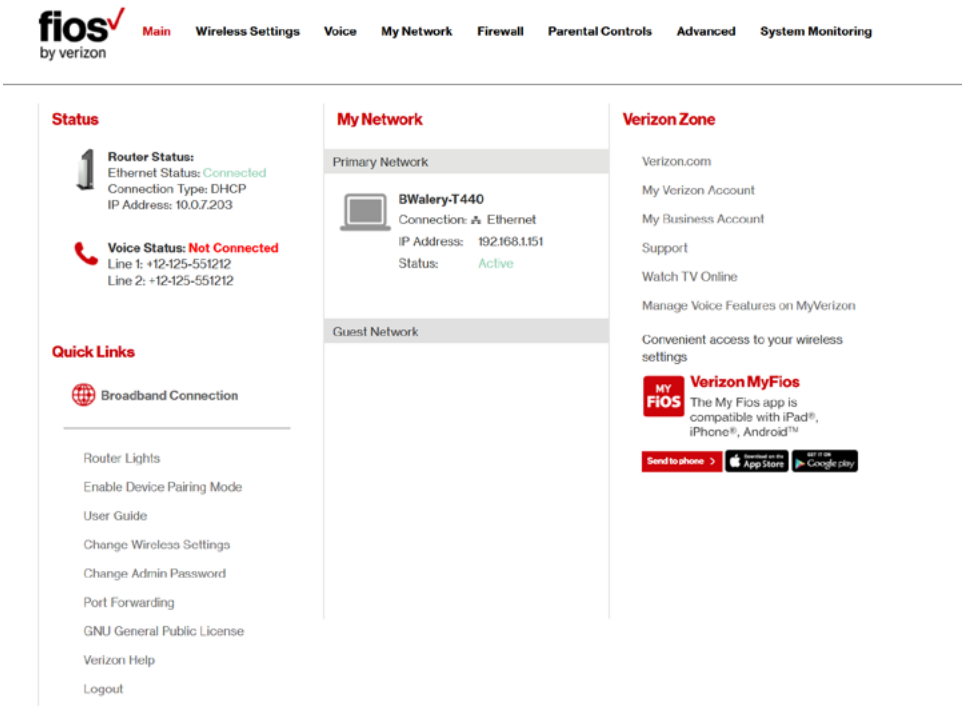
2. Open the device's wireless settings application.
3. Select your Fios Router's wireless network name (SSID) from the device's list of discovered wireless networks.
4. When prompted, enter your Fios Router's wireless password (WPA2 key) into the device's wireless settings. Your Fios Router's default wireless network name and wireless password are located are on the sticker on the side 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 wirelessly connecting to your Fios Router.

2.2/ MAIN SCREEN

When you log into your Fios Router, the page displays showing the Main navigation menu at the top of the page and your Fios Router's Status, including Quick Links, My Network, and Verizon Zone display in the body of the page.

 |

MAIN SCREEN



2.2a/ MENU

The Main menu links across the top of the page to the following configuration options and chapters:

- **Wireless Settings** - Chapter 3
- **Voice** - Chapter 4
- **My Network** - Chapter 5 and 6

- **Firewall** - Chapter 7
- **Parental Controls** - Chapter 8
- **Advanced** - Chapter 9
- **System Monitoring** - Chapter 10

2.2b/ STATUS

This section displays the status of your Fios Router's local network (LAN) and Internet connection (WAN).

BROADBAND CONNECTION

Broadband Connection displays the state of the broadband connection:

- **Broadband interface:** Ethernet or Fiber
- **Connected status:** Connected or No Connection
- **Connection Type:** DHCP or Static
- **WAN IP address:** Address of the broadband connection

QUICK LINKS

Quick Links contains frequently accessed documentation, such as Router Lights, Enable Device Pairing Mode, User Guide, Verizon Help, and settings, such as Change Wireless Settings, Change Admin Password, and Port Forwarding as well as Logout.

 |

MAIN SCREEN

MY NETWORK

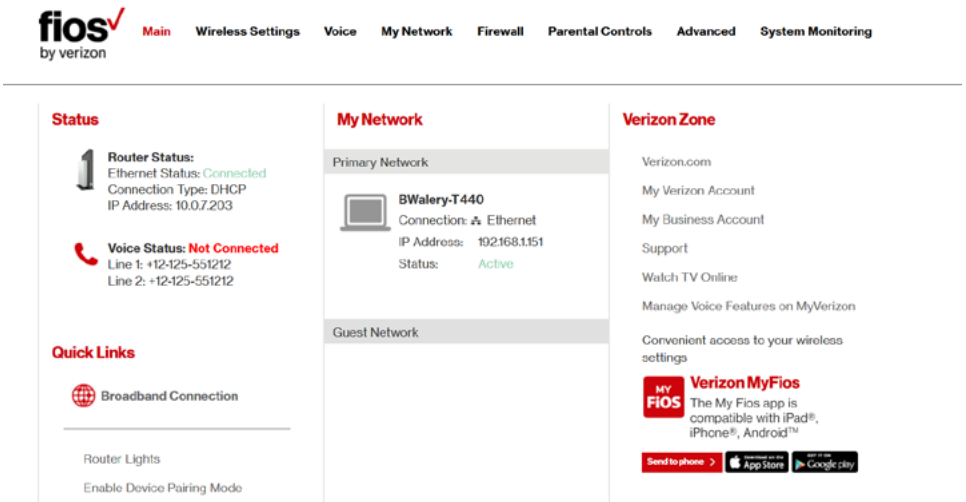
My Network displays the connection type, IP address, and status of all devices that have accessed or are currently connected to the network.

The icon associated with the device displays to signify the device is active or shaded gray to indicate the device has not been active for several minutes. You can view the individual settings of each device by clicking its icon.

VERIZON ZONE

The Verizon Zone contains links to various Verizon web sites and other informational links.

Note: You may see an alert when using an older 802.11b device indicating the Wi-Fi network performance maybe affected, as shown in the example below.



03/

WIRELESS SETTINGS

 |

OVERVIEW

Wireless networking enables you to free yourself from wires and plugs, making your devices more accessible and easier to use.

You can create a wireless network, including accessing and configuring wireless security options.

3.0/ OVERVIEW

Your Fios Router provides you with wireless connectivity using the 802.11b, g, n, or ac standards. These are the most common wireless standards.

802.11b has a maximum data rate of 11 Mbps, 802.11g has a maximum data rate of 54 Mbps, 802.11n has a maximum data rate of 450 Mbps, and 802.11ac has a maximum data rate of 1300 Mbps.

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

Note: 802.11 b is a legacy mode and is not recommended. Even one 802.11b device connected to the network will slow your entire wireless network.

The wireless service and wireless 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 Fios Router.

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

2.4 GHz Wi-Fi :
Fios-ZGN7
5 GHz Wi-Fi :
Fios-ZGN7-5G
Wi-Fi password:
music900key27eagle

 |

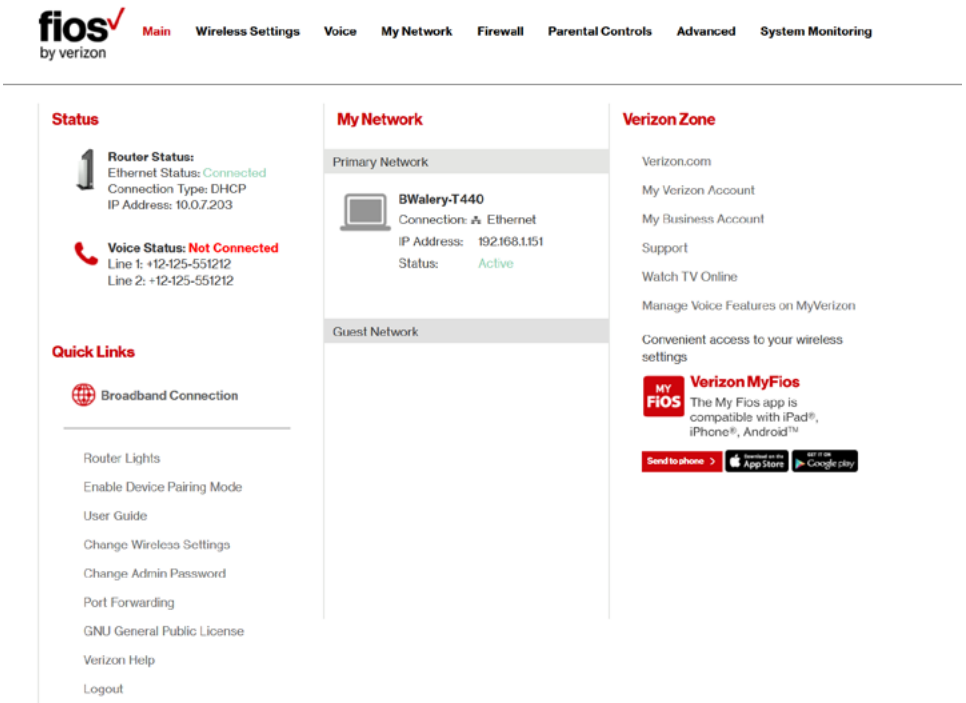
WIRELESS STATUS

3.1/ WIRELESS STATUS

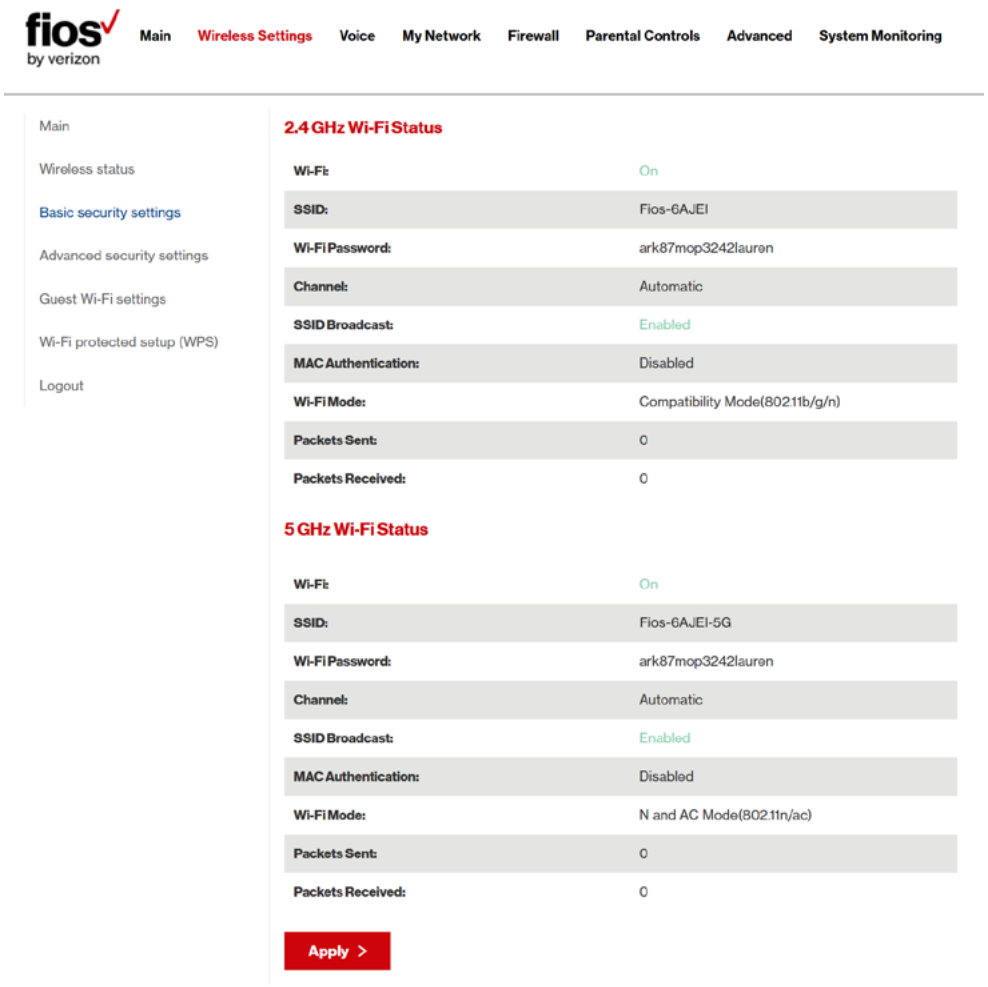
Use the Wireless Status feature to view the status of your Fios Router's wireless network.

To view the status:

1. Access the Main page. You can quickly view your Fios Router's wireless status in the My Network column. This includes all devices that have recently accessed or are currently connected to the network.



2. Select the **Wireless Settings** icon. The Wireless Status page displays additional wireless details.



 |

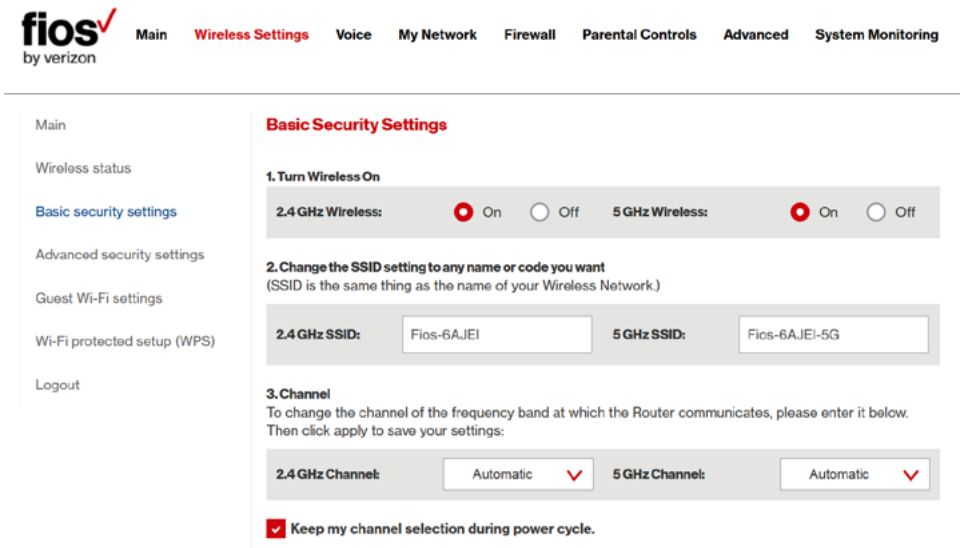
WIRELESS STATUS AND BASIC SECURITY SETTINGS

3. On the Wireless Status page for either 2.4 GHz or 5 GHz, the following information displays:
    - **Radio Enabled** - displays whether the wireless radio is active. When the radio is not enabled, no wireless devices will be able to connect to the home network.
    - **SSID** - displays the SSID (Service Set Identifier) shared among all devices on a wireless network. The SSID is the network name. All devices must use the same SSID.
    - **Channel** - displays the channel the wireless connection is currently using.
    - **Security Enabled** - displays the type of security active on the wireless connection as well as the security encryption key.
    - **SSID Broadcast** - displays whether your Fios Router is broadcasting its SSID. If activated, the SSID of your Fios Router wireless network is broadcast wirelessly. If not activated, the SSID is hidden and the wireless clients must be manually configured to use the SSID.
    - **MAC Authentication** - displays whether your Fios Router is using MAC (Media Access Control) address authentication to allow wireless devices to join the network.
    - **Wireless Mode** - displays the types of wireless device that can join the network.

- **WMM** - displays if WMM is enabled on your Fios Router.
- **Packets Received/Sent** - displays the number of packets received and sent since the wireless capability was activated.

3.2/ BASIC SECURITY SETTINGS

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



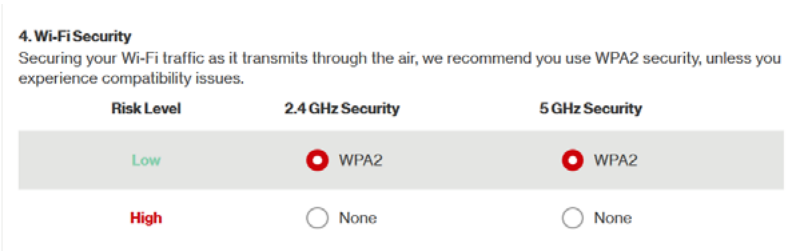
 |

BASIC SECURITY SETTINGS AND ADVANCED SECURITY SETTINGS

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

1. On the Wireless Setting page, select **Basic Security Settings**.
2. To activate the wireless radio, click the **On** radio button.
3. If desired, enter a new name for the wireless network in the **SSID** field or leave the default name that displays automatically.
4. Select the channel you want the wireless radio to use to communicate or accept the default Automatic channel, then select the **Keep my channel selection during power cycle** check box to save your channel selection when your Fios Router is rebooted.

To configure the basic Wi-Fi Security settings, select a Security option:

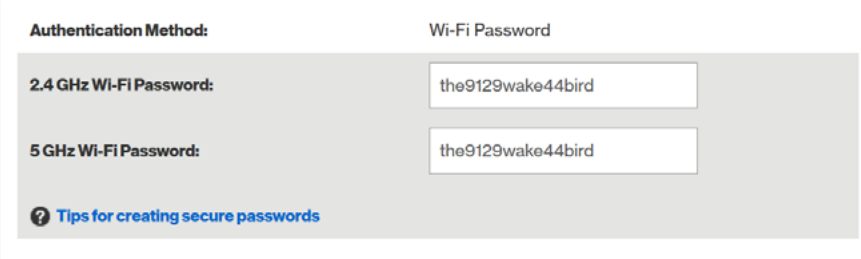


WPA2

If WPA2 (Wi-Fi Protected Access II) was selected, the WPA2 page displays.

To set the WPA2 security:

1. Enter the Pre-Shared Key.



2. Click **Apply** to save the changes.

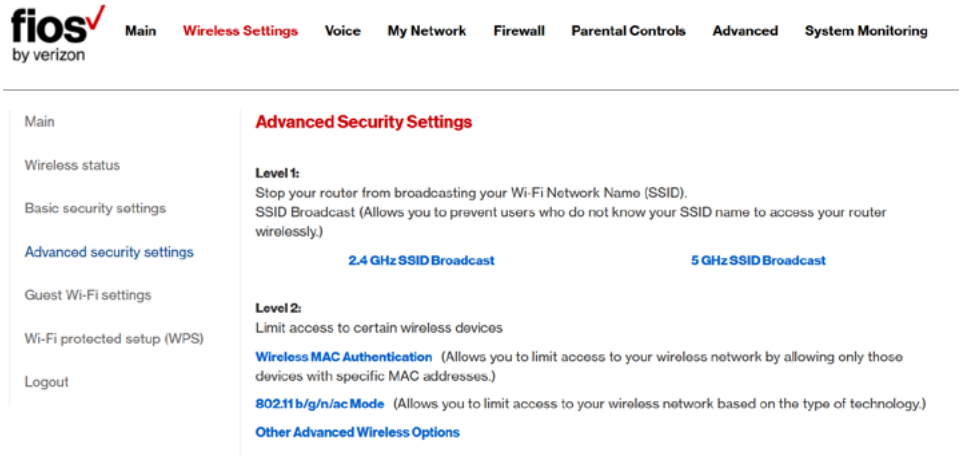
3.3/ ADVANCED SECURITY SETTINGS

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

 |

ADVANCED SECURITY SETTINGS

To modify the advanced security settings, select the option from the level to be modified for either 2.4 GHz or 5 GHz:

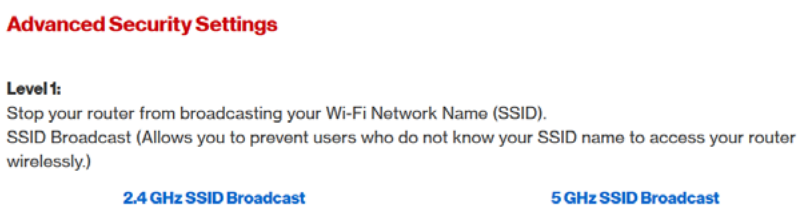


3.3a/ LEVEL 1: SSID BROADCAST

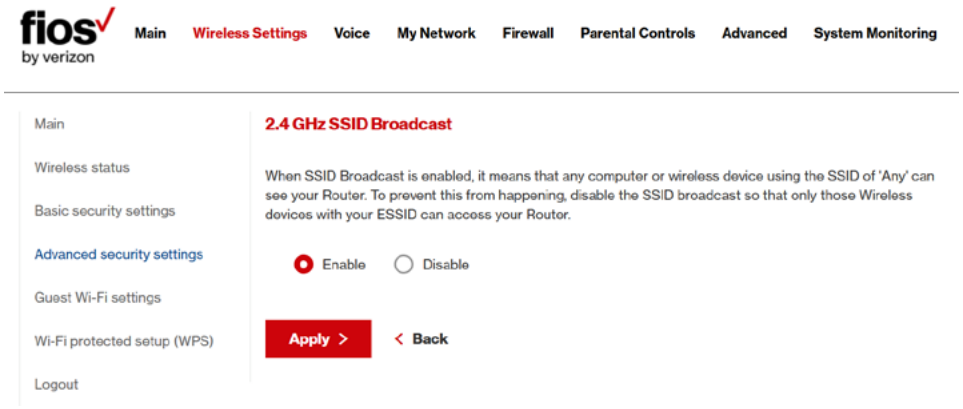
You can configure your Fios Router's SSID broadcast capabilities to allow or disallow wireless devices from automatically using a broadcast SSID name to detect your Fios Router wireless network.

To enable or disable SSID broadcast:

1. In the Advanced Settings page, locate the **Level 1** section.



2. Click the **2.4 GHz SSID Broadcast** or **5 GHz SSID Broadcast** link for the wireless network you wish to modify. The following example uses the 2.4 GHz network. The display configuration looks basically the same for the 5 GHz network.



 |

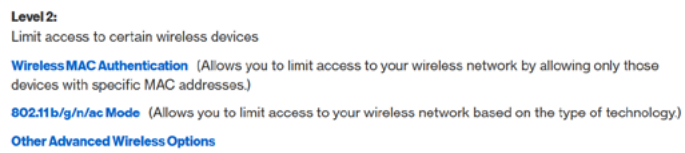
3. To enable SSID broadcasting, click the **Enable** radio button. SSID broadcast is enabled by default. The SSID of the wireless network will be broadcast to all wireless devices.
4. To disable SSID broadcasting, click the **Disable** radio button. The public SSID broadcast will be hidden from all wireless devices. You will need to manually configure additional wireless devices to join the wireless network.
5. Click **Apply** to save the changes.

3.3c/ LEVEL 2: LIMIT ACCESS

You can configure your Fios Router to limit access to your wireless network allowing access only to those devices with specific MAC addresses or based on the type of wireless technology used.

To limit access:

1. In the Advanced Settings page, locate the **Level 2** section.



2. To allow only devices with specific MAC addresses, click the **Wireless MAC Authentication** link. The Wireless MAC Authentication page displays. For additional details, refer to the **Wireless MAC Authentication** section.

3. To limit access based on the type of technology, click the **802.11 b/g/n/ac Mode** link. The 802.11 b/g/n/ac Mode page displays. For additional details, refer to the **802.11 b/g/n/ac Mode** section.
4. To access other advanced wireless options, click the **Other Advanced Wireless Options** link. The Other Advanced Wireless Options page displays. For additional details, refer to the **Other Advanced Wireless Options** section.

3.4/ WIRELESS MAC AUTHENTICATION

You can allow or deny access to your wireless network by specifying devices with specific MAC addresses.

To set wireless MAC authentication:

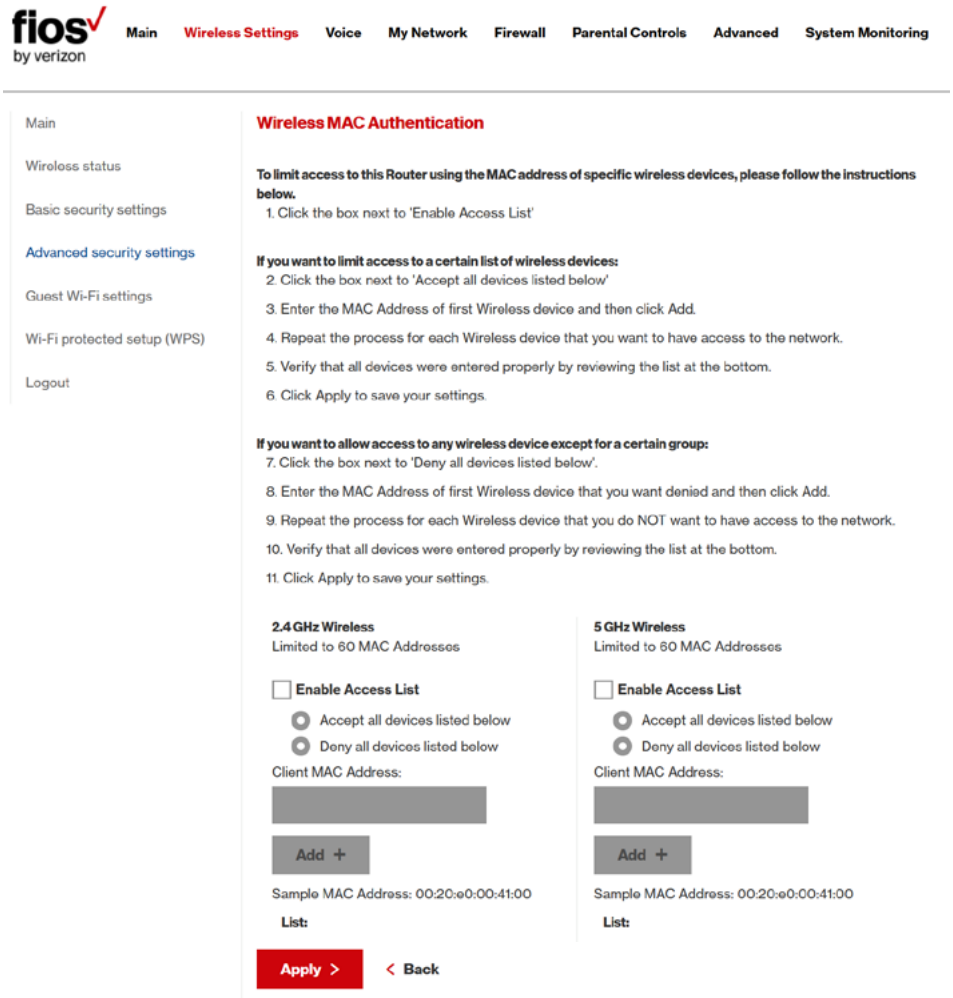
1. On the Advanced Settings page, locate the **Level 2** section and click the **Wireless MAC Authentication** link. The Wireless MAC Authentication page displays.
2. To enable access control, select the **Enable Access List** check box.
3. Select either:
   - **Accept all devices listed below** – allows only the listed devices to access the wireless network.

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

 |

WIRELESS MAC AUTHENTICATION AND 802.11 MODE

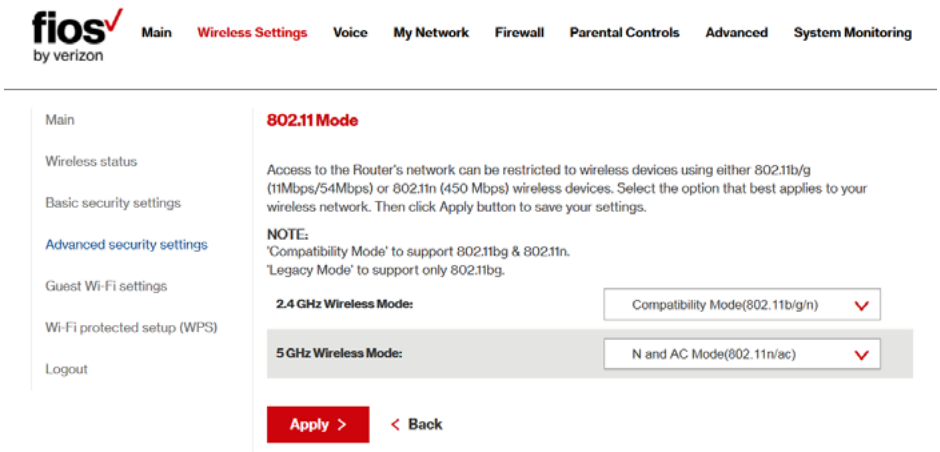
- **Deny all devices listed below** – denies access to the listed devices. All other wireless devices will be able to access the wireless network if they use the correct wireless password.



4. Enter the MAC address of a device, then click **Add**.
5. Repeat step 2 to add additional devices, as needed.
6. To remove a specific device's MAC address, click the **Remove** button next to the specific MAC address.
7. When all changes are complete, click **Apply** to save changes.

3.5/ 802.11 MODE

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



 |

802.11 MODE AND OTHER ADVANCED WIRELESS OPTIONS

To select the 802.11 Mode:

1. On the Advanced Settings page, locate the Level 2 section and click the 802.11 Mode link. The 802.11 Mode page displays.
2. Select the 2.4 GHz Wireless Mode as follows:
    - **Compatibility** – This is the default mode setting, providing a good balance of performance and compatibility with existing wireless devices. 802.11b, g, and n devices can connect.
    - **Legacy** – For older wireless devices. Only 802.11b and g devices can connect. 802.11b (legacy mode) will cause your wireless network to slow and is not recommended.
    - **Performance** – For newer wireless 802.11n devices only. No other devices can be used.
3. Select the 5 GHz Wireless Mode as follows:
    - **N and AC Mode** – This is the default setting. Both 802.11n and 802.11ac are available on the 5 GHz frequencies.
    - **AC Only Mode** – This provides maximum performance. 802.11ac devices will have exclusive use of the 5 GHz frequencies and 802.11n devices will not be able to connect at 5 GHz.
4. Click **Apply** to save the changes.

3.6/ OTHER ADVANCED WIRELESS OPTIONS

You can view additional wireless options.

Comment: Recommend leaving defaults as is unless otherwise directed.

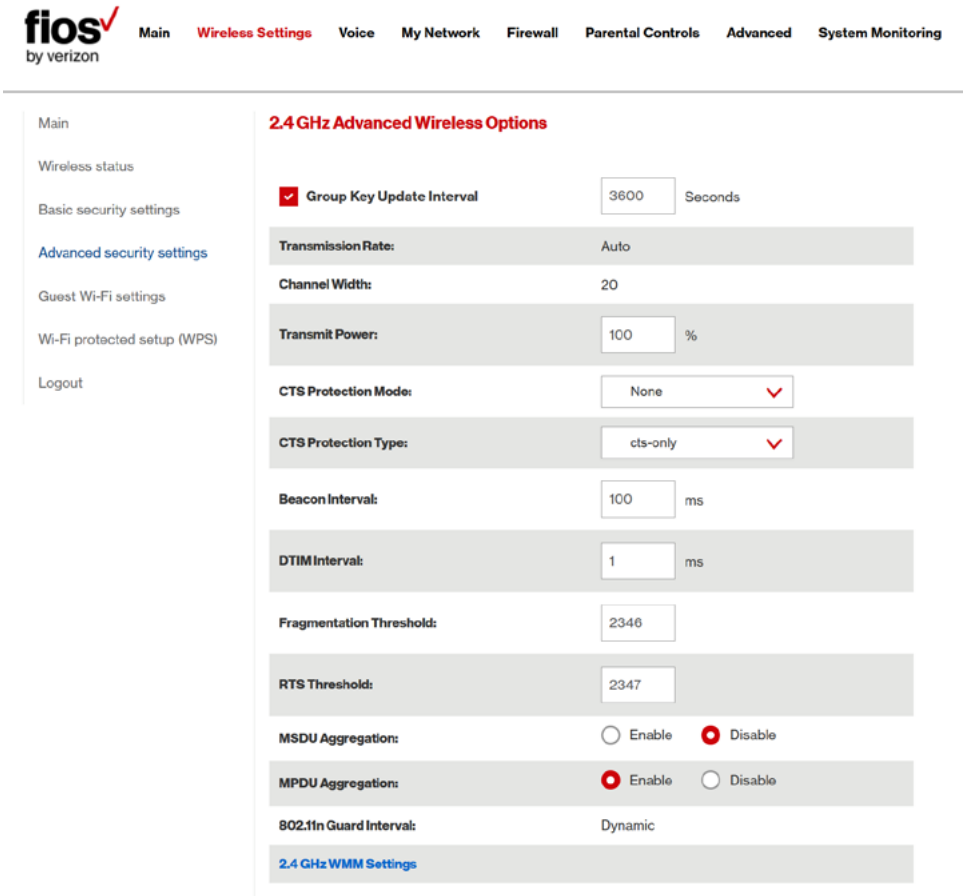
To view the options:

1. In the Advanced Settings page, locate the **Level 2** section and click **Other Advanced Wireless Options** link. A warning message displays.
2. Click **Yes**. The Other Advanced Wireless Options page displays.

   Comment: The following example uses the 2.4 GHz network. The display configuration looks basically the same for the 5 GHz network.

 |

OTHER ADVANCED WIRELESS OPTIONS



3. 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 Fios Router and your local network.

- **Group Key Update Interval** – time interval used to update the WPA shared key (used to generate the group key)
- **Transmission Rate** – displays status as Auto
- **Channel Width** – Controls the bandwidth of the wireless signal
- **Transmit Power** – adjusts the power of the wireless signal
- **CTS (Clear to Send) Protection Mode** – allows mixed 802.11b/g/n/ac networks to operate at maximum efficiency
- **CTS Protection Type** – displays cts, which is only for mixed 802.11b/g/n/ac networks or rts_cts, which is for 802.11a/b/g networks
- **Beacon Interval** – displays the time period of the beacon interval
- **DTIM (Delivery Traffic Indication Message) Interval** – provides a countdown mechanism, informing wireless network clients of the next window for listening to broadcast and multicast messages

 |

- **Fragmentation Threshold** – increases the reliability of frame transmissions on the wireless network
- **RTS Threshold** – controls the size of the data packet that the low level RF protocol issues to an RTS packet
- **MSDU Aggregation** – enables or disables MSDU aggregation
- **MPDU Aggregation** – enables or disables MPDU aggregation

5. To access the WMM settings, click the **WMM Settings** link.
6. Click **Apply** to save changes.

3.6a/ WMM SETTINGS

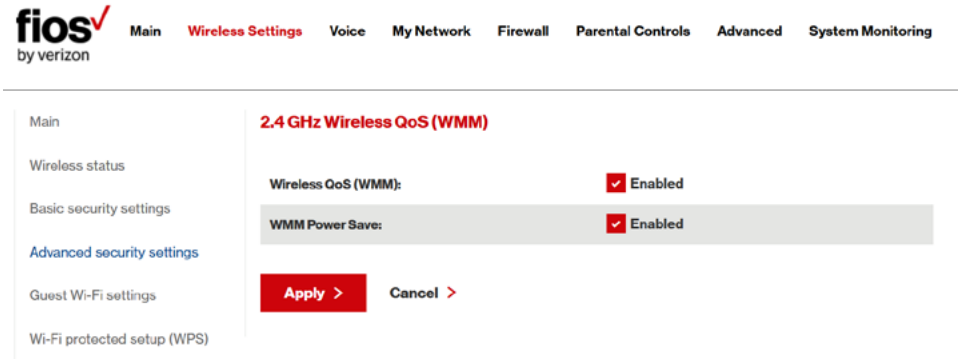
You can prioritize the types of data transmitted over the wireless network using the advanced WMM settings. Wireless QoS (WMM) can improve the quality of service (QoS) for voice, video, and audio streaming over Wi-Fi by prioritizing these data streams.

WMM Power Save can improve battery life on mobile Wi-Fi devices such as smart phones and tablets by fine-tuning power consumption.WMM (Wi-Fi Multimedia) QoS and Power Save require a wireless client device which also supports WMM.

Note: The following example uses the 2.4 GHz network. The display configuration looks basically the same for the 5 GHz network.

To set the options:

1. In the Advanced Wireless Options page, click **WMM Settings** link. A warning message displays.



2. Click **Yes**. The WMM Settings page displays.
3. To enable Wireless QoS (WMM), select the **Enabled** check box.
4. To enable WMM Power Save, enable **Wireless QoS (WMM)** first, then enable WMM Power Save by selecting the **Enabled** check box.
5. Click **Apply** to save changes.

3.7/ GUEST WI-FI SETTINGS

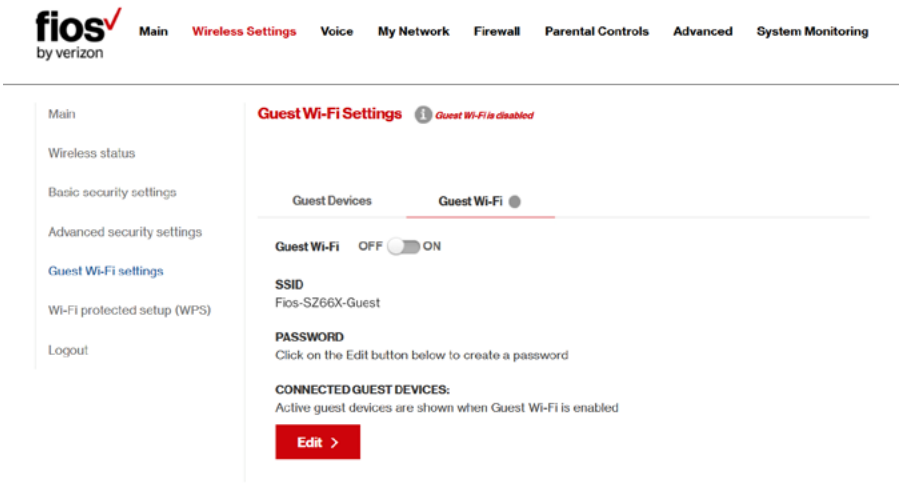
The Guest Wi-Fi network is designed to provide Internet connectivity to your guests but restricts access to your primary network and shared files. The primary network and the guest network are separated from each other through firewalls. You create one Guest Wi-Fi SSID and one password and use it for all guests. Guest Wi-Fi can be managed using either the Fios Router's web interface, or via

 |

GUEST WI-FI SETTINGS

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 wireless network name (ESSID) which is displayed on a sticker located at the side 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”.

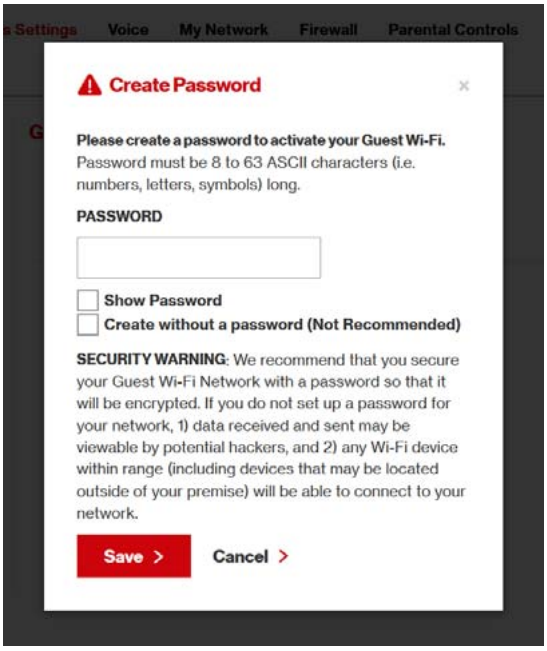


3.7a/ GUEST WI-FI

To enable Guest Wi-Fi:

1. From the Main menu, select Wireless Settings, then select Guest Wi-Fi Settings

2. Select the Guest Wi-Fi tab
3. Press the Edit button and enter a valid SSID and password
4. Press **Save** to save changes



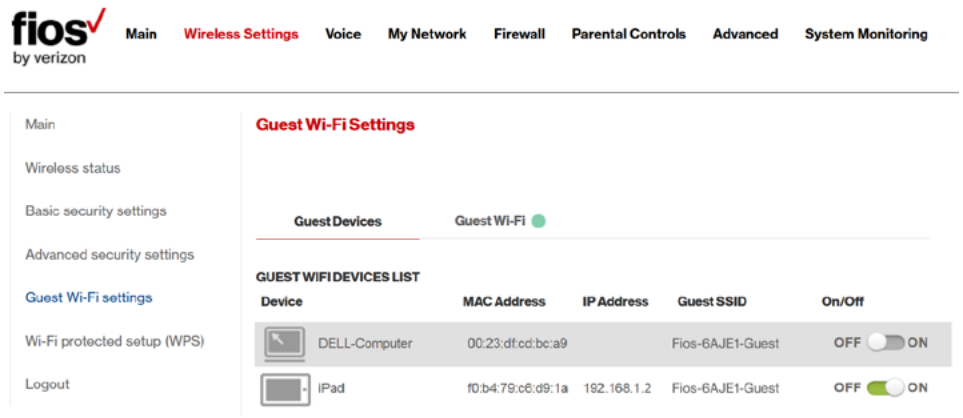
5. Toggle the Guest Wi-Fi button to ON

 |

GUEST WI-FI SETTINGS

3.7b/ GUEST DEVICES

The devices on the Guest Wi-Fi network can be viewed on the Guest Devices page. If the admin toggles the button next to a device to OFF, that device will be blocked from accessing the Internet.



04/

VOICE

 |

OVERVIEW AND VOICE STATUS

The Fios Router functions as a base station for DECT 6.0 handsets and Wireless Phone Jacks. DECT 6.0 delivers superior voice and sound quality compared to older phones.

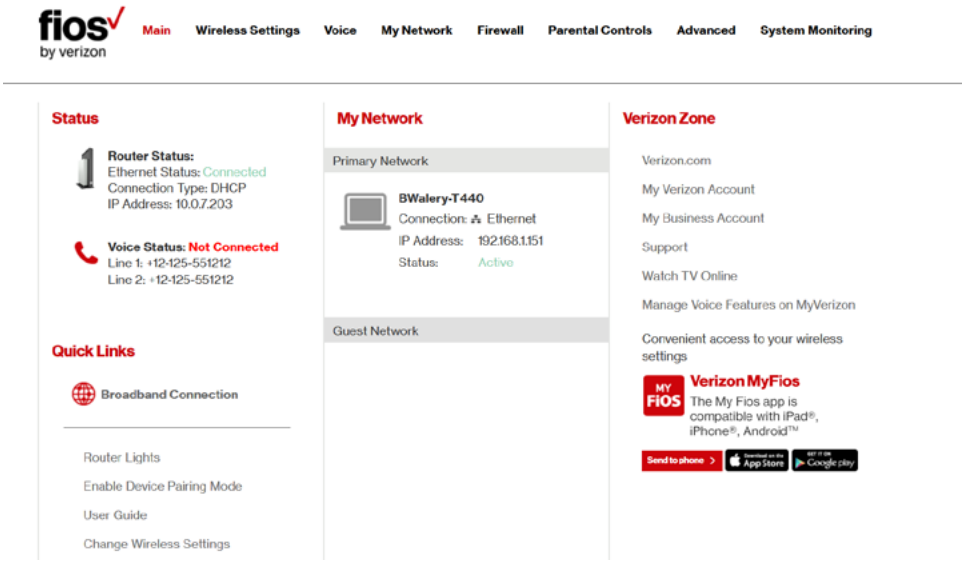
4.0/ OVERVIEW

The Fios Router can support up to 2 active phone numbers and are assigned to the RJ-11 ports on the back of the Fios Router. You can connect to the active phone numbers using either the RJ-11 ports or via DECT 6.0 technology. The Fios Router has an integrated DECT 6.0 base station that allows you to connect up to five of your compatible DECT 6.0 devices.

4.1/ VOICE STATUS

To view status:

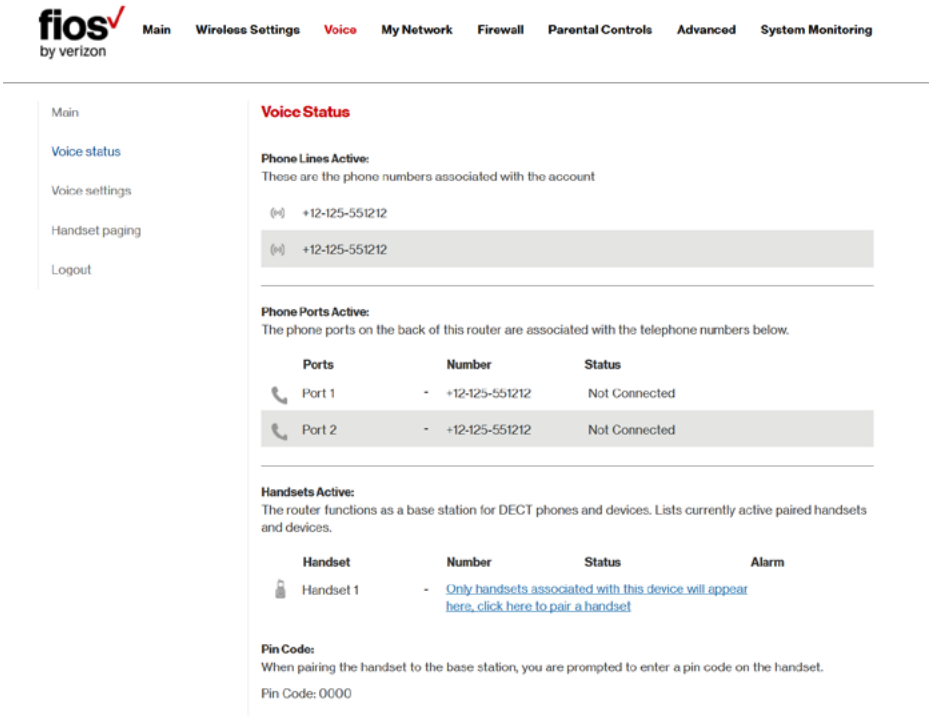
1. Access the Main page.



 |

VOICE STATUS AND VOICE SETTINGS

2. Click on **Voice**. The Voice Status page displays additional details.



3. On the Voice Status page, the following information is displayed
   - **Phone Lines Active** – displays the phone numbers associated with the account.

- **Phone Ports Active** – displays the phone ports associated with the phone numbers linked to the account.
- **Handsets Active** – The Fios Router functions as a base station for DECT phone and devices. Displays the devices paired to the Fios Router.
- **Pin Code** – displays the pin code. When pairing the handset to the base station, you are prompted to enter the pin code into the handset.

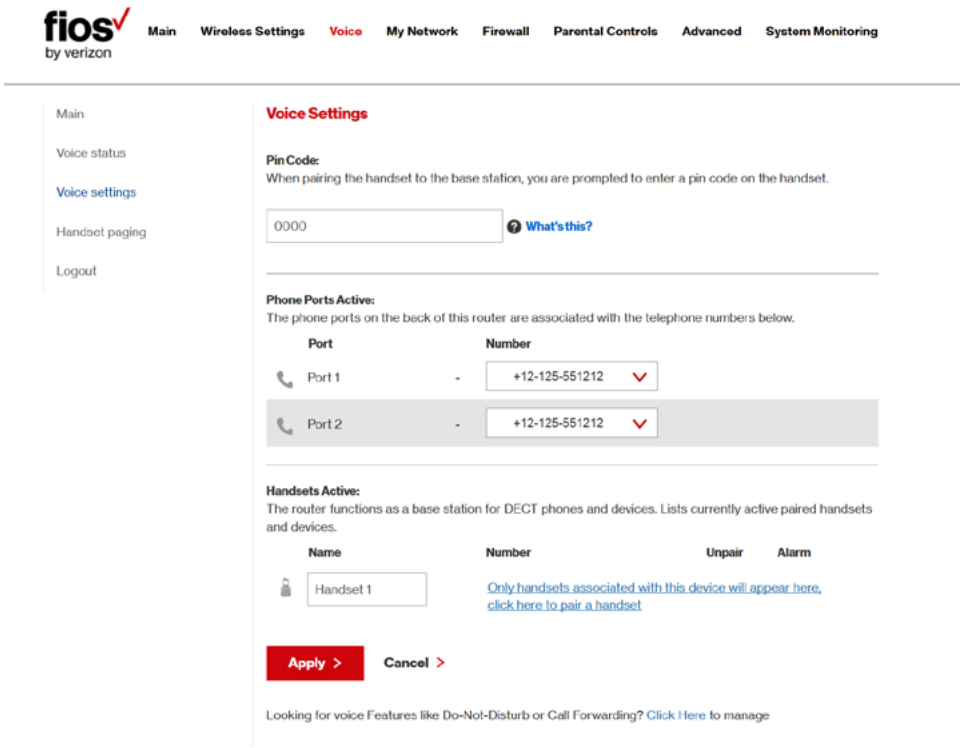
4.2/ VOICE SETTINGS

You can configure the voice settings on your Fios Router:

1. To pair your DECT 6.0 device (e.g. your DECT 6.0 handset) press the Unified Button located on the front panel of your Fios Router for 2-5 seconds. The Unified Button will begin to slowly blink blue.
2. Then follow your DECT 6.0 devices instructions of pairing to the Fios Router.
3. Once the DECT 6.0 pairing process has completed successfully, the Unified Button on the Fios Router's front panel will turn solid blue for 2 minutes.

 |

VOICE SETTINGS AND HANDSET PAGING



To configure the voice settings:

1. **Pin Code** – You can enter a new Pin code or you can leave the default Pin code that displays automatically.
2. **Phone Ports Active** – You can associate a phone number to the ports on the back of this router.

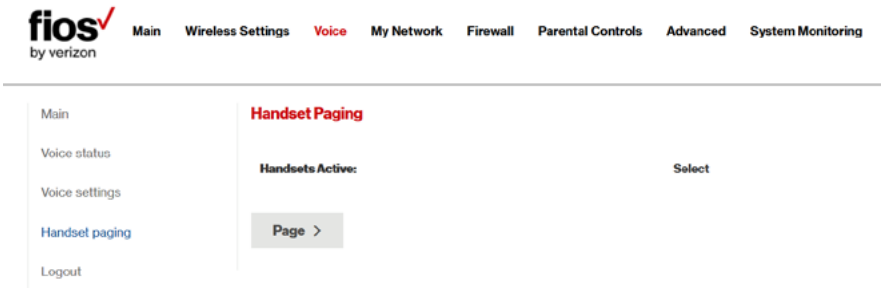
3. **Handsets Active** – You can enter a new name for your DECT phones and devices or you can leave the default name that displays automatically. You can also assign phone number to the phones and devices. To unpair a device, check the Unpair box. Only a Wireless Phone Jack can be assigned as an Alarm. Setting an alarm for the Wireless Phone Jack will allow the Alarm to seize the associated phone line in case of an emergency.

4.3/ HANDSET PAGING

You can page the Handsets that are connected to your Fios Router using one of the two following methods:

To page all DECT 6.0 devices press the Unified Button located on the front panel of your Fios Router for 10+ seconds.

To page an individual DECT 6.0 devices, select the checkbox against that handset and click the Page button.



 |

HANDSET PAGING

05/

CONFIGURING MY NETWORK SETTINGS

 |

ACCESSING MY NETWORK SETTINGS

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

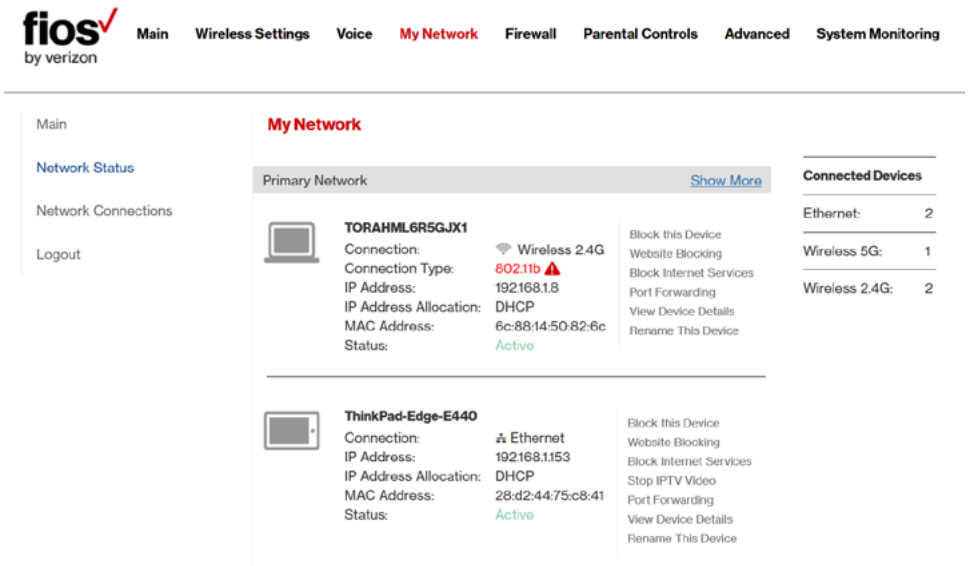
Caution: The settings described in this chapter should only be configured by experienced network technicians. Changes could adversely affect the operation of your Fios Router and your local network.

5.0/ ACCESSING MY NETWORK SETTINGS

My Network 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.

To view your network connections:

1. On the Main page, select the **My Network** icon. The My Network page opens with our current status displayed.



 |

USING MY NETWORK SETTINGS

5.1/ USING MY NETWORK SETTINGS

You can access and configure common network parameters:

- **Block this Device** - Click **Block this Device** 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 8 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 gaming, 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 6 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. You can also click the device's icon in the Main page to display the Device Information page.
- **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 My Network page will open with the new name and icon displayed.

 |

06/

USING NETWORK CONNECTIONS

Your Fios Router supports various local area network (LAN) and wide area network (WAN), or Internet connections using Ethernet or fiber/optical cables.

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

 |

ACCESSING NETWORK CONNECTIONS

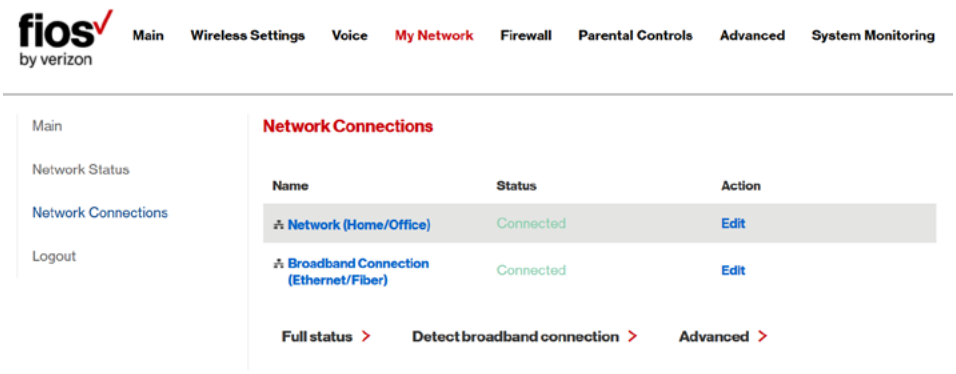
Caution: The settings described in this chapter should only be configured by experienced network technicians. Changes could adversely affect the operation of your Fios Router and your local network.

6.0/ ACCESSING NETWORK CONNECTIONS

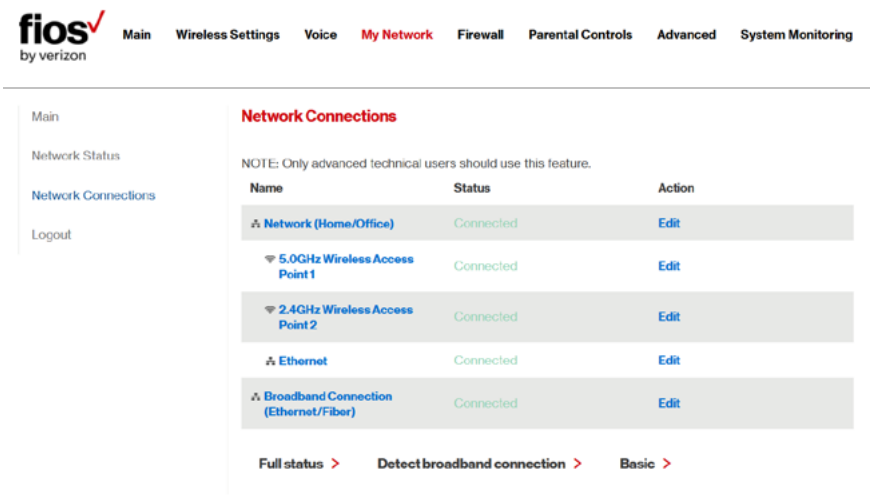
You can access your network connections and view the connections by connection type.

To access the network connections:

1. Select **My 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.

6.1/ 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.

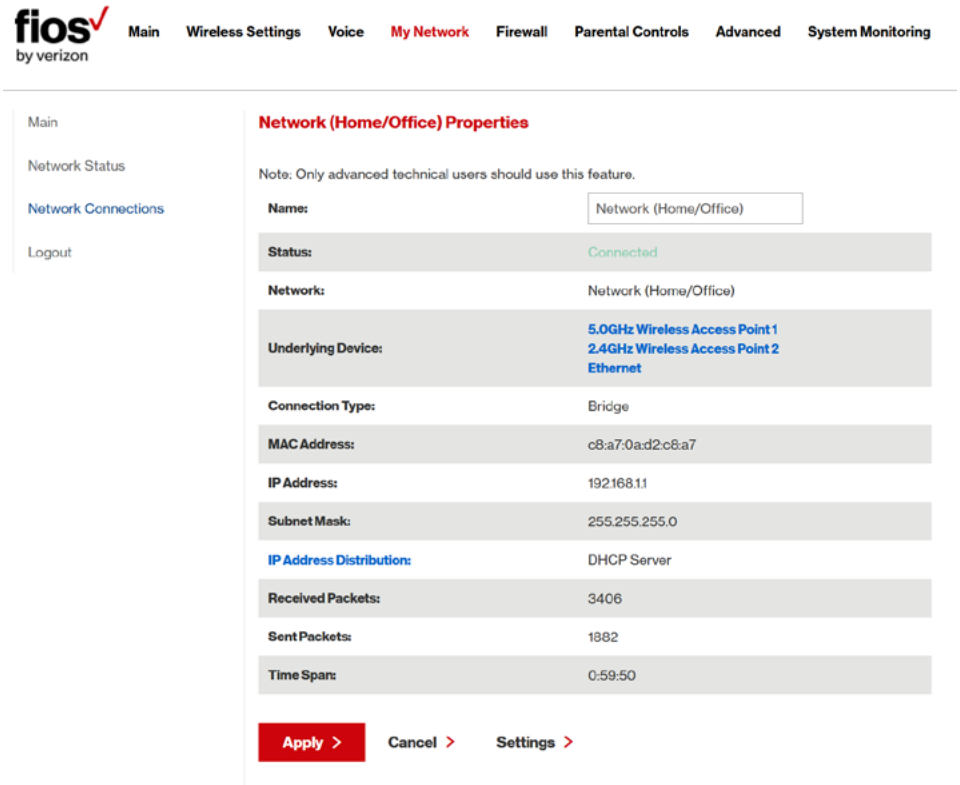
 |

NETWORK (HOME/ OFFICE) CONNECTION

Note: When a network connection is disabled, the formerly underlying devices 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.

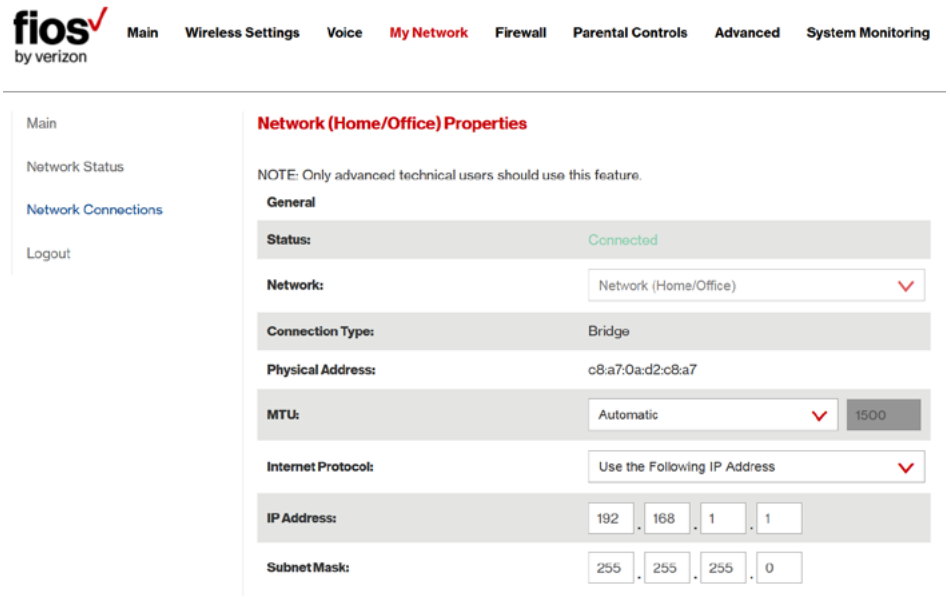


2. To rename a network connection, enter the new network name in the **Name** field.
3. Click **Apply** to save the changes.

CONFIGURING THE HOME/OFFICE NETWORK

To configure the network connection:

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



2. Configure the following sections, as needed.

 |

NETWORK (HOME/ OFFICE) CONNECTION

GENERAL

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

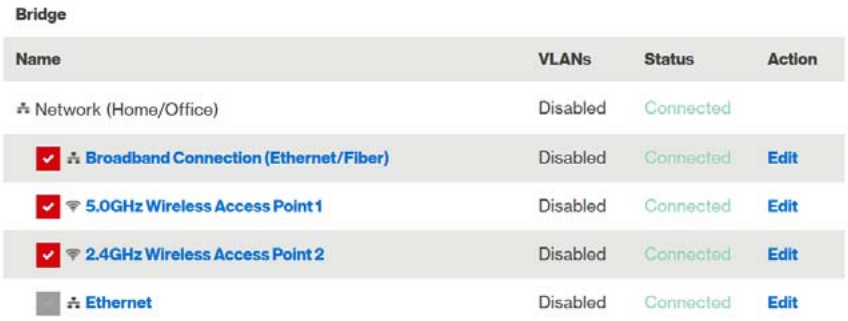
- **Status** - displays the connection status of the network.
- **Network** – displays the type of network connection.
- **Connection Type** - displays the type of connection.
- **Physical Address** - displays the physical address of the network card used for the network
- **MTU** - specifies the Maximum Transmission Unit (MTU) specifies the largest packet size permitted for Internet transmissions:
  - Automatic - sets the MTU 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
  - 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 Configure Network (Home/Office), you can configure the various LAN interfaces. By default, the Ethernet

and Wireless Access Point connections are included in the ‘Network (Home/Office)’ bridge.

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:

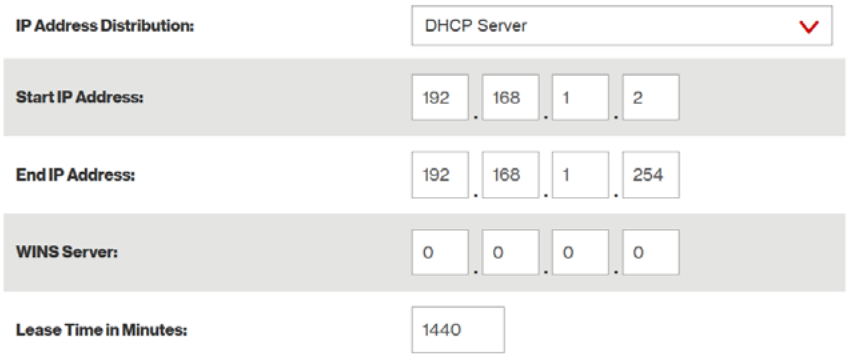
- **Status** – displays the connection status of a specific network connection.
- **Action** – contains an Edit hyperlink that, when clicked, generates the next lower-level configuration page for the specific network connection or network device.

IP ADDRESS DISTRIBUTION

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

 |

NETWORK (HOME/ OFFICE) CONNECTION



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.

ROUTING

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

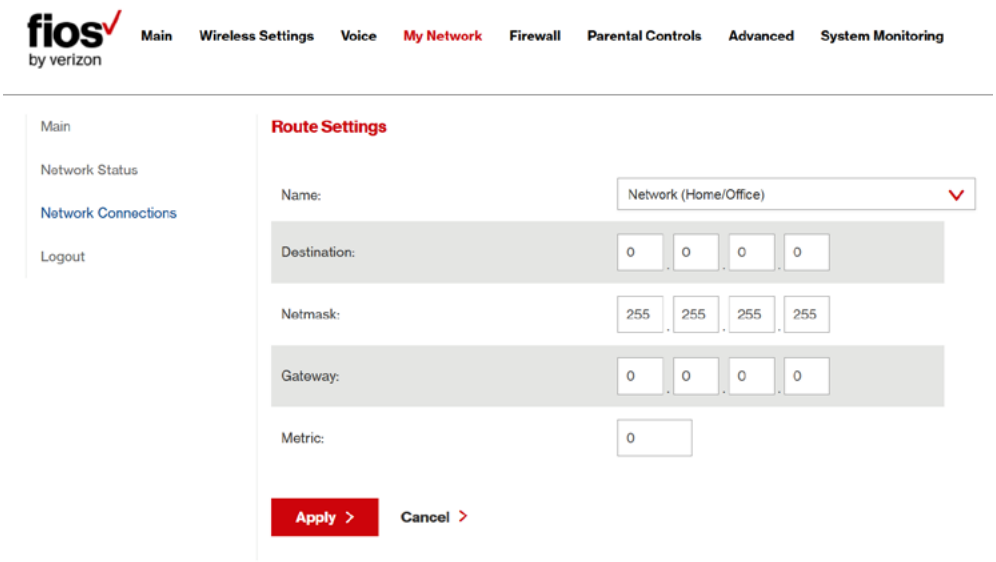
- **Static routing** – specifies a fixed routing path to neighboring destinations based on predetermined metrics.
- **Dynamic routing** – automatically adjusts how packets travel on the network. The path determination is based on network/device reachability and status of network being traveled.

To configure routing:

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

 |

NETWORK (HOME/ OFFICE) CONNECTION



COMPLETE NETWORK CONNECTION CONFIGURATION UPDATES

To save your changes click **Apply**.

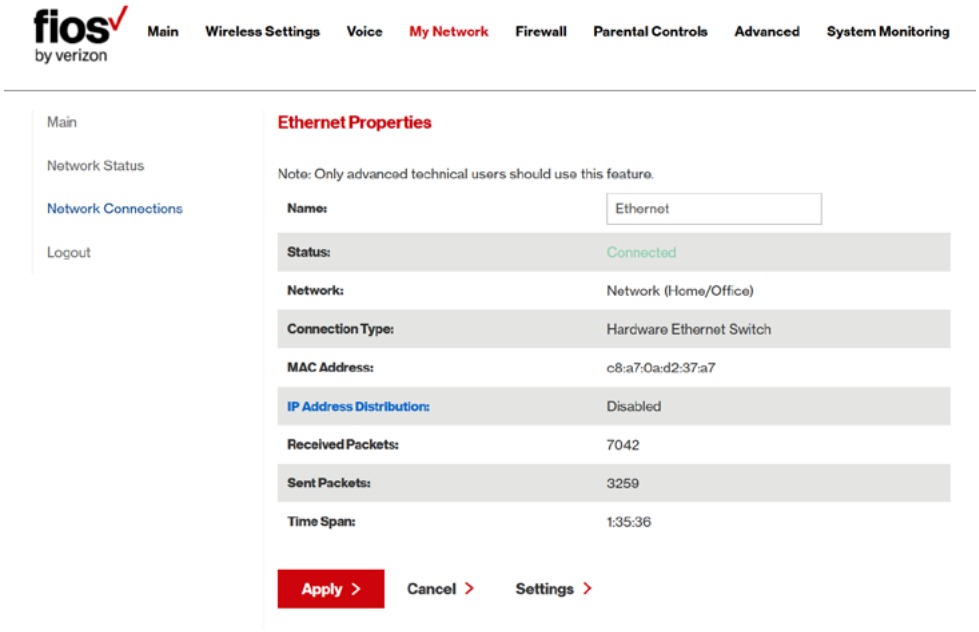
6.2/ ETHERNET CONNECTION

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.

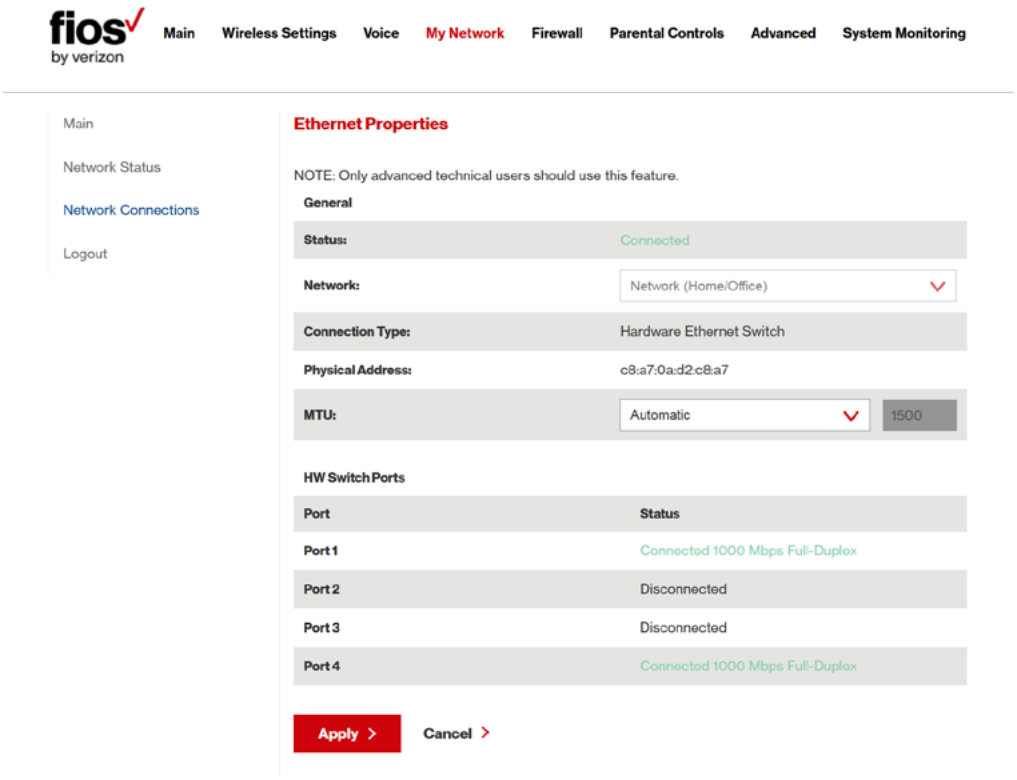
 |

ETHERNET CONNECTION

6.2a/ CONFIGURING THE ETHERNET/FIBER BROADBAND CONNECTION

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 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 to be set.
- **HW Switch Ports** - displays the status of each Local Network Ethernet port.

6.3/ WIRELESS ACCESS POINT CONNECTION

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

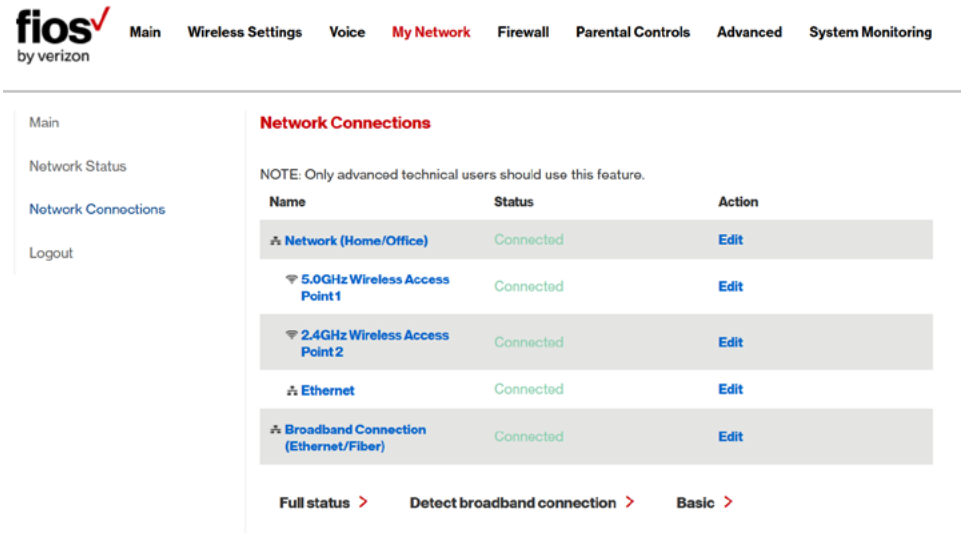
Note: Once disabled, all wireless devices connected to that wireless network will be disconnected from the LAN network and Internet.

 |

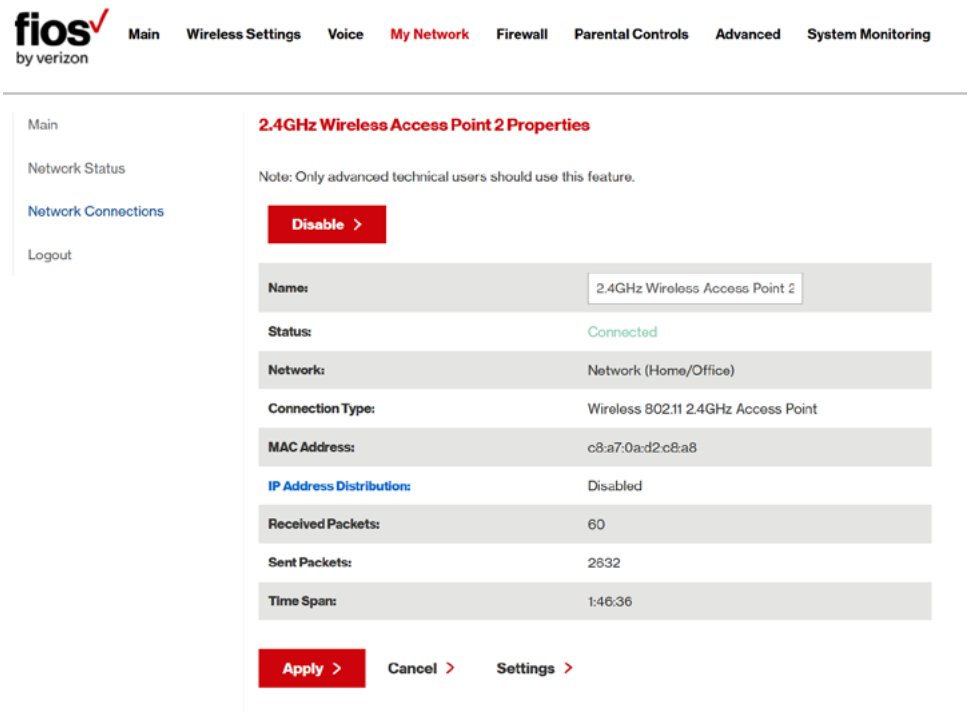
WIRELESS ACCESS POINT CONNECTION

To view the connection:

1. In the Network Connections page, click **Advanced**.



2. Click **5 GHz Wireless Access Point 1** or **2.4 GHz Wireless Access Point 2**.



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

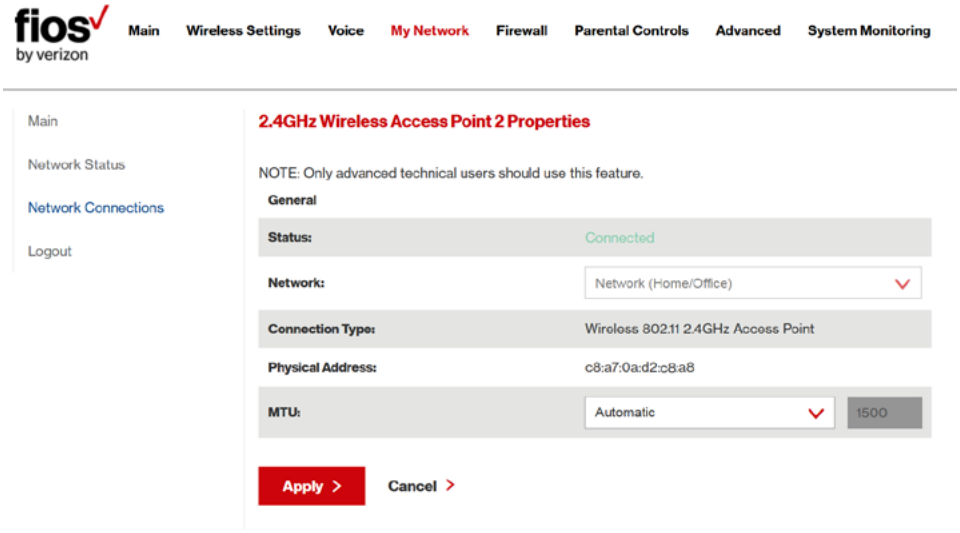
 |

WIRELESS ACCESS POINT CONNECTION

6.3a/ CONFIGURING WIRELESS ACCESS POINT PROPERTIES

To configure the connection:

1. In the Wireless Access Point Properties page, click **Settings**. The configuration page displays.



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.
   - **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.

6.4/ BROADBAND ETHERNET/FIBER CONNECTION

A Broadband Ethernet connection connects computers to your Fios Router using Ethernet cables. The connections are either direct or use network hubs and switches.

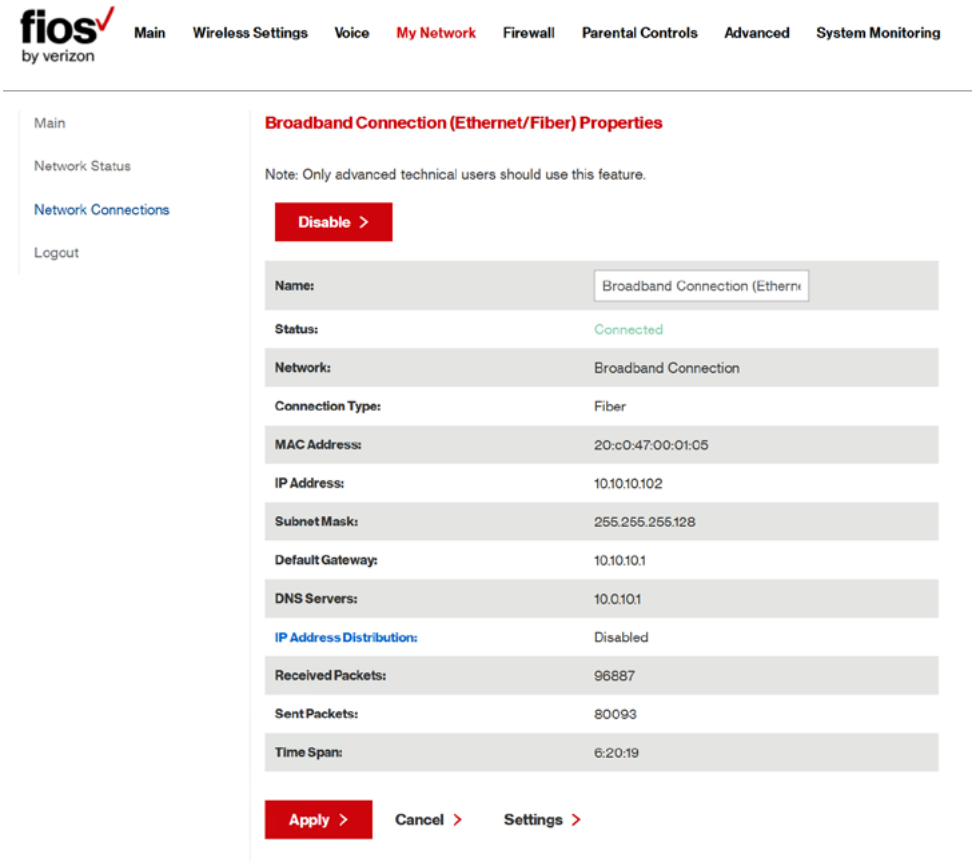
Note: If disabling the connection, you must reboot your Fios Router for the change to take effect.

To view the connection:

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

 |

BROADBAND ETHERNET/ FIBER CONNECTION

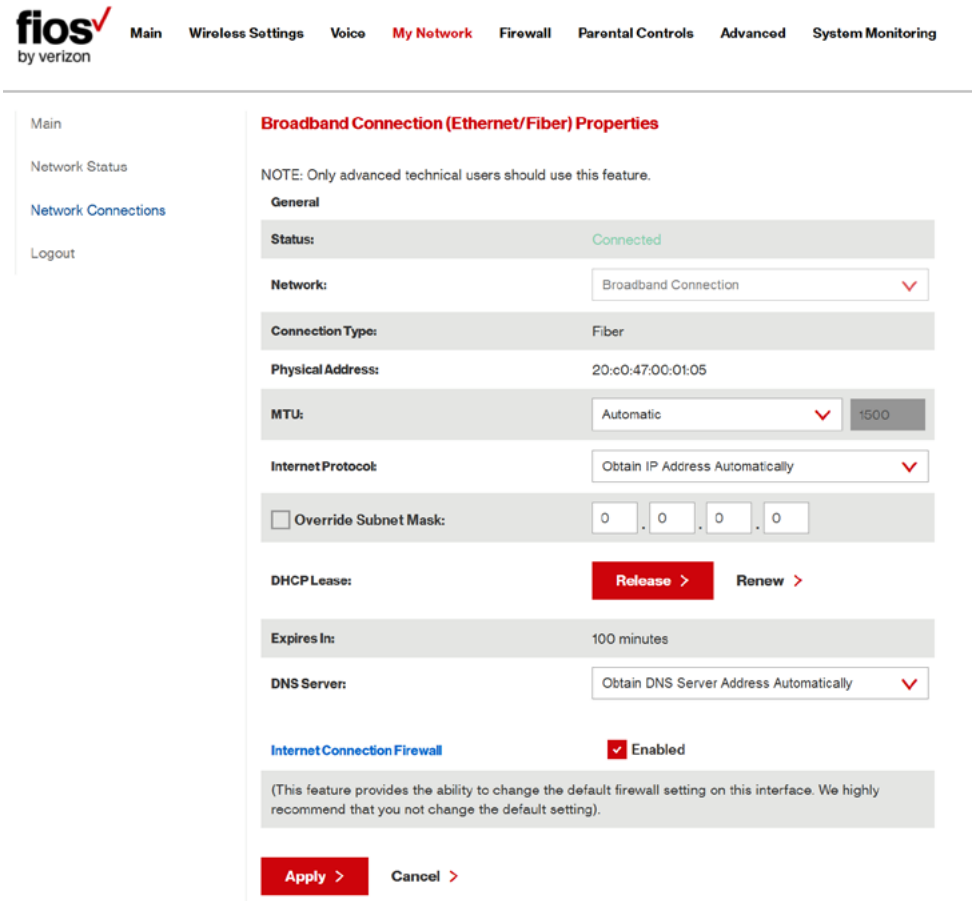


2. To rename the network connection, enter the new name in the **Name** field.
3. Click **Apply** to save changes.

6.4a/ CONFIGURING THE ETHERNET/FIBER CONNECTION

To configure the connection:

1. In the Broadband Connection (Ethernet/Fiber) 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 the type of connection
- **Physical Address** - displays the physical address of the network card used for the network
- **MTU** - specifies the largest packet size permitted for Internet transmissions

INTERNET PROTOCOL

1. In the Internet Protocol section, specify one of the following:
    - **No IP Address** – the connection has no IP address. This is useful if the connection operates under a bridge.
    - **Obtain an IP 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, then the IP address and subnet mask address.

2. To override the subnet mask, select the **Override Subnet Mask** check box, then enter the new subnet mask.

 |

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 Internet Gaming.
- **Remote Administration** - enable remote configuration of your Fios Router from any Internet-accessible computer.
- **Static NAT** - allow multiple static NAT IP addresses to be designated to devices on the network.
- **Security Log** - view and configure the security log.

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

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

The firewall regulates the flow of data between the local network and the Internet. Both incoming and outgoing data are inspected, then either accepted and allowed to pass through your 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.

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

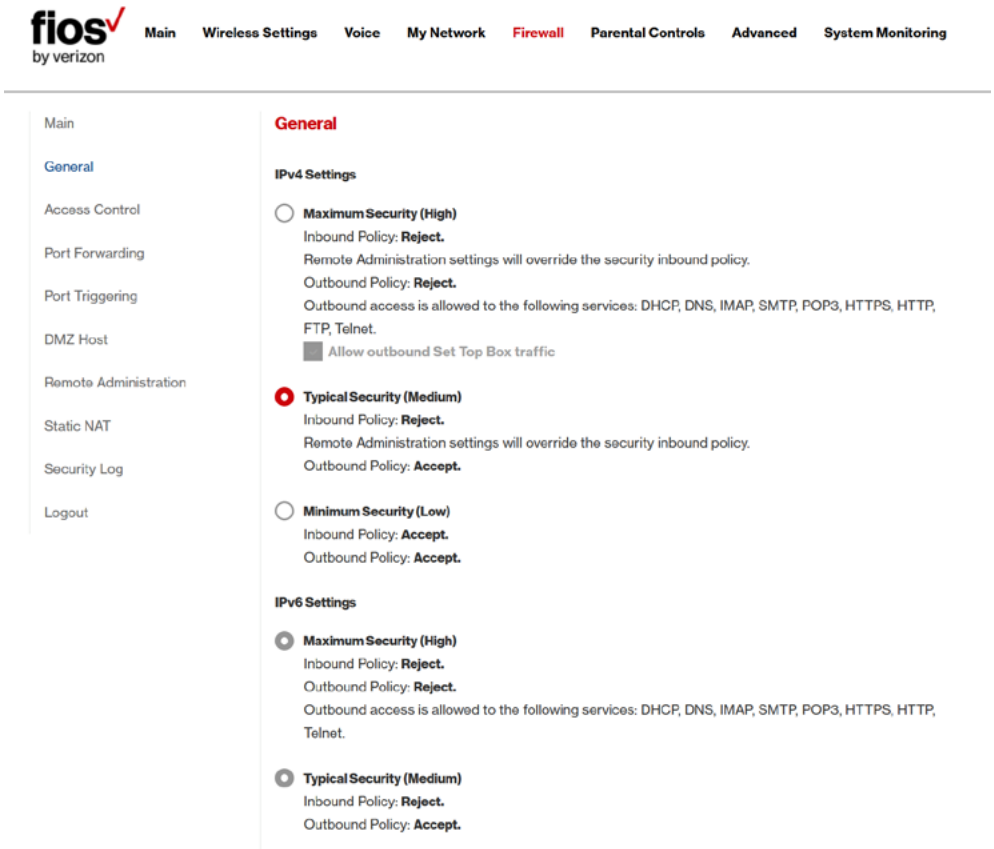
The request access is defined as:

- **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 IPv6 option to configure IPv6 security:



 |

ACCESS CONTROL

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.

7.1/ ACCESS CONTROL

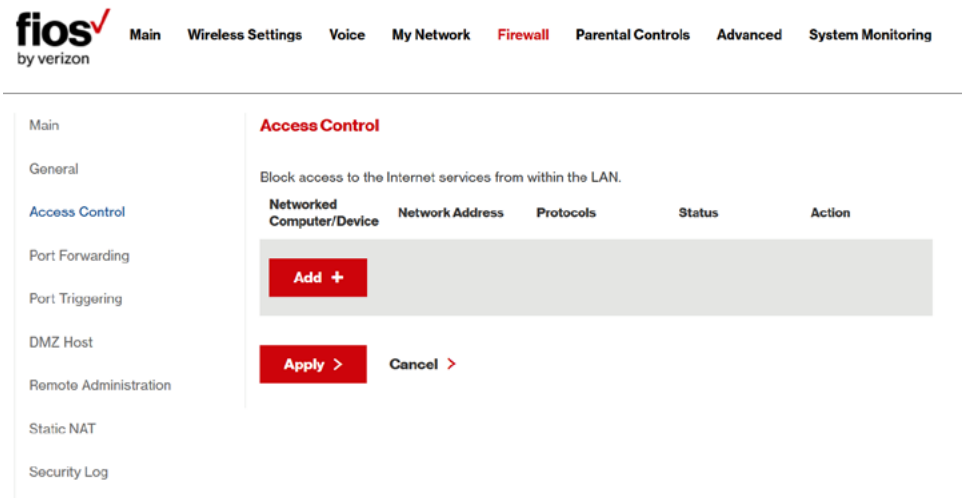
You can block individual computers on your local network from accessing specific services on the Internet. For example, you could block one computer from accessing the Internet, then block a second computer from transferring files using FTP as well as prohibit the computer from receiving incoming email.

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

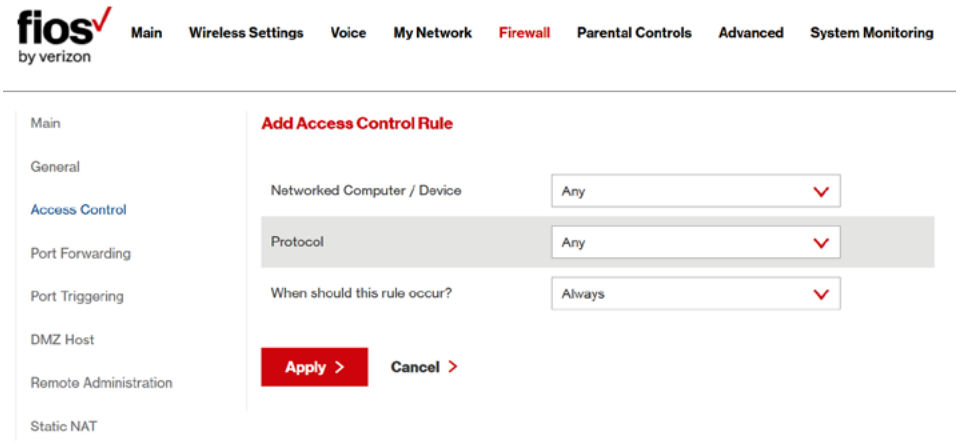
7.1a/ ALLOW OR RESTRICT SERVICES

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:
   - **All networked devices** - select **Any**.
   - **Specific devices only** - select **User Defined**, then click **Add** and create a network object.
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** and click **Add** to create the schedule.
6. Click **Apply** to save changes. 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.

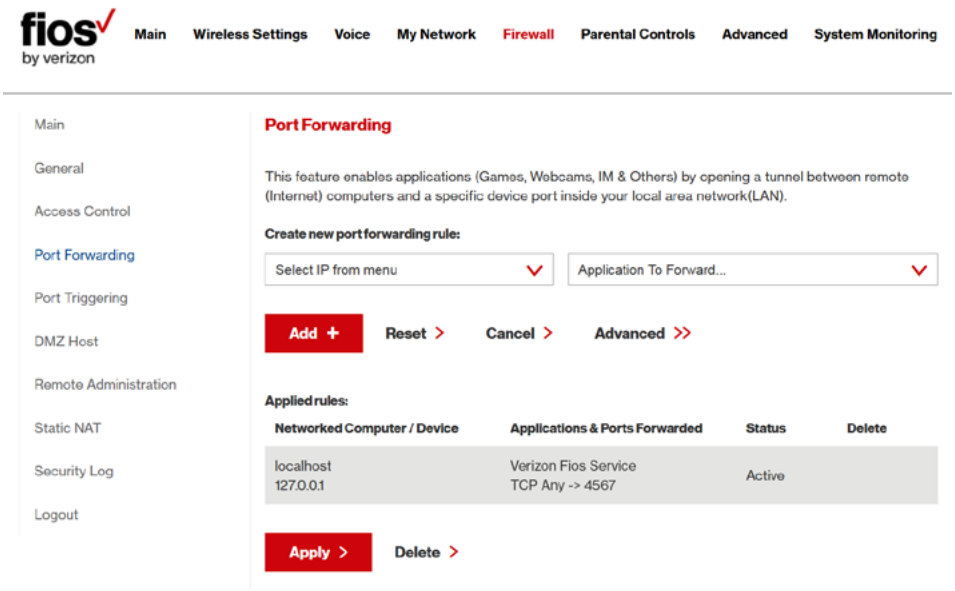
- To disable an access control, clear the check box next to the service name.
- To reinstate the restriction, select the check box next to the service name.
- To remove an access restriction, select the service and click Remove. The service is removed from the Access Control table.

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 gaming 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.



2. To create a new rule, select the IP address in the **Select IP from Menu** drop down.

 |

PORT FORWARDING AND PORT TRIGGERING

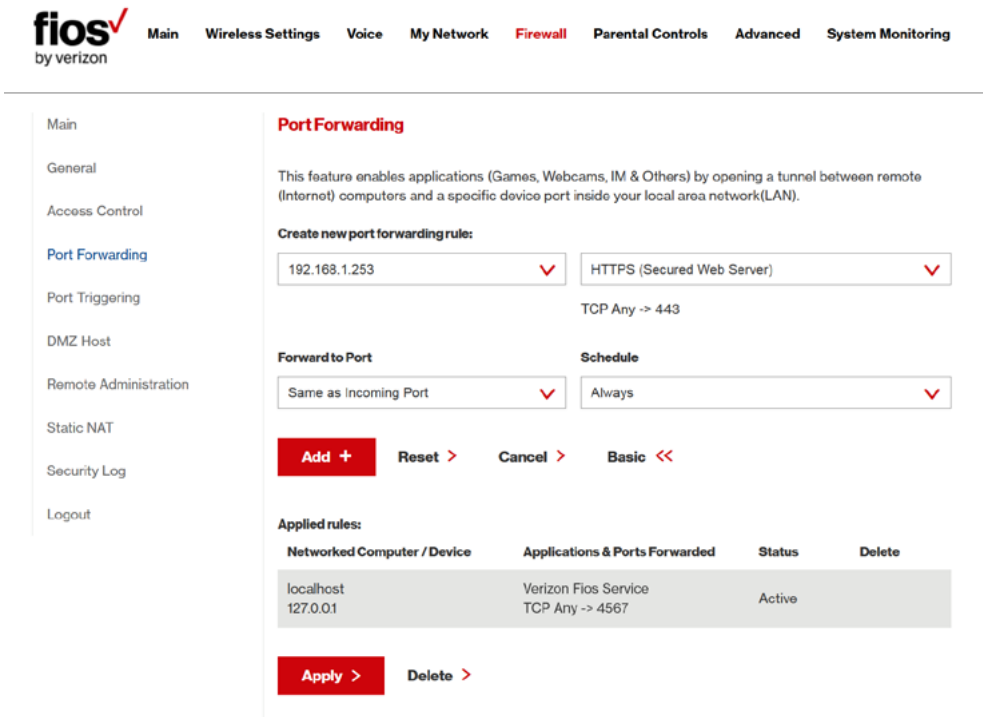
3. Select the application in the **Application to Forward** drop down.
4. Click **Add**. The rule displays in the **Applied Rules** section.
5. Click **Apply** to save changes.

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 **Forward to Port** list box.
3. If a single port or range of ports is selected, a text box displays. Enter 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 gaming server is accessed using UDP protocol on port 2222. The gaming server then responds by connecting the user using UDP on port 3333, when a gaming session is initiated.

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

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

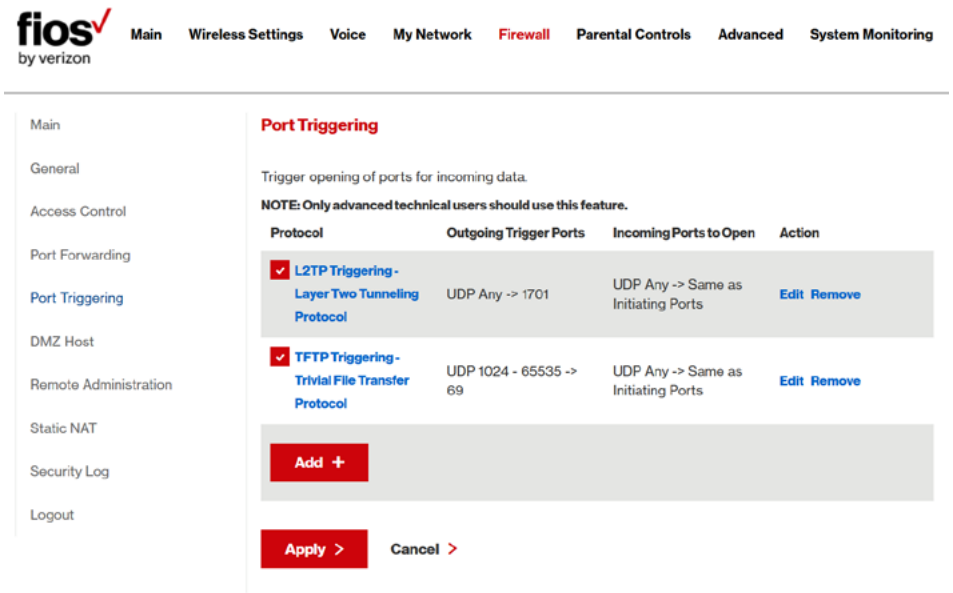
 |

PORT TRIGGERING AND REMOTE ADMINISTRATION

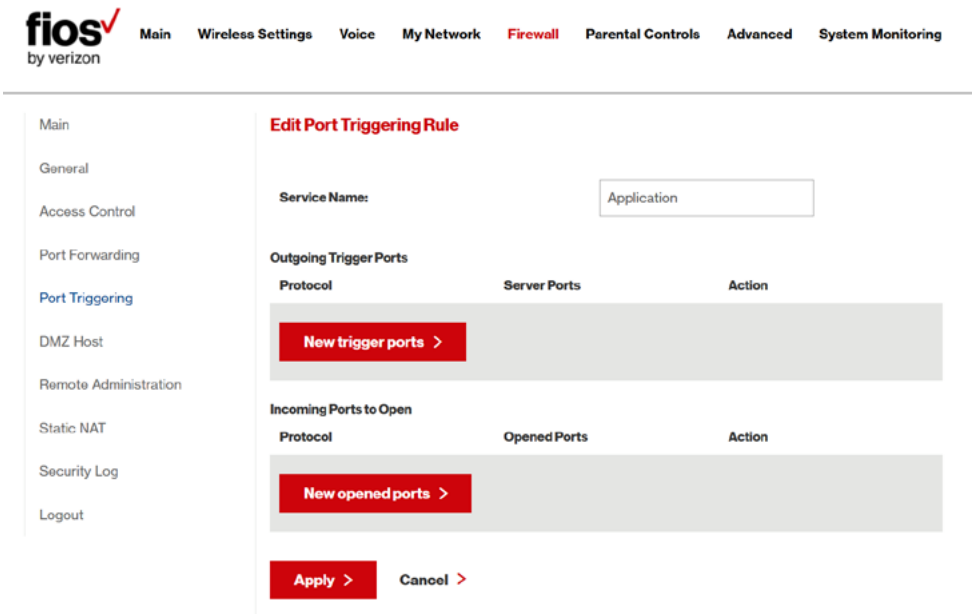
To resolve the conflict, a port triggering entry must be defined, which allows inbound traffic on UDP port 3333 only after a network host generated traffic to UDP port 2222. This results in your Fios Router accepting the inbound traffic from the gaming server and sending it back to the network host which 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 **Apply** to save User Defined changes. The Port Triggering page displays.
4. Click **Apply** again 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 like Internet gaming.

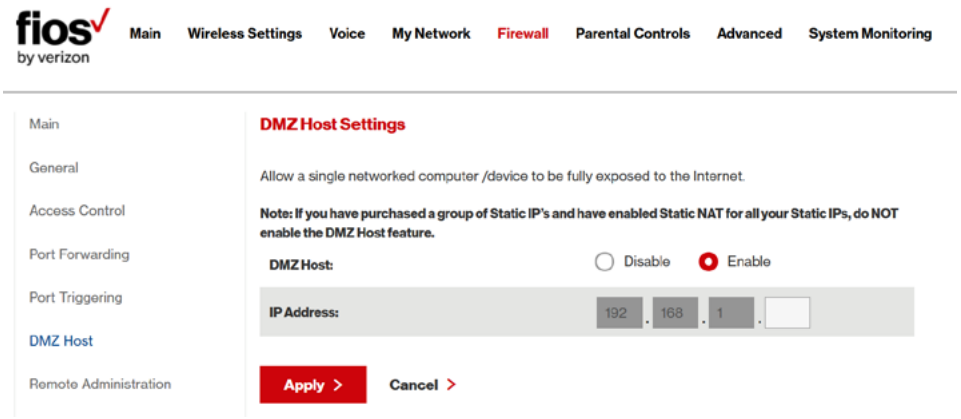
 |

DMZ HOST

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



7.5/ 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:

- **Web Management** - used to obtain access to your Fios Router's GUI 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. Local IP addresses and other settings can also be changed, making it difficult or impossible to access your Fios Router from the local network. Remote administration access to SSH or Web Management services should be activated only when absolutely necessary.

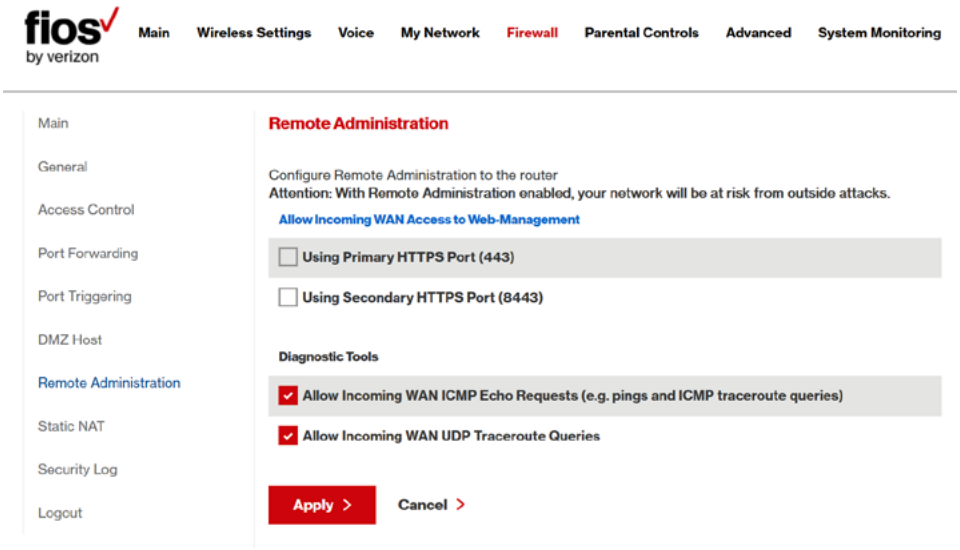
Note: Encrypted remote administration is performed using a secure SSL connection and requires a SSL certificate. When accessing your Fios Router for the first time using encrypted remote administration, a warning page opens with a certificate authentication message displayed. This is due to your Fios Router SSL certificate being self-generated. When this message display under that circumstance, ignore the message and continue. Even though this message displays, the self-generated certificate is safe and provides a secure SSL connection.

 |

REMOTE ADMINISTRATION AND STATIC NAT

To enable remote administration:

1. Select **Remote Administration**.



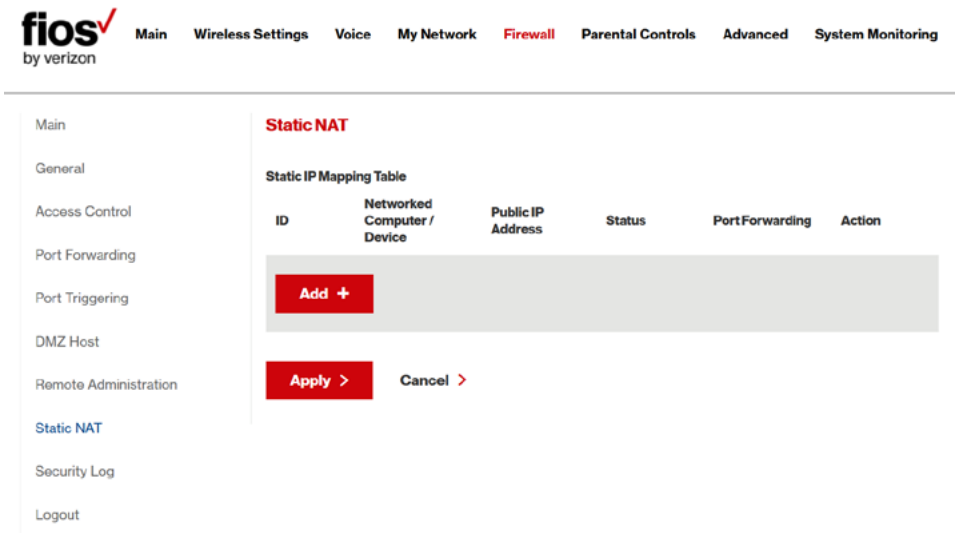
2. To enable access, select the check box.
3. Click **Apply** to save changes.
4. To remove access, clear the check box.
5. Click **Apply** again to save changes.

7.6/ 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:

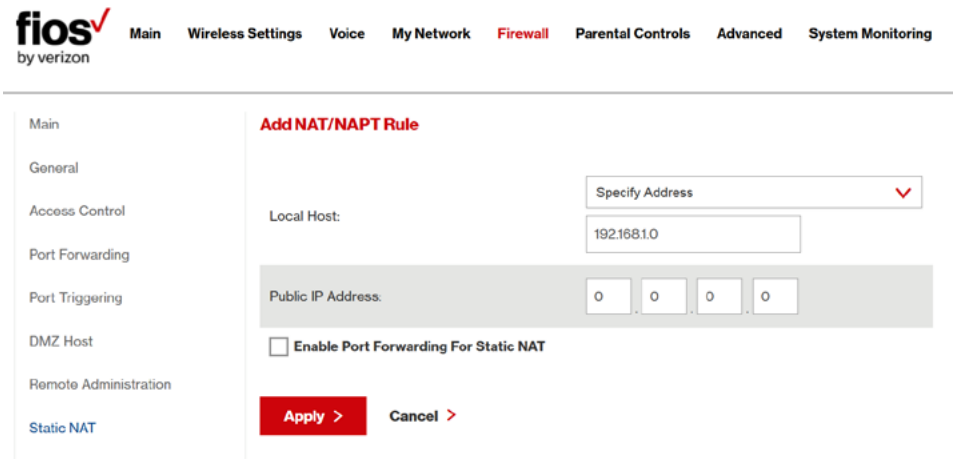
1. Select **Static NAT**.



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

 |

STATIC NAT AND SECURITY LOG



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.

7.7/ SECURITY LOG

You can view events that your firewall has blocked by accessing the security log. Your Fios Router reports events, such as attempts to establish inbound and outbound connections, attempts to authenticate at an administrative interface, such as your Fios Router GUI, firewall configuration, and system start-up.

The security log reports the following information:

- **Time** - based on the date and time in your Fios Router
- **Event Type** - consists of firewall information, firewall setup, and system log
- **Log Level** - describes the event that occurred, such as a fragmented packet or parental controls.
- **Details** - provide a reason the event occurred, such as a packet has been blocked because of parental controls.

You can modify the type of events that display in the security log. This does not modify the event itself. It simply changes the information that displays in the log.

7.7a/ EVENT TYPES

The security log records the following event types:

- **Access control** – a packet has been accepted/blocked due to an access control rule.
- **Advance filter rule** – a packet has been accepted/blocked due to an advanced filter rule.
- **ARP** – an ARP packet has been accepted.
- **AUTH:113 request** - an outbound packet for AUTH protocol has been accepted (for maximum security level).
- **Broadcast/Multicast protection** – a packet with a broadcast/multicast source IP has been blocked.

 |

SECURITY LOG

- **Default policy** – a packet has been accepted/blocked according to the default policy.
- **Defragmentation failed** – the fragment has been stored in memory and blocked until all fragments have arrived and defragmentation can be performed.
- **DHCP request** – your Fios Router sent a DHCP request (depends on the distribution).
- **DHCP response** - your Fios Router sent a DHCP response (depends on the distribution).
- **Echo/Chargen/Quote/Snork protection** – a packet has been blocked due to Echo/Chargen/Quote/Snork protection.
- **Firewall internal** – from the firewall internal mechanism, event type is recorded and an accompanying explanation will be added.
- **Firewall rules were changed** – the rule set has been modified.
- **Firewall status changed** – the firewall status changed from up to down or vice versa, as specified in the event type description.
- **First packet in connection is not a SYN packet** – a packet has been blocked due to a TCP connection that started without a SYN packet.
- **Fragmented packet** – a fragment has been rejected.
- **Fragmented packet, bad align** – a packet has been blocked because, after defragmentation, the packet was badly aligned.
- **Fragmented packet, header too big** – a packet has been blocked because, after defragmentation, the header was too big.

- **Fragmented packet, header too small** – a packet has been blocked because, after defragmentation, the header was too small.
- **Fragmented packet, no memory** – a packet has been blocked because there is no memory for fragments.
- **Fragmented packet, overlapped** – a packet has been blocked because, after defragmentation, there were overlapping fragments.
- **Fragmented packet, packet exceeds** – a packet has been blocked because, after defragmentation, the packet exceeded.
- **Fragmented packet, packet too big** – a packet has been blocked because, after defragmentation, the packet was too big.
- **FTP port request to 3rd party is forbidden** – possible bounce attack – a packet has been blocked.
- **ICMP flood protection** – a broadcast ICMP (Internet Control Message Protocol) flood.
- **ICMP protection** – a broadcast ICMP message has been blocked.
- **ICMP redirect protection** – an ICMP redirected message has been blocked.
- **ICMP replay** – an ICMP replay message has been blocked.
- **Illegal packet options** – the options field in the packet's header is either illegal or forbidden.
- **IP Version 6** – an IPv6 packet has been accepted.

 |