# Verizon

# FiOS Quantum Gateway
# User Guide

**Model FiOS-G1100**

# Contents

# Chapter 1 Introduction

The Verizon FiOS® Quantum Gateway lets you transmit and distribute digital entertainment and information to multiple devices in your home/office. Your Gateway supports networking using coaxial cables, Ethernet, or Wi-Fi, making it one of the most versatile and powerful gateways available.

## Package Content

Your package contains:

- The FiOS Quantum Gateway
- Power adapter
- WAN Ethernet cable (white)
- LAN Ethernet cable (yellow)
- Quick Start Guide
- Installation Guide

## 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

## Features

Your Gateway features include:

- Support for multiple networking standards, including
  - WAN – Gigabit Ethernet and MoCA 2.0 interfaces
  - LAN – 802.11 b/g/n/ac, Gigabit Ethernet and MoCA 2.0 interfaces
- Integrated wired networking with 4-port Ethernet switch and MoCA
  - Ethernet supports speeds up to 1000 Mbps
  - MoCA 2.0 and 1.1 enabled to support speeds up to 700 Mbps over coaxial cable

- Integrated wireless networking with 802.11b/g/n/ac access point featuring:
  - 802.11b enabled to support speeds up to 11 Mbps wirelessly
  - 802.11g enabled to support speeds up to 54 Mbps wirelessly
  - 802.11n enabled to support speeds up to 450 Mbps wirelessly
  - 802.11ac enabled to support speeds up to 1300 Mbps wirelessly
- Enterprise-level security, including:
  - Fully customizable firewall with Stateful Packet Inspection (SPI)
  - Content filtering with URL-keyword based filtering, parental control, 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
  - Intrusion detection
  - MAC address filtering
  - Static NAT
  - Port forwarding
  - Port triggering
  - Access control
  - Advanced wireless protection featuring WPA2/~~, ~~WPA~~2~~ Mixed Mode, WEP 64/128 bit encryption, and MAC address filtering
  - ICSA certification
- Options, including:
  - DHCP server
  - WAN interface auto-detection
  - 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
  - Remote management and secured remote management using HTTPS
  - Static routing
  - Time zone support

- VPN (VPN pass through only)
- Port forwarding rules
- IGMP proxy
- Security logging of multiple event types
- Daylight savings time support

## Getting to Know your Gateway

### Front Panel

The front panel has two lighted indicators and a WPS (Wi-Fi Protected Setup) button.

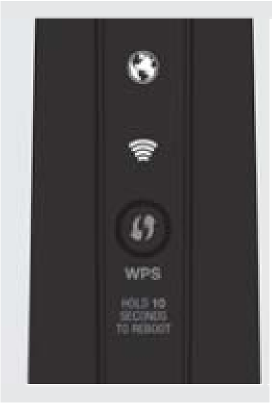
The Power/Internet light will be on and solid when your Gateway is turned on, connected to the Internet, and functioning normally.

The Wireless light will be on when your Gateway Wi-Fi is turned on.

For additional information on the front lights and error indications, refer the **Troubleshooting** section in this Guide.

The WPS button is used to initiate Wi-Fi Protected Setup. This is an easy way to add WPS capable devices to your wireless network.

When WPS is initiated from your Gateway, the wireless light slowly flashes white for up to two minutes, allowing time to complete the WPS pairing process on your wireless client device.



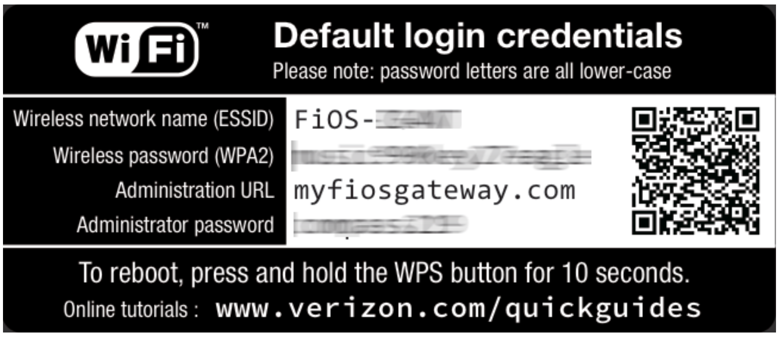
When a device begins connecting to your Gateway using WPS, the wireless light rapidly flashes white for a few seconds, then turns solid white as the connection completes.

If there is an error during the WPS pairing process, the wireless light flashes red rapidly for two minutes after the error occurs.

The WPS button can also be used to reboot the router. To perform a soft reboot, press and hold the WPS button for at least 10 seconds.

**Side Panel**

The side panel of your Gateway has a label that contains important information about your device, including the default settings for the Gateway's wireless network name (ESSID), wireless password (WPA2 key), local URL for accessing the Gateway's administrative pages, and Gateway administrator password.



**Default login credentials**

Please note: password letters are all lower-case

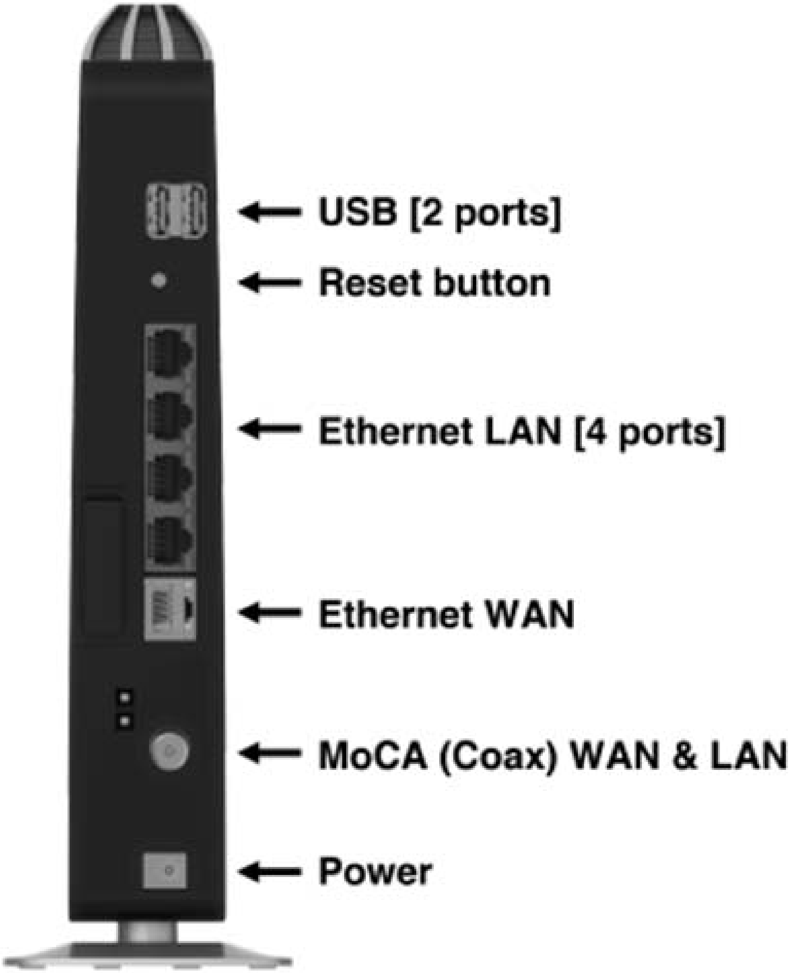
|  |  |
|---|---|
| Wireless network name (ESSID) | FiOS-[redacted] |
| Wireless password (WPA2) | [redacted] |
| Administration URL | myfiosgateway.com |
| Administrator password | [redacted] |

To reboot, press and hold the WPS button for 10 seconds.

Online tutorials : www.verizon.com/quickguides

**Rear Panel**

The rear panel of your Gateway has 8 ports; MoCA (COAX), Ethernet LAN [4], Ethernet WAN, and USB [2]. The rear panel also includes a DC power jack and a reset button.



- **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.
- **Reset button** – allows you to reset your Gateway to the factory default settings. To reset the Gateway, press and hold the Reset button for at least three seconds.
- **Ethernet LAN** – connects devices to your Gateway 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 Gateway to the Internet using an Ethernet cable.
- **MoCA (COAX) WAN and LAN** – connects your Gateway 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.
- **Power** – connects your Gateway to an electrical wall outlet using the supplied power adapter.

## Mount Gateway to Wall Option

For optimum performance, the FiOS Quantum Gateway is designed to stand in a vertical upright position. Verizon does not recommend wall mounting the FiOS Quantum Gateway. However, if you wish to mount your Gateway, 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 mounting screws will fit the existing bracket.

To mount your Gateway to a wall:

1. Remove the foot by turning the Gateway upside down and removing the single screw that holds the foot to the Gateway.
2. Slide the foot toward the front of the Gateway and pull the foot from the holes. You may need to wiggle the foot slightly.
3. You may use the wall mount bracket as a template for positioning the Gateway.
4. Mark the mounting holes, then remove the wall mount bracket from the wall.
5. Drill holes for the screw anchors.
6. Insert the screws in the screw anchors, then insert the screw anchors in the holes. Leave screws extended about 0.2 inches from the wall.
7. Verify the screws are positioned correctly by placing the wall bracket on the screws. Remove the wall bracket from the wall.

8. Place the Gateway on the wall bracket and slide the Gateway forward until it locks in place.
9. To secure the Gateway, attach the bracket to the Gateway using the single screw you removed from the foot.
10. Slide the wall mount bracket with the attached Gateway on the screws, then slide the bracket down until it locks in place.

# Chapter 2 Connecting your Gateway

Connecting your Gateway 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.

## Setting Up your Gateway

There are three basic steps to setting up your Gateway:

**Step 1**: Connect your Gateway to the Internet

**Step 2:** Connect your network device to your Gateway

**Step 3:** Configure your Gateway

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

### Step 1: Connect your Gateway

1. Remove your Gateway, Ethernet cables, and power adapter from the box.
2. Locate your high-speed Internet (WAN) outlet. This would be the wall jack installed previously by Verizon. Note the type of jack may be either Ethernet or coaxial.
3. Connect your Gateway to the Internet (WAN).

   a. If connecting the WAN using Ethernet, use the supplied white Ethernet cable and plug one end into the white Ethernet WAN port on the back of your Gateway. Plug the other end of the cable into the high-speed Ethernet wall jack.

   b. If connecting the WAN using coaxial cable, locate a coaxial cable and connect one end to the coax port on the back of your Gateway. Connect the other end of the coaxial cable to a coax wall jack.

   Tighten the coaxial cables by hand until snug. The cables should not require a wrench.
4. Plug the power cord into the power port on the back of your Gateway and then into a power outlet. The Gateway automatically turns on as soon as power is plugged in.

*__IMPORTANT:__ Wait until the Power/Internet light on the front of the Gateway stops flashing and is solid white. If after several minutes it is still not solidly lit, check the troubleshooting steps in the **Troubleshooting** section of the user guide.*

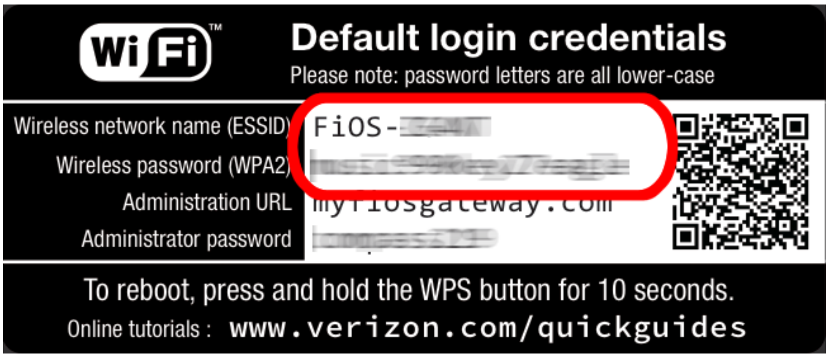
## Step 2: Connect Your Device to your Gateway

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

- Plug one end of the supplied yellow Ethernet cable into one of the four yellow Ethernet ports in the back of your Gateway.
- Plug the other end of the yellow Ethernet cable into the Ethernet port of your network device.

If connecting a wireless device using the wireless network:

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



Default login credentials

Please note: password letters are all lower-case

Wireless network name (ESSID) FiOS-[redacted]

Wireless password (WPA2) [redacted]

Administration URL myfiosgateway.com

Administrator password [redacted]

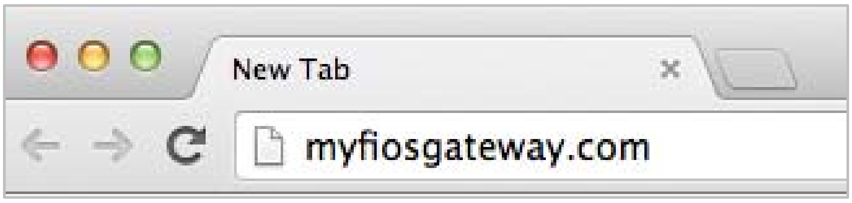
To reboot, press and hold the WPS button for 10 seconds.

Online tutorials : www.verizon.com/quickguides

## Step 3: Configure your Gateway

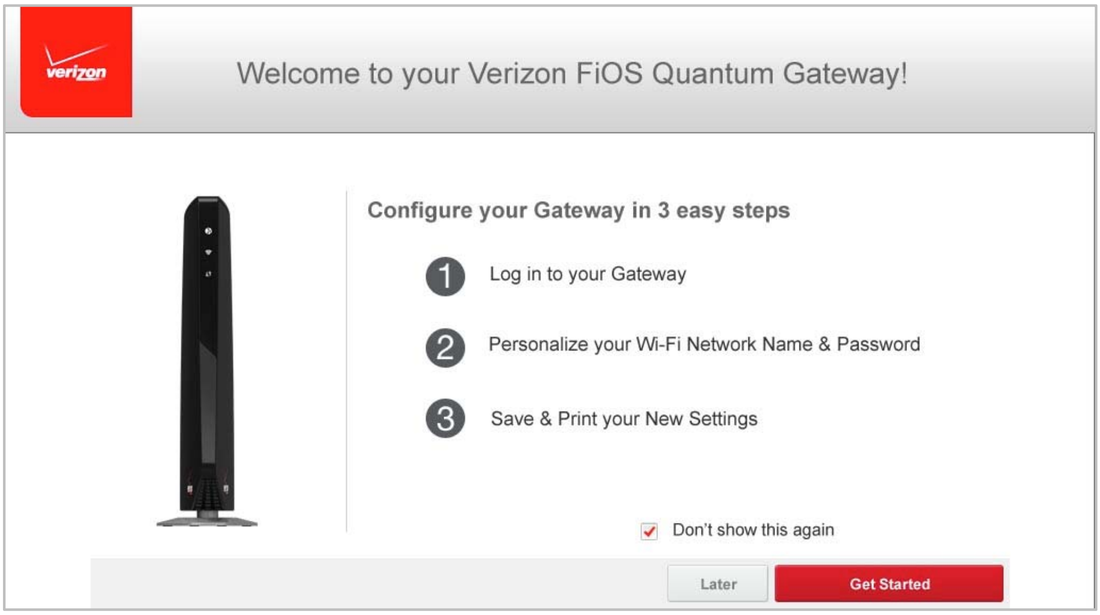
1. Open a web browser on the device connected to your Gateway network.
2. In the browser address field (URL), enter: **myfiosgateway.com**, then press the **Enter** key on your keyboard.

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



myfiosgateway.com

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



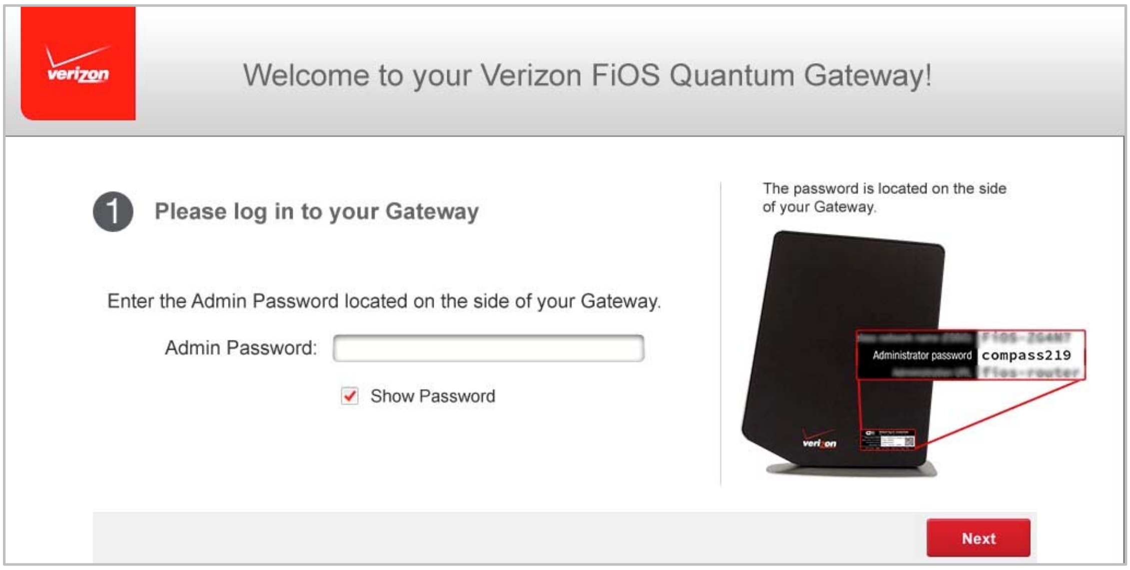
Welcome to your Verizon FiOS Quantum Gateway!

Configure your Gateway in 3 easy steps

1. Log in to your Gateway
2. Personalize your Wi-Fi Network Name & Password
3. Save & Print your New Settings

☑ Don't show this again

3. Click the **Get Started** button. The Gateway Login screen displays.



Welcome to your Verizon FiOS Quantum Gateway!

1 Please log in to your Gateway

Enter the Admin Password located on the side of your Gateway.

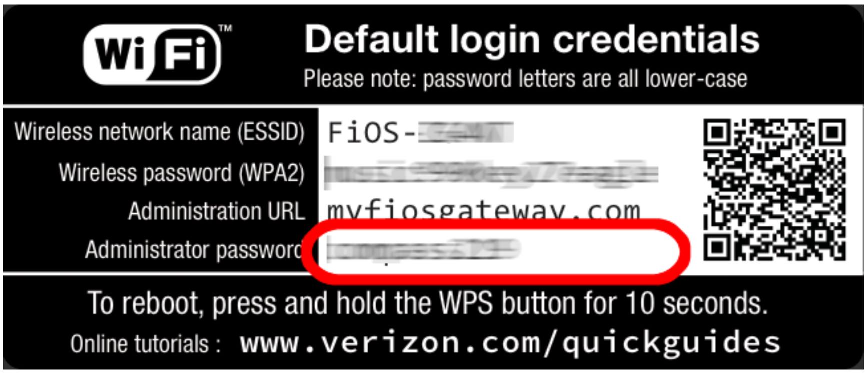
Admin Password:

☑ Show Password

The password is located on the side of your Gateway.

Administrator password compass219

4. In the **Admin Password** field, enter the password that is printed next to the Administrator Password on the label on the side of your Gateway.



**Default login credentials**

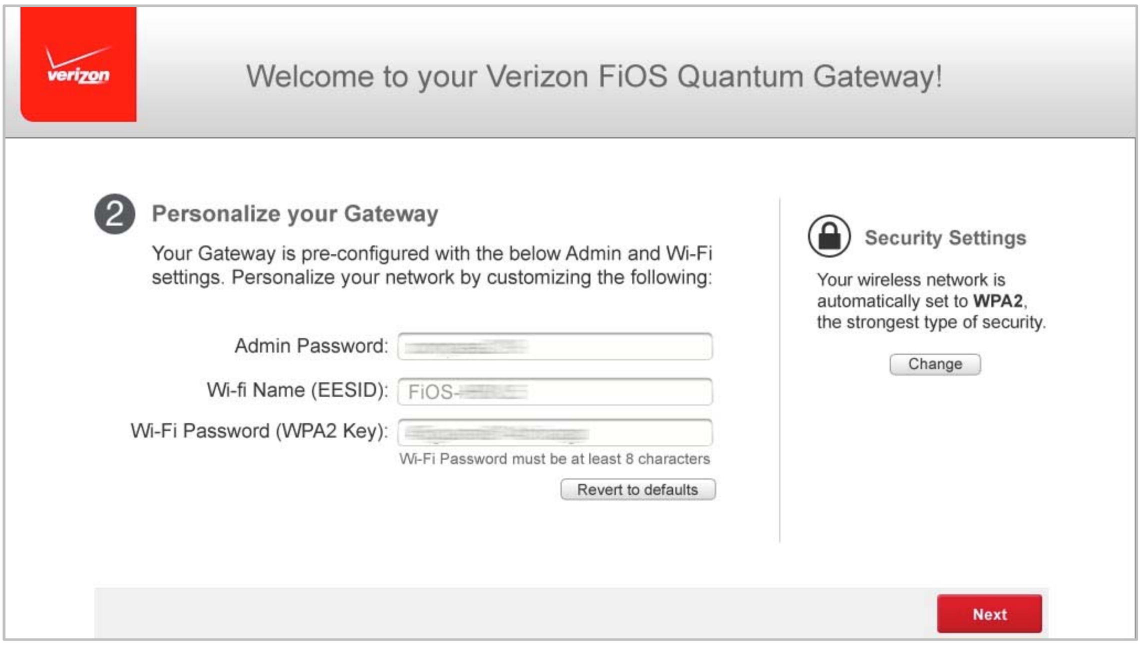
Please note: password letters are all lower-case

| | |
|---|---|
| Wireless network name (ESSID) | FiOS-[redacted] |
| Wireless password (WPA2) | [redacted] |
| Administration URL | myfiosgateway.com |
| Administrator password | [redacted] |

To reboot, press and hold the WPS button for 10 seconds.

Online tutorials : www.verizon.com/quickguides

5. Click **Next**. The Personalize your Gateway screen displays.



Welcome to your Verizon FiOS Quantum Gateway!

2 **Personalize your Gateway**

Your Gateway is pre-configured with the below Admin and Wi-Fi settings. Personalize your network by customizing the following:

Admin Password: [redacted]

Wi-fi Name (EESID): FiOS-[redacted]

Wi-Fi Password (WPA2 Key): [redacted]

Wi-Fi Password must be at least 8 characters

**Security Settings**

Your wireless network is automatically set to **WPA2**, the strongest type of security.

For your protection, your Gateway 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.

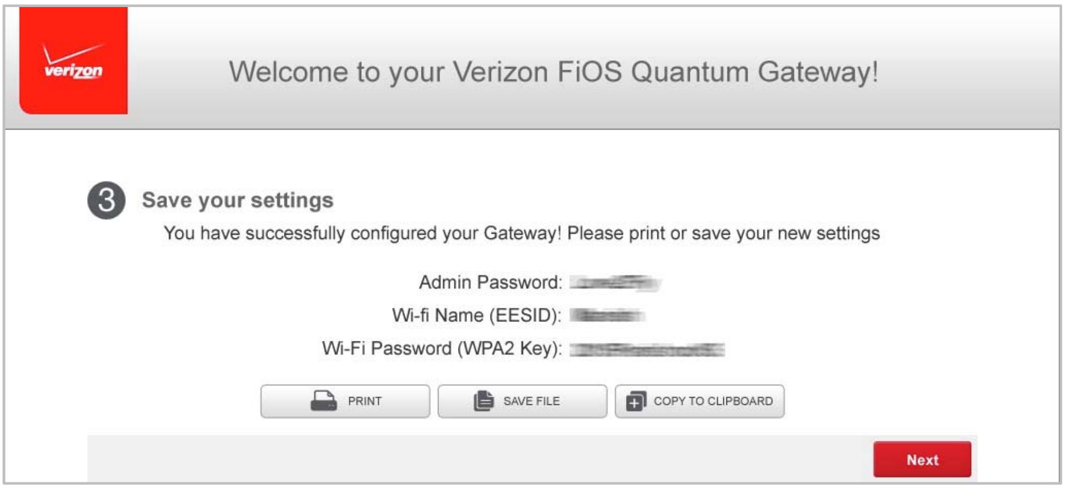
If you have an old wireless device that does not support WPA2, click the **Change** button below the **Lock** icon. This allows you to change the security type to the backwards-compatible ~~the older, less secure~~ WPA2/WPA mixed mode or WEP encryption, or you can disable wireless security entirely by toggling the WEP option on, then off.

**WARNING:** WEP provides a low level of security and is not recommended. The WEP security setting will drop your Gateway's wireless speed performance from a maximum data rate of 450 Mbps to a maximum data rate of 54 Mbps.

6. Click **Next** to continue and save the Admin and Wi-Fi changes to your Gateway.

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

7. Save your settings. Once you have personalized your Gateway settings, you will be prompted to save a record of these settings in case you forget them. You have the option to print or save them to a file and save the file on your device.



Welcome to your Verizon FiOS Quantum Gateway!

3 Save your settings

You have successfully configured your Gateway! Please print or save your new settings

Admin Password: [redacted]

Wi-fi Name (EESID): [redacted]

Wi-Fi Password (WPA2 Key): [redacted]

8. Click **Next** to continue. Your Gateway verifies the final settings and displays that it is successfully connected to the Internet and is ready for use.

Upon the successful completion of setup, the Main screen of the Gateway displays. Your Gateway is now configured. You can change any of the Gateway settings after this initial log in.

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

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

## 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.

### Configuring Dynamic IP Addressing

➢ To configure a computer to use dynamic IP addressing:

**Windows 7**

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.

**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.

## Connecting Other Computers and Network Devices

You can connect your Gateway to other computers or set top boxes using an Ethernet cable, wireless 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 Gateway.
2. Plug the other end of the Ethernet cable into an Ethernet port on the computer.
3. Repeat these steps for each computer to be connected to your Gateway using Ethernet. You can connect up to four.

**Wireless 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 Gateway creates a secure wireless network.

In most cases, this only requires the pressing of a few buttons – one on your Gateway 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.

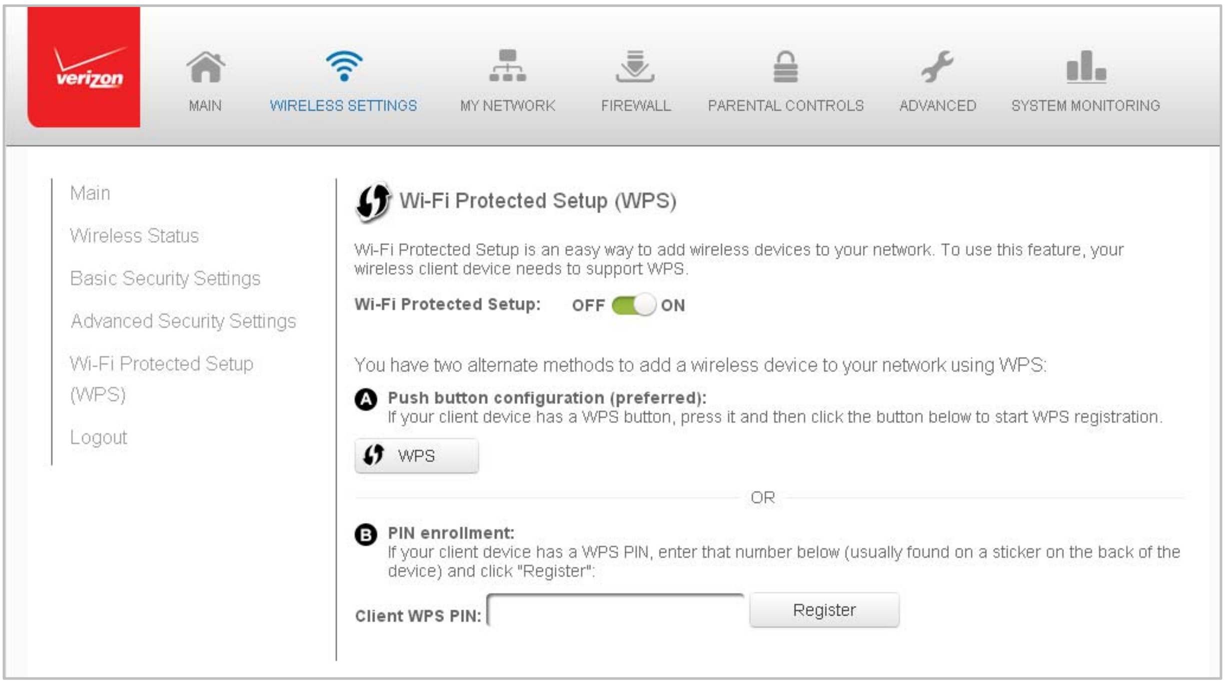
To initialize the WPS process, you can either press and release the WPS button located on the front of your Gateway or use the GUI and press the on-screen button.

If you press the WPS button on your Gateway and change your mind, you can cancel the WPS process by pressing the button a second time.

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)**.



Wi-Fi Protected Setup (WPS)

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

**Wi-Fi Protected Setup:** OFF ● ON

You have two alternate methods to add a wireless device to your network using WPS:

**A Push button configuration (preferred):** If your client device has a WPS button, press it and then click the button below to start WPS registration.

**B PIN enrollment:** If your client device has a WPS PIN, enter that number below (usually found on a sticker on the back of the device) and click "Register":

**Client WPS PIN:**

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 WPS button on your Gateway, then click the WPS button on your wireless 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**.
4. After initializing WPS on your Gateway, you have two minutes to press the WPS button on the client device before the WPS session times out.

   When the WPS button on your Gateway is pressed, the Wireless light on the front of your Gateway begins flashing white. 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 Gateway flashes red for two minutes to indicate the WPS pairing process was unsuccessful. After flashing red, the light returns to solid white to indicate that Wi-Fi is on.

**Wireless using Manual Configuration**

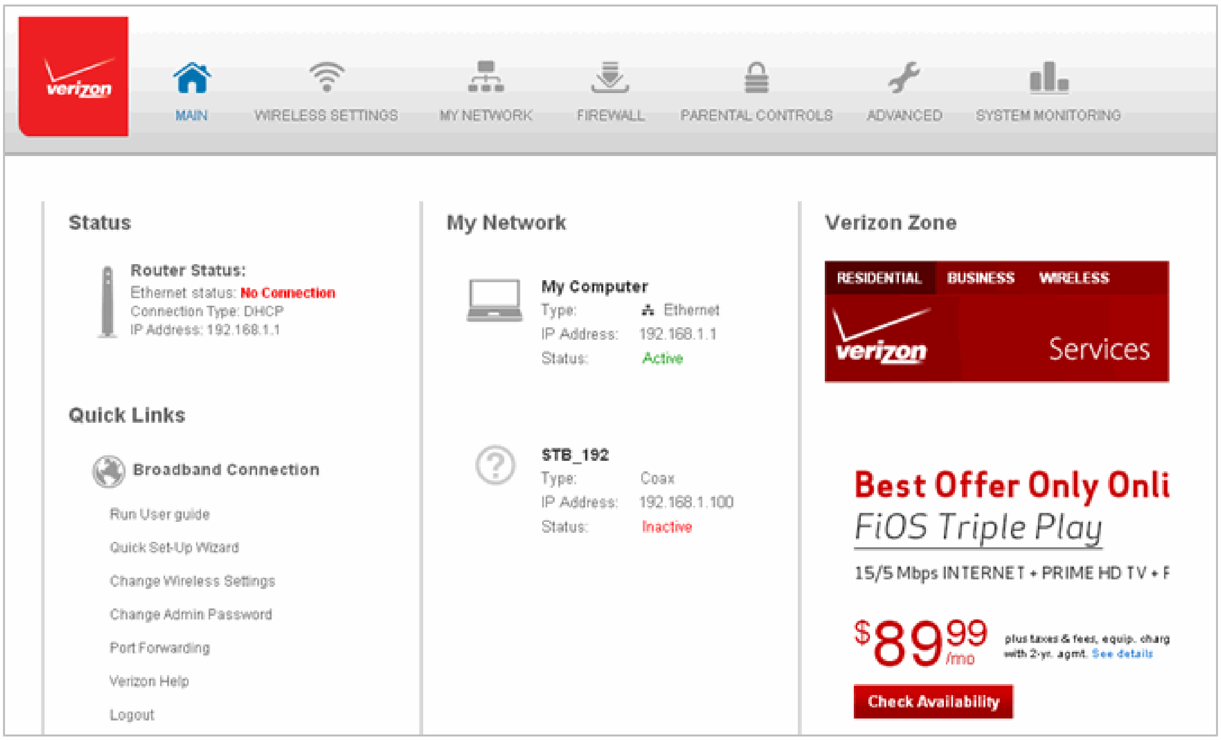
1. Verify each device that you are connecting wirelessly (using Wi-Fi) has a built-in wireless or external wireless adapter.
2. Open the device’s wireless settings application.
3. Select your Gateway’s wireless network name (SSID) from the device’s list of discovered wireless networks.
4. Enter your Gateway’s wireless password (WPA2 key) into the device’s wireless settings. Your Gateway’s default wireless network name and wireless password are located are on the sticker on the side of your Gateway.
5. Verify the changes were implemented by using the device’s web browser to access a site on the Internet.
6. Repeat these steps for every device that you are wirelessly connecting to your Gateway.

**Coaxial**

1. Verify all coax devices are turned off.
2. Disconnect any adapter currently connected to the coaxial wall jack in the room where your Gateway 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.

## Main Screen

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



Status

Router Status:
Ethernet status: No Connection
Connection Type: DHCP
IP Address: 192.168.1.1

Quick Links

Broadband Connection

Run User guide
Quick Set-Up Wizard
Change Wireless Settings
Change Admin Password
Port Forwarding
Verizon Help
Logout

My Network

My Computer
Type: Ethernet
IP Address: 192.168.1.1
Status: Active

STB_192
Type: Coax
IP Address: 192.168.1.100
Status: Inactive

Verizon Zone

Best Offer Only Onli
FiOS Triple Play
15/5 Mbps INTERNET + PRIME HD TV + F
$89.99 /mo plus taxes & fees, equip. charg with 2-yr. agmt. See details

## Menu

The Main menu contains links to the following configuration options and chapters:

- **Wireless Settings** – Chapter 3
- **My Network** – Chapter 5
- **Firewall Settings** – Chapter 6
- **Parental Controls** – Chapter 7
- **Advanced** – Chapter 8
- **System Monitoring** – Chapter 9

## Status

This section displays the status of your Gateway’s local network (LAN) and Internet connection (WAN).

### Broadband Connection

Broadband Connection displays the state of the broadband connection:

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

### Quick Links

Quick Links contain links to frequently accessed documentation, such as User Guide, Quick Setup Wizard, and Verizon Help, and links to settings, such as Change Wireless Settings, Change Admin Password, and Port Forwarding, as well as Logout to logout of your Gateway’s GUI.

### 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.

# Chapter 3 Wireless Settings

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.

## Overview

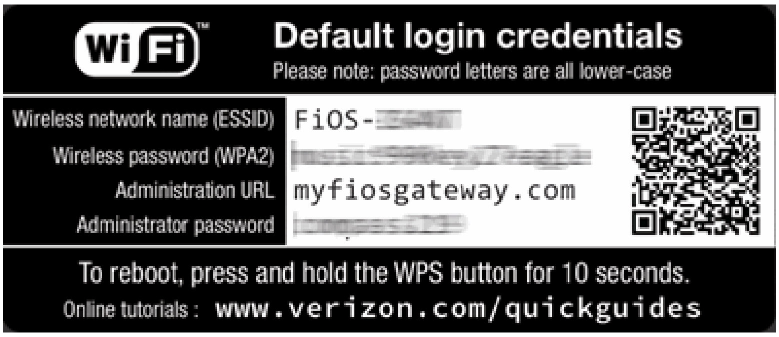
Your Gateway provides you with wireless connectivity using the 802.11b, g, n, or ac standards. These are the most common wireless standards.

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 side of your Gateway.



Default login credentials

Please note: password letters are all lower-case

| | |
|---|---|
| Wireless network name (ESSID) | FiOS-[redacted] |
| Wireless password (WPA2) | [redacted] |
| Administration URL | myfiosgateway.com |
| Administrator password | [redacted] |

To reboot, press and hold the WPS button for 10 seconds.

Online tutorials : www.verizon.com/quickguides

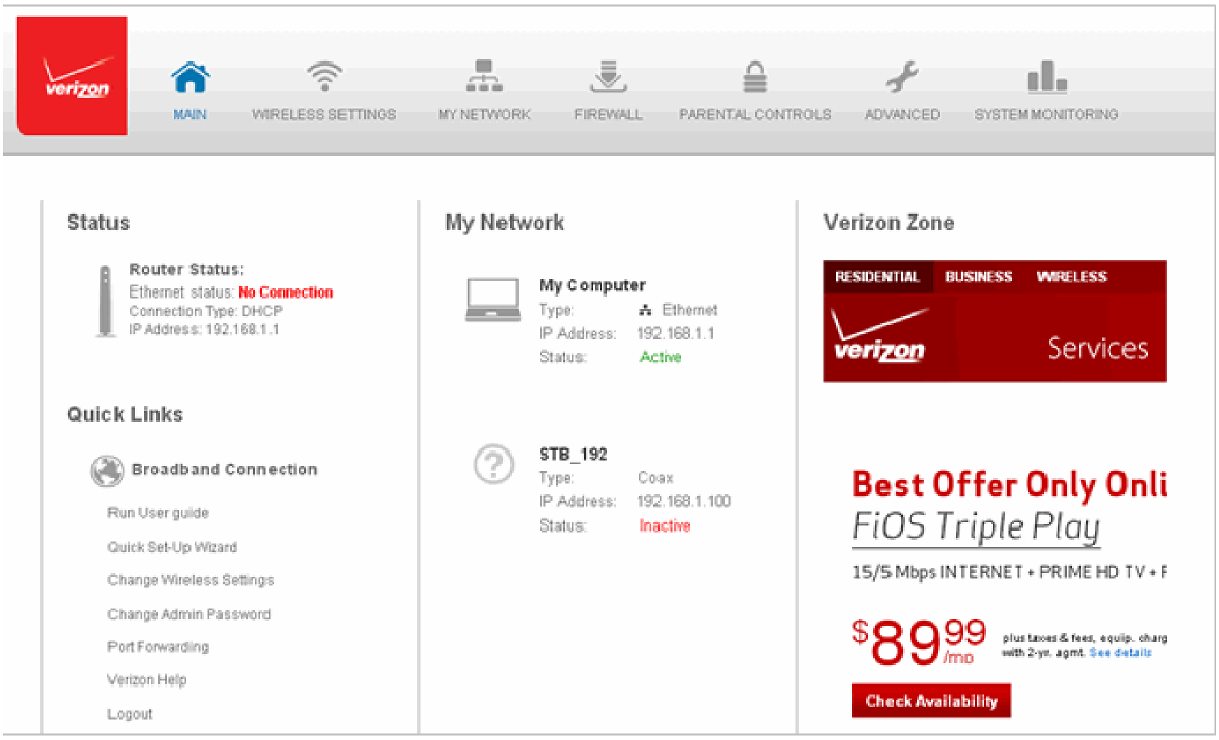
Your Gateway integrates multiple layers of security. These include Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA and WPA2), and firewall.

## Wireless Status

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

➢ To view the status:

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



Status

Router Status:
Ethernet status: No Connection
Connection Type: DHCP
IP Address: 192.168.1.1

Quick Links

Broadband Connection
Run User guide
Quick Set-Up Wizard
Change Wireless Settings
Change Admin Password
Port Forwarding
Verizon Help
Logout

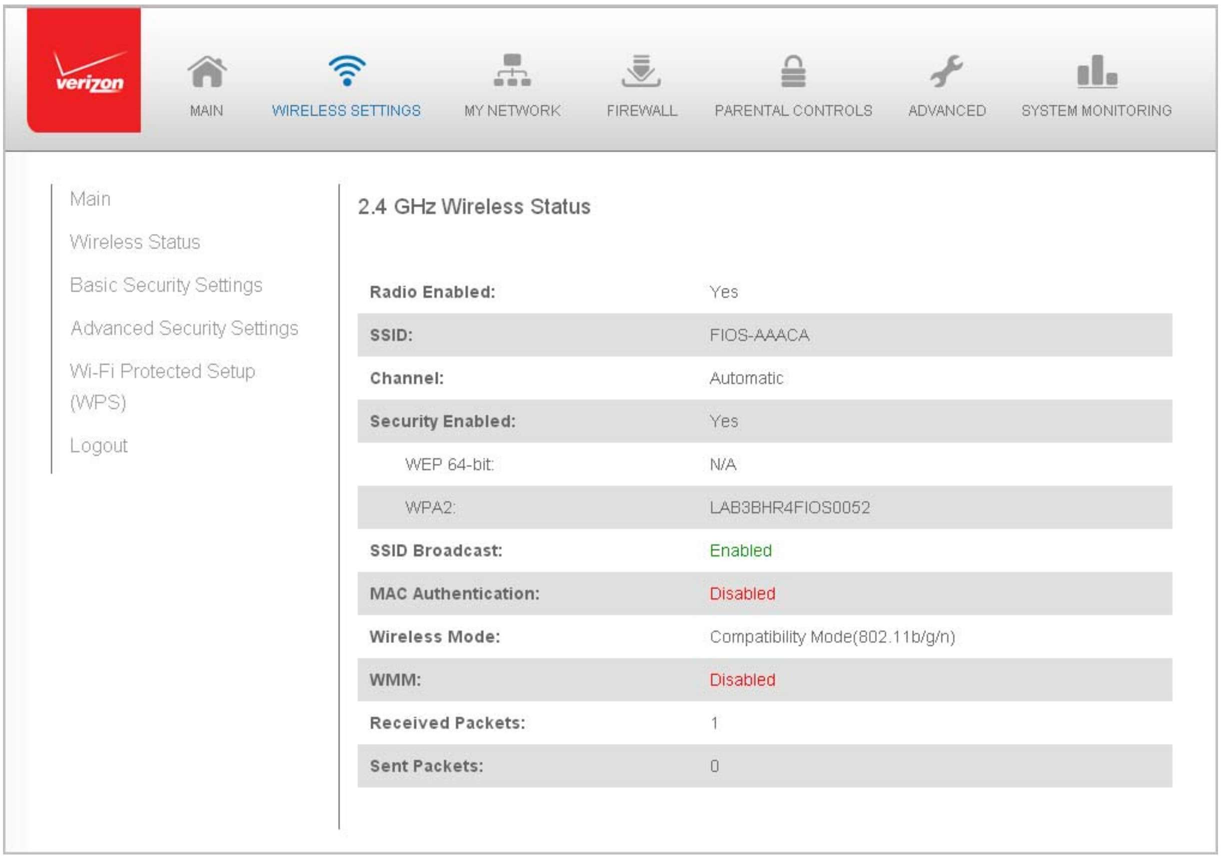
My Network

My Computer
Type: Ethernet
IP Address: 192.168.1.1
Status: Active

STB_192
Type: Coax
IP Address: 192.168.1.100
Status: Inactive

Verizon Zone

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



2.4 GHz Wireless Status

| | |
|---|---|
| **Radio Enabled:** | Yes |
| **SSID:** | FIOS-AAACA |
| **Channel:** | Automatic |
| **Security Enabled:** | Yes |
| WEP 64-bit: | N/A |
| WPA2: | LAB3BHR4FIOS0052 |
| **SSID Broadcast:** | Enabled |
| **MAC Authentication:** | Disabled |
| **Wireless Mode:** | Compatibility Mode(802.11b/g/n) |
| **WMM:** | Disabled |
| **Received Packets:** | 1 |
| **Sent Packets:** | 0 |

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.
   - **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 Gateway is broadcasting its SSID. If activated, the SSID of your Gateway 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 Gateway 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 whether WMM is enabled on your Gateway.
- **Packets Received/Sent** – displays the number of packets received and sent since the wireless capability was activated.

## Basic Security Settings

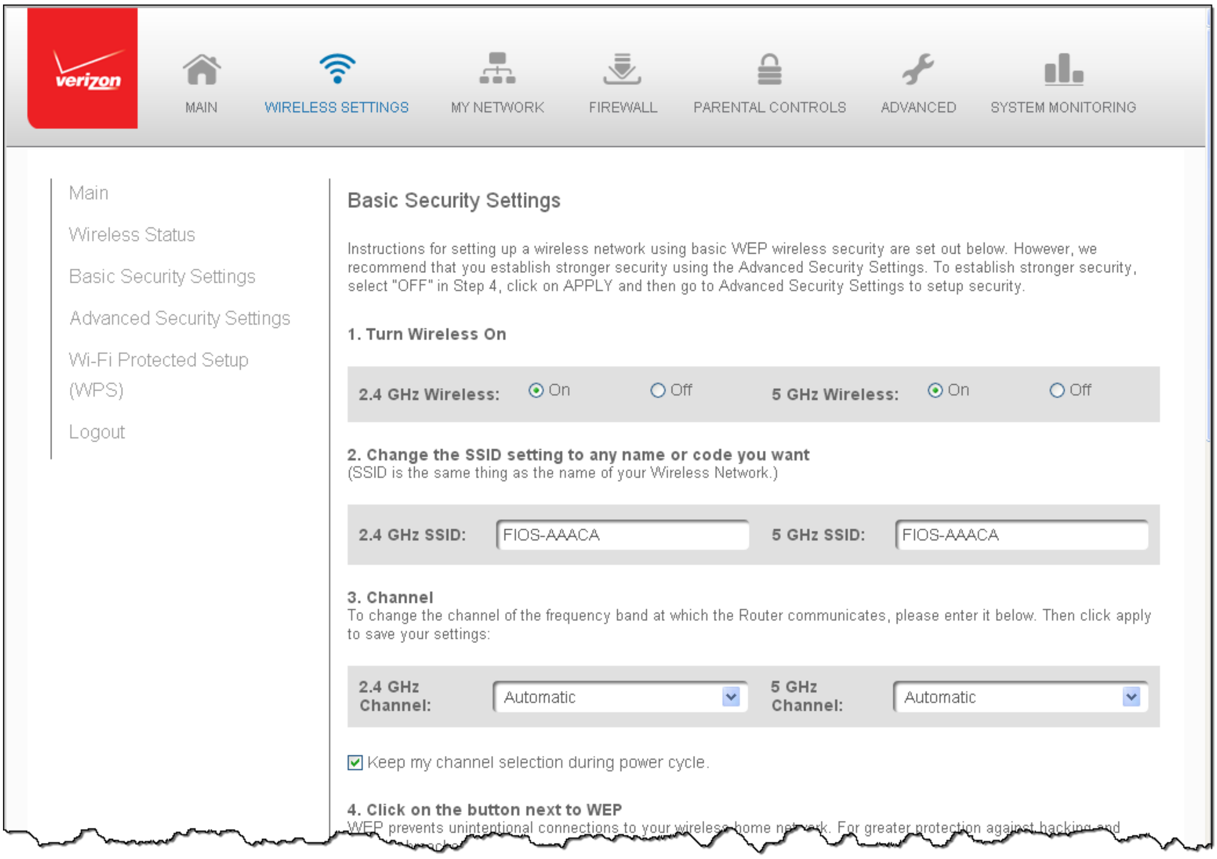
You can configure the basic security settings for your Gateway’s wireless network.

**Note:** Your Gateway’s recommended wireless security encryption is set to WPA2. This is the factory default.

This section explains how to activate WEP (Wired Equivalent Privacy) wireless security. WEP is a significantly less robust security compared to WPA or WPA2 and is not recommended. To set up WPA2 wireless security, refer to the WPA2 section.

➢ To configure basic security to WEP:

1. On the Wireless Settings page, select **Basic Security Settings**.



Basic Security Settings

Instructions for setting up a wireless network using basic WEP wireless security are set out below. However, we recommend that you establish stronger security using the Advanced Security Settings. To establish stronger security, select "OFF" in Step 4, click on APPLY and then go to Advanced Security Settings to setup security.

**1. Turn Wireless On**

| | | | | | |
|---|---|---|---|---|---|
| **2.4 GHz Wireless:** | ● On | ○ Off | **5 GHz Wireless:** | ● On | ○ Off |

**2. Change the SSID setting to any name or code you want**
(SSID is the same thing as the name of your Wireless Network.)

| | | | |
|---|---|---|---|
| **2.4 GHz SSID:** | FIOS-AAACA | **5 GHz SSID:** | FIOS-AAACA |

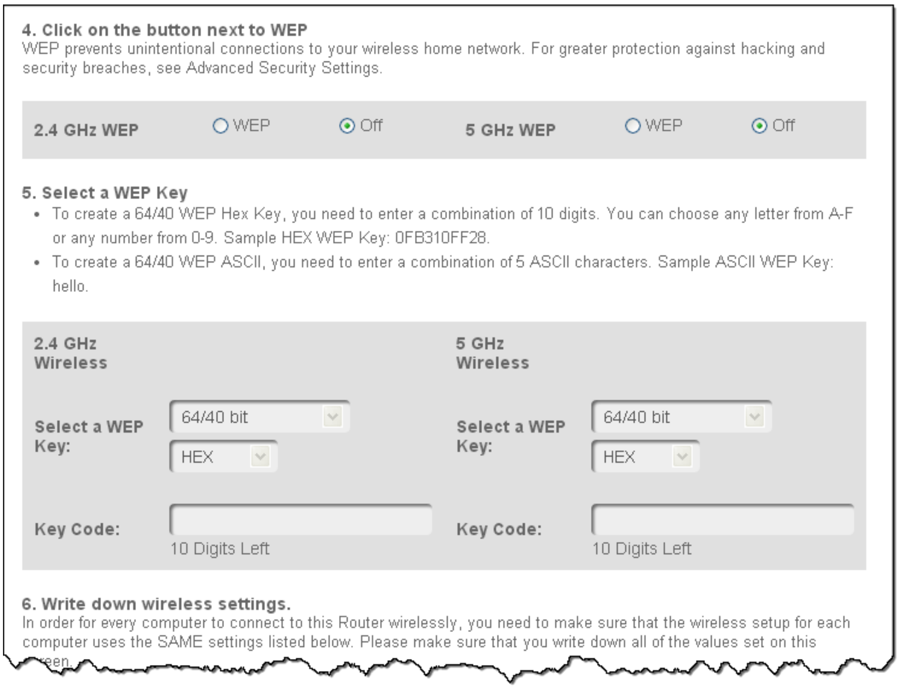
**3. Channel**
To change the channel of the frequency band at which the Router communicates, please enter it below. Then click apply to save your settings:

| | | | |
|---|---|---|---|
| **2.4 GHz Channel:** | Automatic | **5 GHz Channel:** | Automatic |

☑ Keep my channel selection during power cycle.

**4. Click on the button next to WEP**
WEP prevents unintentional connections to your wireless home network. For greater protection against hacking and

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 channel, then select the K**eep my channel selection during power cycle** check box to save your channel selection when your Gateway is rebooted.



**4. Click on the button next to WEP**

WEP prevents unintentional connections to your wireless home network. For greater protection against hacking and security breaches, see Advanced Security Settings.

**2.4 GHz WEP** ○ WEP ◉ Off **5 GHz WEP** ○ WEP ◉ Off

**5. Select a WEP Key**

- To create a 64/40 WEP Hex Key, you need to enter a combination of 10 digits. You can choose any letter from A-F or any number from 0-9. Sample HEX WEP Key: 0FB310FF28.
- To create a 64/40 WEP ASCII, you need to enter a combination of 5 ASCII characters. Sample ASCII WEP Key: hello.

| | | | |
|---|---|---|---|
| **2.4 GHz Wireless** | | **5 GHz Wireless** | |
| **Select a WEP Key:** | 64/40 bit<br>HEX | **Select a WEP Key:** | 64/40 bit<br>HEX |
| **Key Code:** | 10 Digits Left | **Key Code:** | 10 Digits Left |

**6. Write down wireless settings.**

In order for every computer to connect to this Router wirelessly, you need to make sure that the wireless setup for each computer uses the SAME settings listed below. Please make sure that you write down all of the values set on this reen.

5. To active WEP (Wired Equivalent Privacy) security, click the **WEP** radio button.
6. Select a WEP security level as 64/40 bit or 128/104 bit.
7. Enter the key code. If using a HEX key, each character must be a letter from A to F or a number from 0 to 9. If the key is ASCII, each character can be either any ASCII or alphanumeric character.

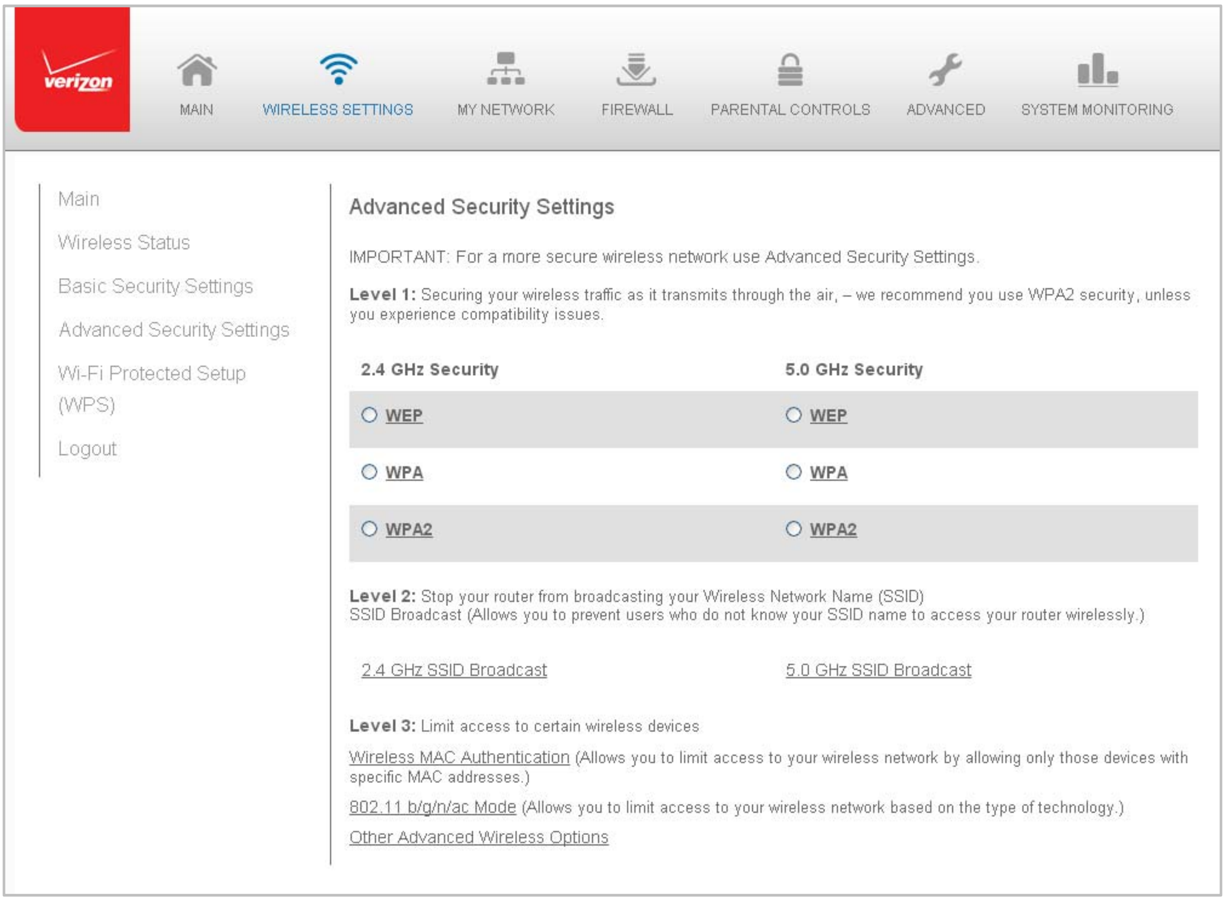
   If using 64/40 bit, enter 10 HEX or 5 ASCII/alphanumeric characters. If 128/104, enter 26 HEX or 5 ASCII/alphanumeric characters.
8. Be sure to write down the wireless settings for future use. Other wireless devices that will be connected to your Gateway must be configured to use these settings to join your Gateway's wireless network.
9. Click **Apply** to save changes.

## Advanced Security Settings

You can change your advanced wireless security settings, such as configuring wireless encryption to prevent unauthorized access or damage to your network devices; disable your SSID broadcast to secure your wireless traffic; stop your Gateway 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.

➢ To modify the security settings for either 2.4 GHz or 5 GHz:

1. In the Wireless Settings page, select **Advanced Security Settings**.



Advanced Security Settings

IMPORTANT: For a more secure wireless network use Advanced Security Settings.

**Level 1:** Securing your wireless traffic as it transmits through the air, – we recommend you use WPA2 security, unless you experience compatibility issues.

| 2.4 GHz Security | 5.0 GHz Security |
|---|---|
| ○ WEP | ○ WEP |
| ○ WPA | ○ WPA |
| ○ WPA2 | ○ WPA2 |

**Level 2:** Stop your router from broadcasting your Wireless Network Name (SSID)
SSID Broadcast (Allows you to prevent users who do not know your SSID name to access your router wirelessly.)

2.4 GHz SSID Broadcast    5.0 GHz SSID Broadcast

**Level 3:** Limit access to certain wireless devices

Wireless MAC Authentication (Allows you to limit access to your wireless network by allowing only those devices with specific MAC addresses.)

802.11 b/g/n/ac Mode (Allows you to limit access to your wireless network based on the type of technology.)

Other Advanced Wireless Options

## Level 1: Securing your Network

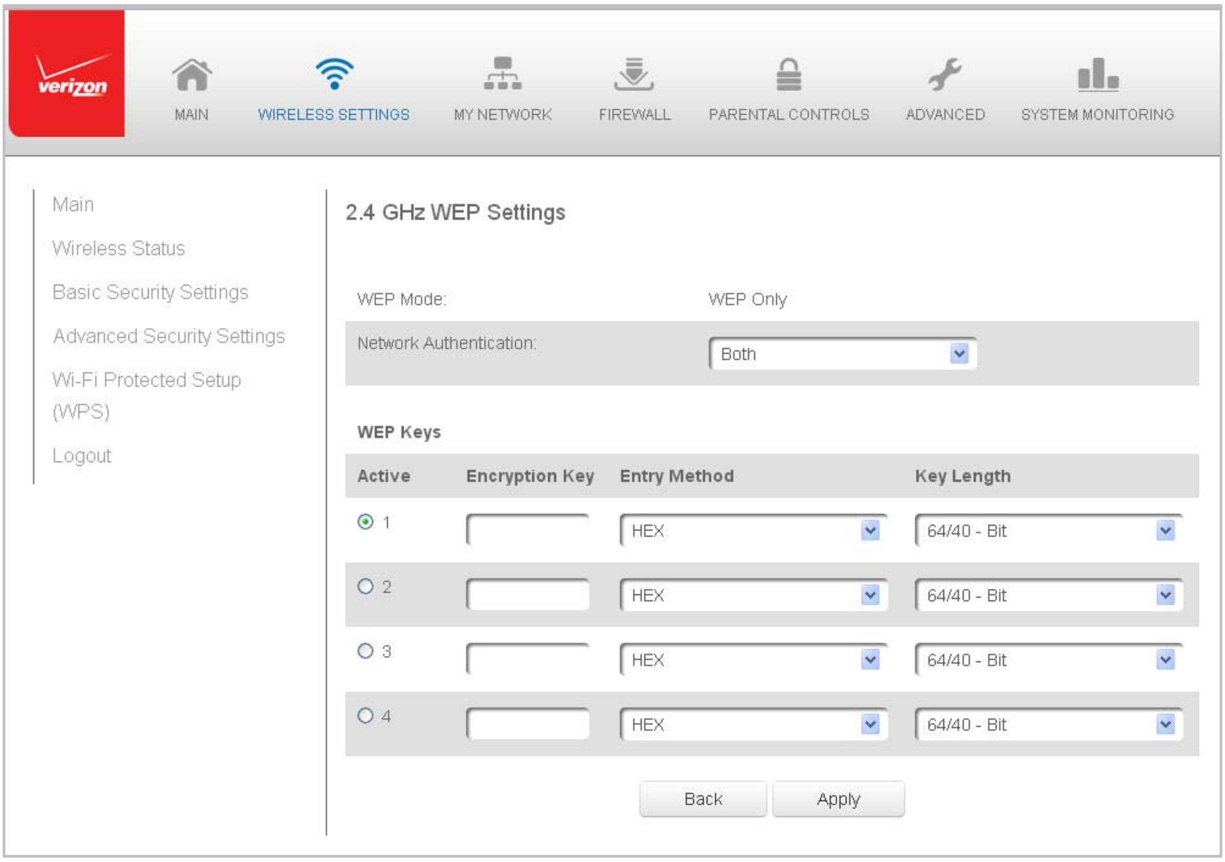
In the **Level 1** section, select the type of wireless security. Depending on your selection, one of the following pages displays.

**WEP**

If WEP was selected, the WEP Settings page displays.

➢ To set the WEP security:

1. In the **Network Authentication** field, select the authentication level as Open System Authentication, Shared Key Authentication or Both.



2.4 GHz WEP Settings

WEP Mode: WEP Only

Network Authentication: Both

WEP Keys

| Active | Encryption Key | Entry Method | Key Length |
|---|---|---|---|
| ● 1 | | HEX | 64/40 - Bit |
| ○ 2 | | HEX | 64/40 - Bit |
| ○ 3 | | HEX | 64/40 - Bit |
| ○ 4 | | HEX | 64/40 - Bit |

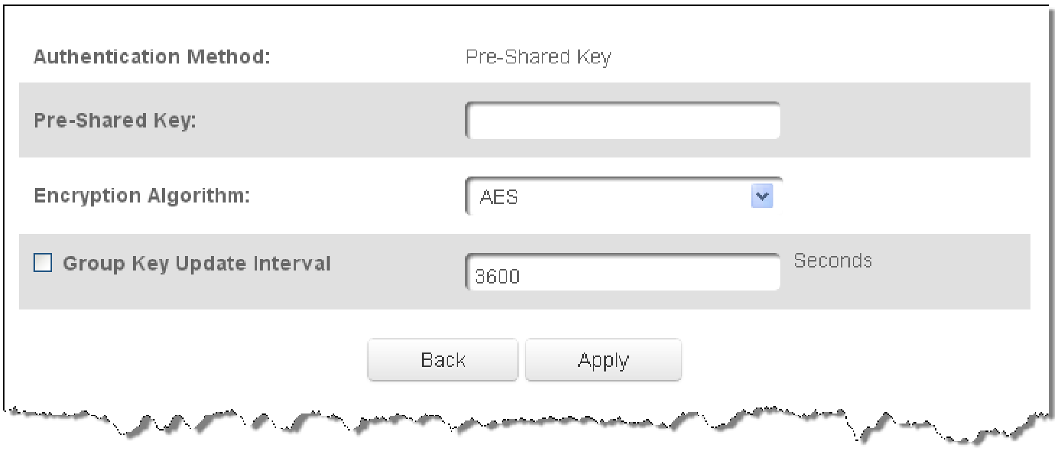
2. In the **WEP Keys** section, activate the encryption key be entering the key name in the **Encryption Key** column. If HEX, the key must be hexadecimal digits. If ASCII, any characters can be used.
3. Specify the length of key 1 by selecting 64/40 bit or 128/104 bit in the **Key Length** field and HEX or ASCII in the **Entry Method** field.
4. Click **Apply** to save changes.

### WPA

If WPA (Wi-Fi Protected Access) was selected, the WPA Key page displays. You can review the **User Guidance on Password Selection** section.

➢ To set the WPA security:

1. Enter the Pre-Shared Key as a wireless password or WPA key.



| | |
|---|---|
| Authentication Method: | Pre-Shared Key |
| Pre-Shared Key: | |
| Encryption Algorithm: | AES |
| □ Group Key Update Interval | 3600 Seconds |

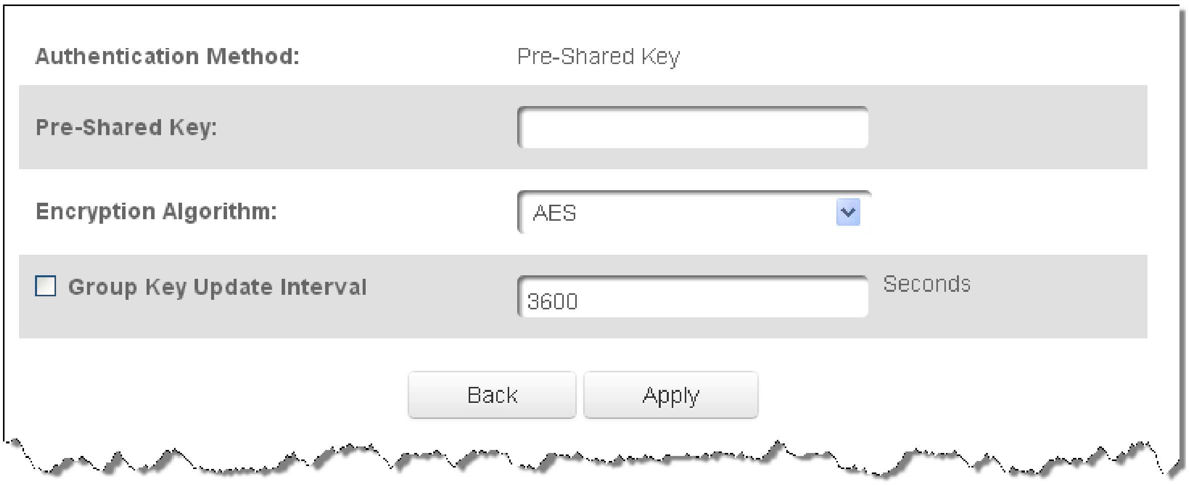
2. To activate the group key update interval, select the **Group Key Update Interval** check box and set the interval time in seconds.
3. Click **Apply** to save the changes.

### WPA2

If WPA2 (Wi-Fi Protected Access II) was selected, the WPA2 page displays. WPA2 is the default wireless security protocol. You can review the **User Guidance on Password Selection** section.

➢ To set the WPA2 security:

1. Enter the Pre-Shared Key.



|  |  |
|---|---|
| Authentication Method: | Pre-Shared Key |
| Pre-Shared Key: |  |
| Encryption Algorithm: | AES |
| □ Group Key Update Interval | 3600 Seconds |

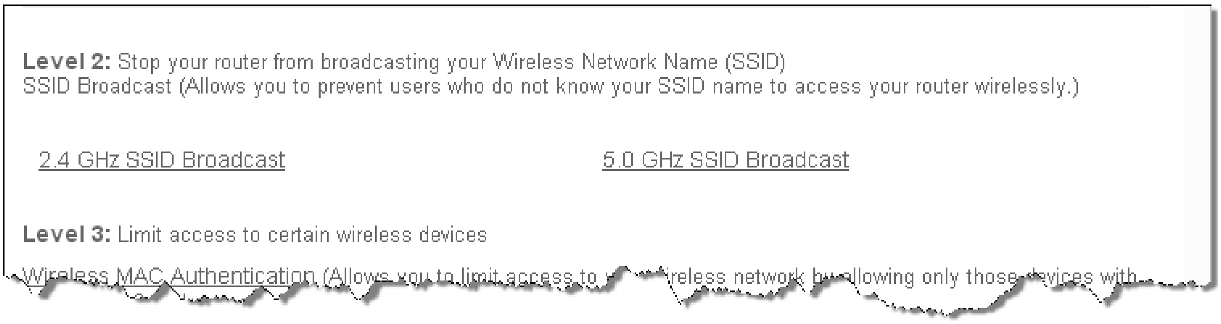
2. Select the encryption algorithm as TKIP and AES or AES.
3. To activate the group key update interval, select the **Group Key Update Interval** check box and set the interval time in seconds.
4. Click **Apply** to save the changes.

### Level 2: SSID Broadcast

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

➢ To enable or disable SSID broadcast:

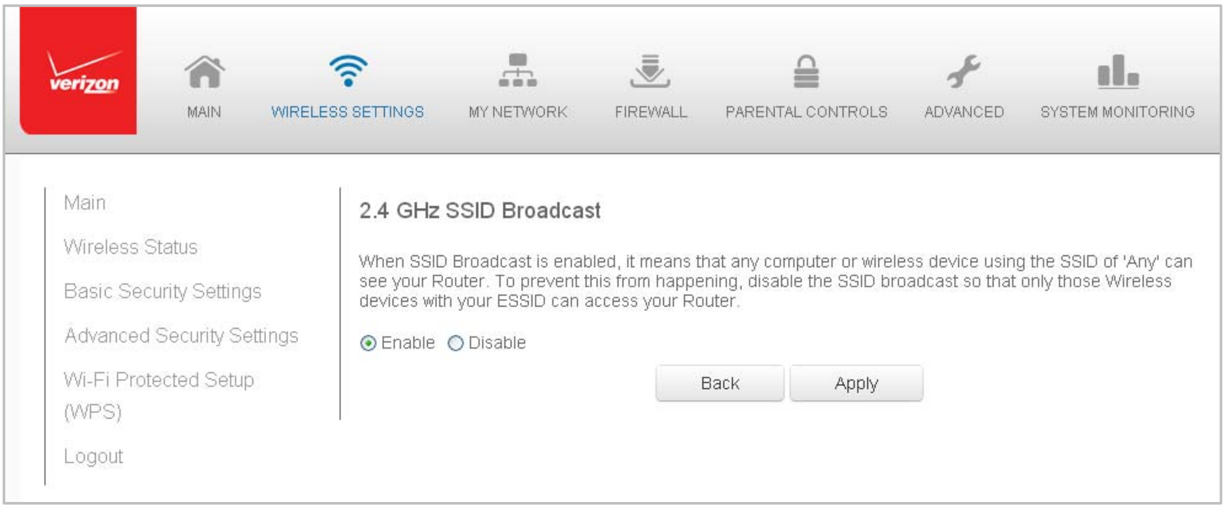
1. In the Advanced Settings page, locate the **Level 2** section.



**Level 2:** Stop your router from broadcasting your Wireless Network Name (SSID)
SSID Broadcast (Allows you to prevent users who do not know your SSID name to access your router wirelessly.)

**Level 3:** Limit access to certain wireless devices
Wireless MAC Authentication (Allows you to limit access to ireless network by allowing only those devices with

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.



2.4 GHz SSID Broadcast

When SSID Broadcast is enabled, it means that any computer or wireless device using the SSID of 'Any' can see your Router. To prevent this from happening, disable the SSID broadcast so that only those Wireless devices with your ESSID can access your Router.

● Enable ○ Disable

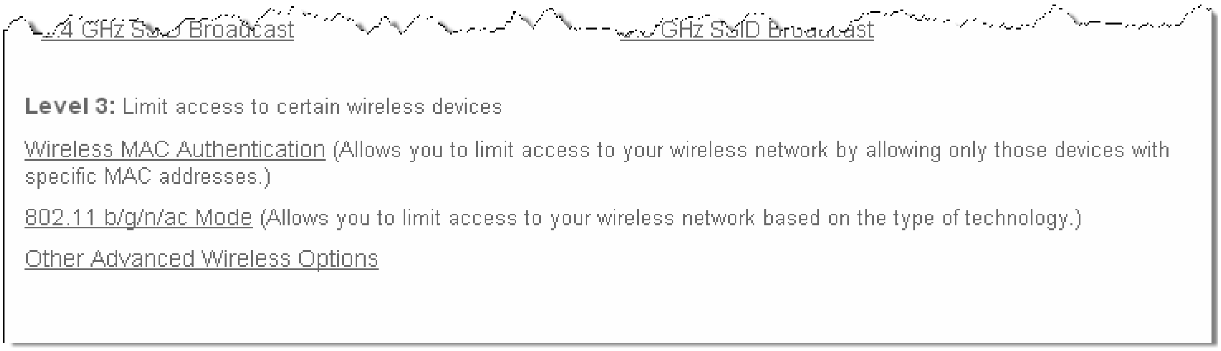
3. To enable SSID broadcasting, click the **Enable** radio button. SSID broadcast is enabled by default. The SSID of the wireless network will be broadcast to all wireless devices.
4. To disable SSID broadcasting, click the **Disable** radio button. The public SSID broadcast will be hidden from all wireless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

## Level 3: Limit Access

You can configure your Gateway 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 3** section.



**Level 3:** Limit access to certain wireless devices

Wireless MAC Authentication (Allows you to limit access to your wireless network by allowing only those devices with specific MAC addresses.)

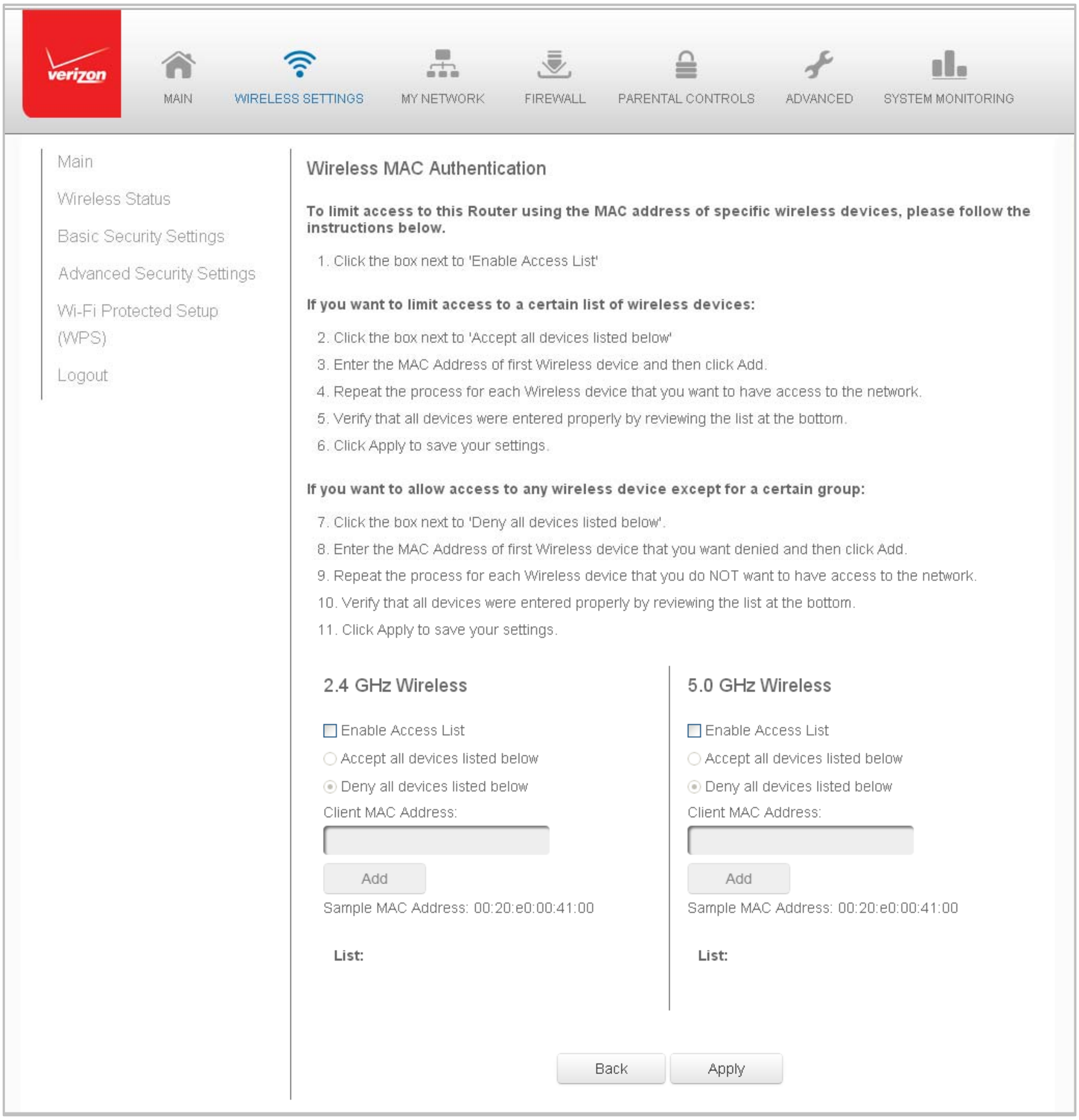
802.11 b/g/n/ac Mode (Allows you to limit access to your wireless network based on the type of technology.)

Other Advanced Wireless Options

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.

## Wireless MAC Authentication

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



Wireless MAC Authentication

**To limit access to this Router using the MAC address of specific wireless devices, please follow the instructions below.**

1. Click the box next to 'Enable Access List'

**If you want to limit access to a certain list of wireless devices:**

2. Click the box next to 'Accept all devices listed below'
3. Enter the MAC Address of first Wireless device and then click Add.
4. Repeat the process for each Wireless device that you want to have access to the network.
5. Verify that all devices were entered properly by reviewing the list at the bottom.
6. Click Apply to save your settings.

**If you want to allow access to any wireless device except for a certain group:**

7. Click the box next to 'Deny all devices listed below'.
8. Enter the MAC Address of first Wireless device that you want denied and then click Add.
9. Repeat the process for each Wireless device that you do NOT want to have access to the network.
10. Verify that all devices were entered properly by reviewing the list at the bottom.
11. Click Apply to save your settings.

2.4 GHz Wireless

□ Enable Access List
○ Accept all devices listed below
● Deny all devices listed below
Client MAC Address:

Add

Sample MAC Address: 00:20:e0:00:41:00

**List:**

5.0 GHz Wireless

□ Enable Access List
○ Accept all devices listed below
● Deny all devices listed below
Client MAC Address:

Add

Sample MAC Address: 00:20:e0:00:41:00

**List:**

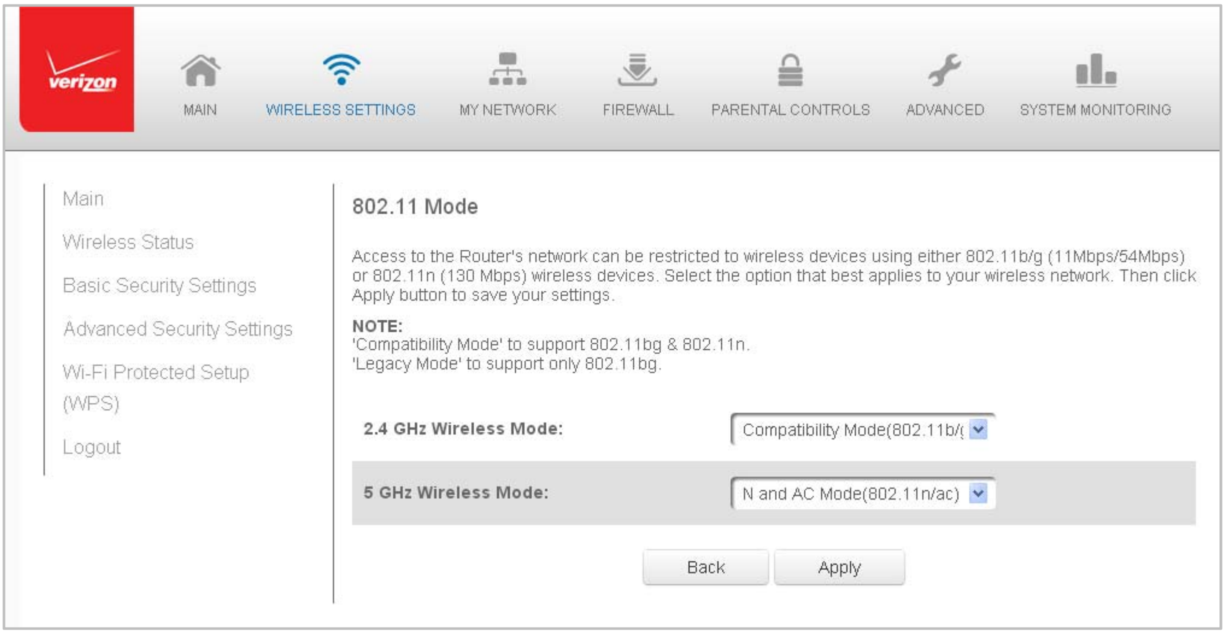
Back Apply

- To set Wireless MAC Authentication:
  1. On the Advanced Settings page, locate the **Level 3** 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.
     - **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.

## 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

Access to the Router's network can be restricted to wireless devices using either 802.11b/g (11Mbps/54Mbps) or 802.11n (130 Mbps) wireless devices. Select the option that best applies to your wireless network. Then click Apply button to save your settings.

NOTE:
'Compatibility Mode' to support 802.11bg & 802.11n.
'Legacy Mode' to support only 802.11bg.

2.4 GHz Wireless Mode: Compatibility Mode(802.11b/(

5 GHz Wireless Mode: N and AC Mode(802.11n/ac)

➢ To select the 802.11 Mode:

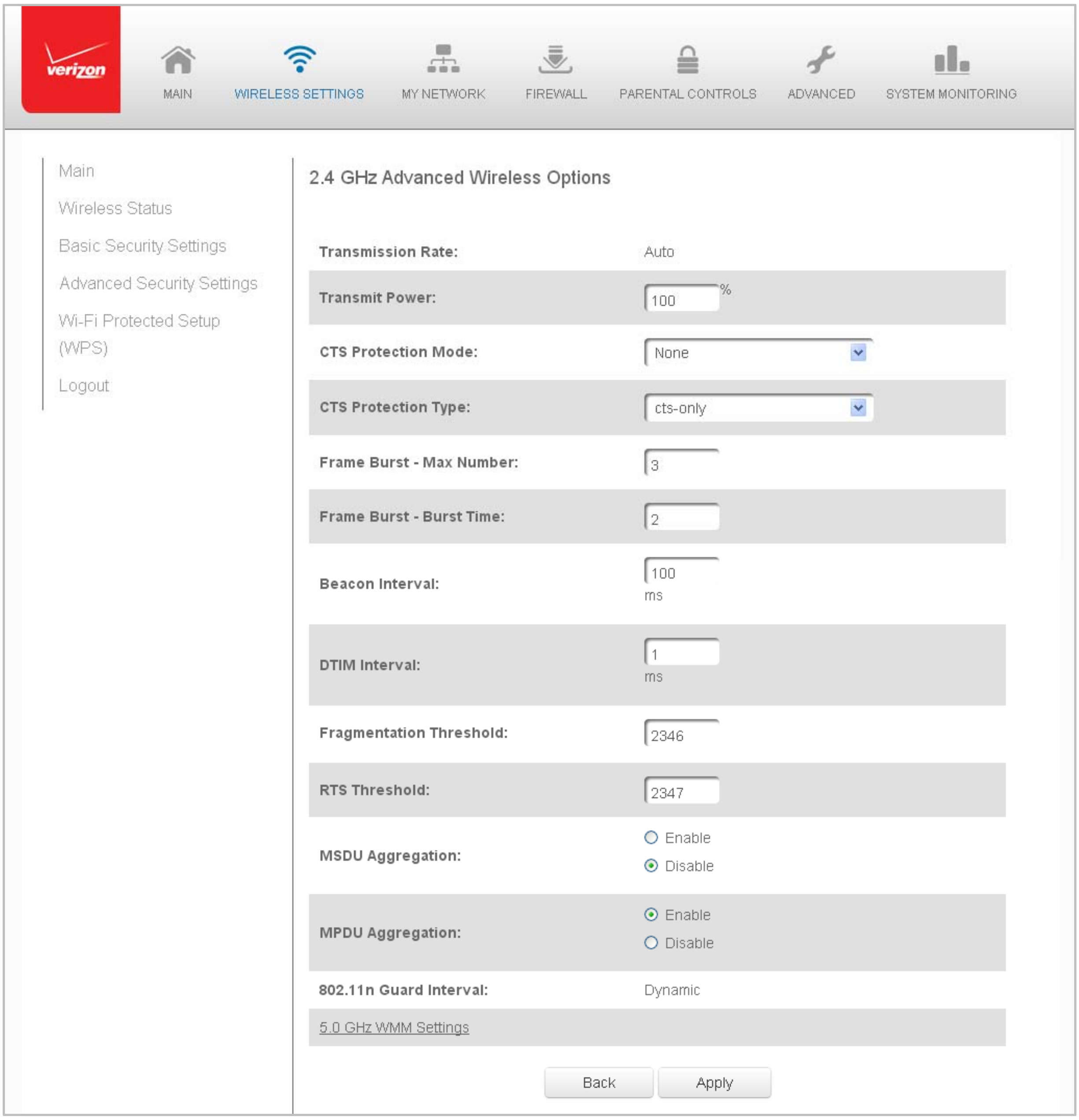
1. On the Advanced Settings page, locate the **Level 3** section and click the **802.11 Mode** link. The 802.11 Mode page displays.
2. Select the 2.4 GHz Wireless Mode as follows:
   - **Compatibility** – This is the default mode setting, providing a good balance of performance and compatibility with 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.
   - **N Only Mode** – The 5 GHz frequencies are available to 802.11n devices. 802.11ac is not enabled.
   - **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.

## Other Advanced Wireless Options

You can view additional wireless options.

➢ To view the options:

1. In the Advanced Settings page, locate the **Level 3** section and click **Other Advanced Wireless Options** link. A warning message displays.
2. Click **OK**. The Other Advanced Wireless Options page displays.



2.4 GHz Advanced Wireless Options

| | |
|---|---|
| Transmission Rate: | Auto |
| Transmit Power: | 100 % |
| CTS Protection Mode: | None |
| CTS Protection Type: | cts-only |
| Frame Burst - Max Number: | 3 |
| Frame Burst - Burst Time: | 2 |
| Beacon Interval: | 100<br>ms |
| DTIM Interval: | 1<br>ms |
| Fragmentation Threshold: | 2346 |
| RTS Threshold: | 2347 |
| MSDU Aggregation: | ○ Enable<br>● Disable |
| MPDU Aggregation: | ● Enable<br>○ Disable |
| 802.11n Guard Interval: | Dynamic |

5.0 GHz WMM Settings

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 Gateway and your local network.

- **Transmission Rate** – displays status as Auto
- **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
- **Frame Burst – Max Number** – allows packet bursting, which increases overall network speed
- **Frame Burst – Burst Time** – indicates the burst time of the frame bursts
- **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

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

## WMM Settings

You can prioritize the types of data transmitted over the wireless network using the advanced WMM settings.

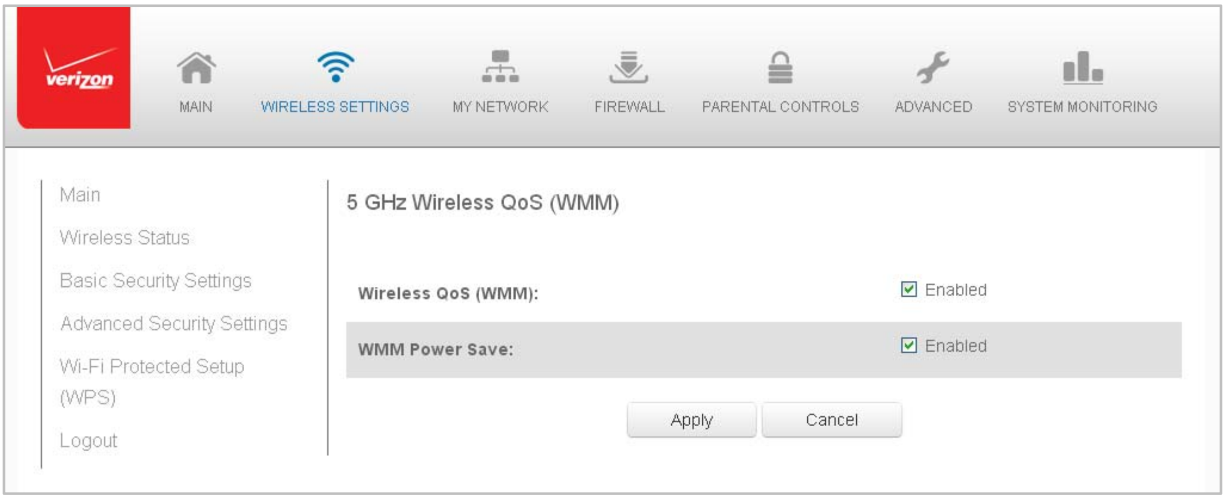
Wireless QoS (WMM) can improve the quality of service (QoS) for voice, video, and audio streaming over Wi-Fi by prioritizing these data streams.

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.

➢ 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.



5 GHz Wireless QoS (WMM)

Wireless QoS (WMM): ☑ Enabled

WMM Power Save: ☑ Enabled

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.

# Chapter 4  Configuring My Network Settings

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

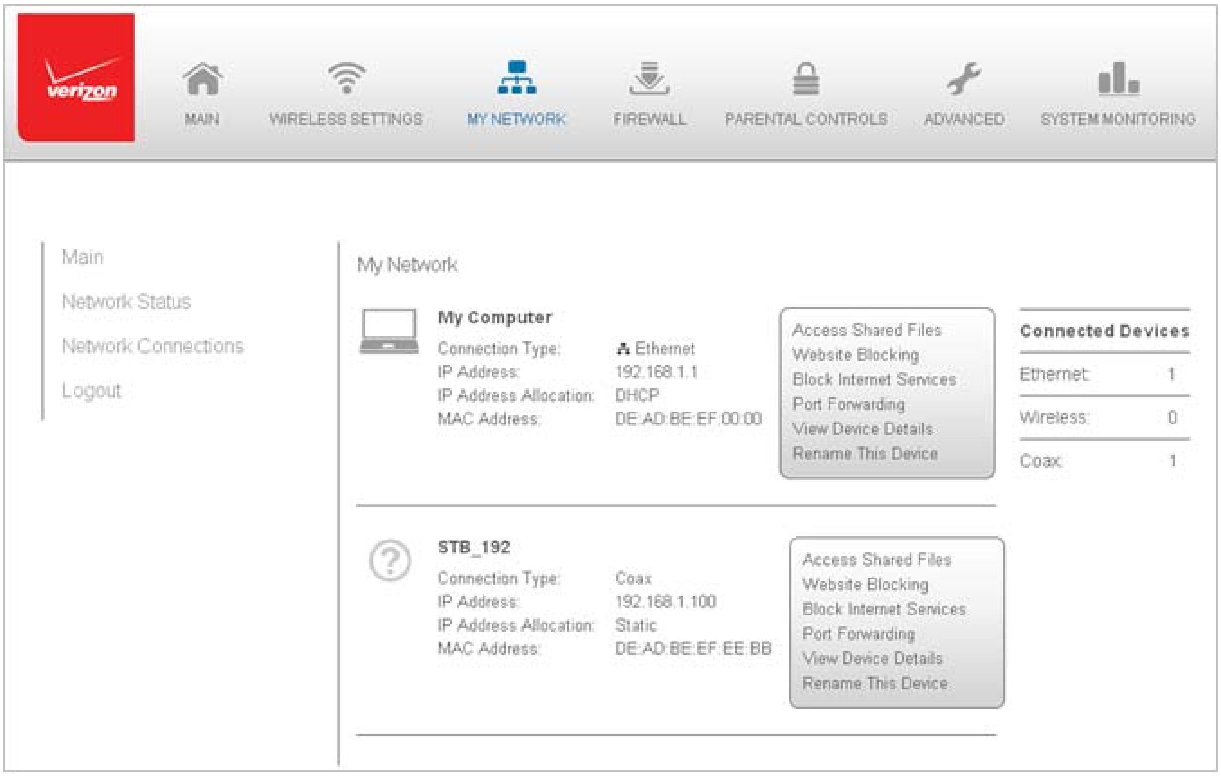
**Caution!** The settings described in this chapter should only be configured by experienced network technicians. Changes could adversely affect the operation of your Gateway and your local network.

## 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.



My Network

**My Computer**

| | |
|---|---|
| Connection Type: | Ethernet |
| IP Address: | 192.168.1.1 |
| IP Address Allocation: | DHCP |
| MAC Address: | DE:AD:BE:EF:00:00 |

**STB_192**

| | |
|---|---|
| Connection Type: | Coax |
| IP Address: | 192.168.1.100 |
| IP Address Allocation: | Static |
| MAC Address: | DE:AD:BE:EF:EE:BB |

| Connected Devices | |
|---|---|
| Ethernet: | 1 |
| Wireless: | 0 |
| Coax: | 1 |

## Using My Network Settings

You can access and configure common network parameters:

- **Website Blocking**

  To block specific websites, click **Website Blocking**. The Parental Control page displays.

  For additional information about blocking websites, refer to **Chapter 7 Using 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 6 Configuring System 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 System 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, and Windows Shared Folder 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.

# Chapter 5 Using Network Connections

Your Gateway 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.

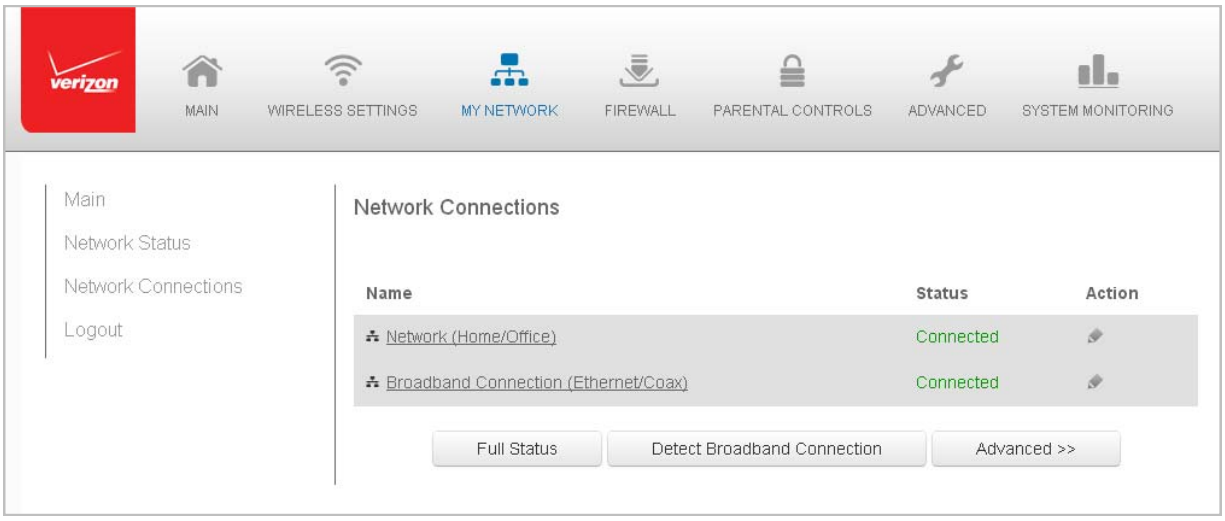
**Caution!** The settings described in this chapter should only be configured by experienced network technicians. Changes could adversely affect the operation of your Gateway and your local network.

## Accessing Network Connections

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

➢ To access the network connections:

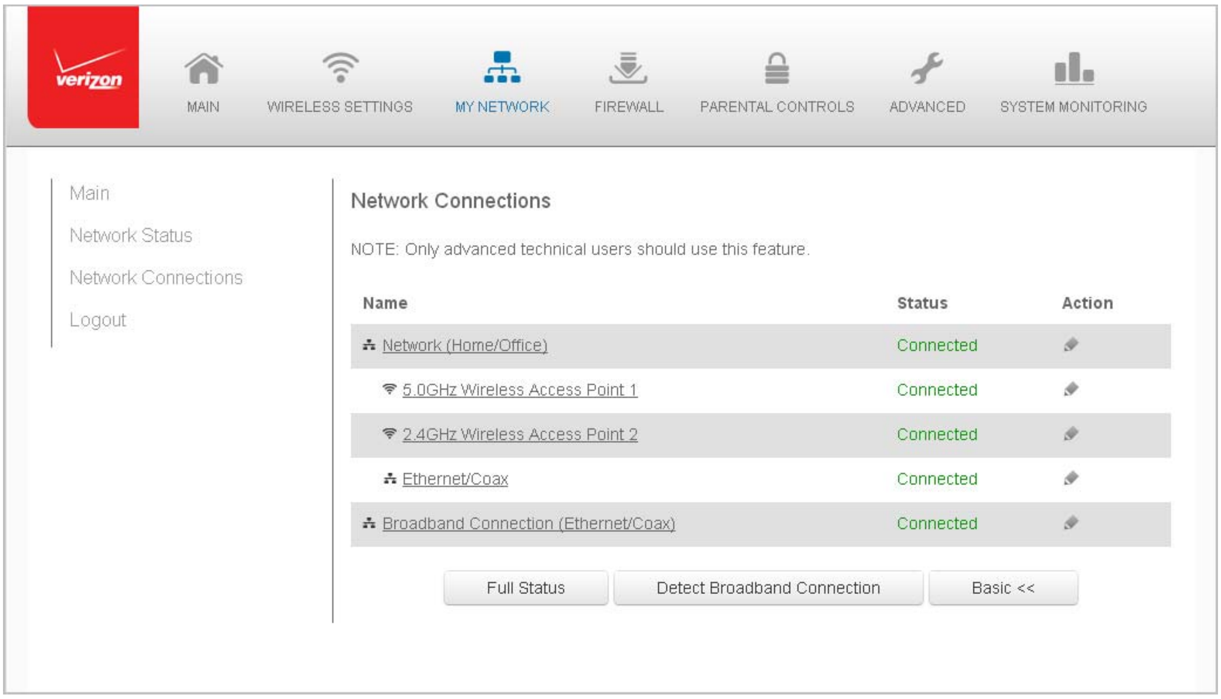
1. Select **My Network**, then select **Network Connections**.



Network Connections

| Name | Status | Action |
|---|---|---|
| Network (Home/Office) | Connected | |
| Broadband Connection (Ethernet/Coax) | Connected | |

2. To display all connection entries, click the **Advanced** button.



Network Connections

NOTE: Only advanced technical users should use this feature.

| Name | Status | Action |
|---|---|---|
| Network (Home/Office) | Connected | ✎ |
| 5.0GHz Wireless Access Point 1 | Connected | ✎ |
| 2.4GHz Wireless Access Point 2 | Connected | ✎ |
| Ethernet/Coax | Connected | ✎ |
| Broadband Connection (Ethernet/Coax) | Connected | ✎ |

3. To select a specific network connection, click the hyperlinked name. The following sections detail the types of network connections that you can view.

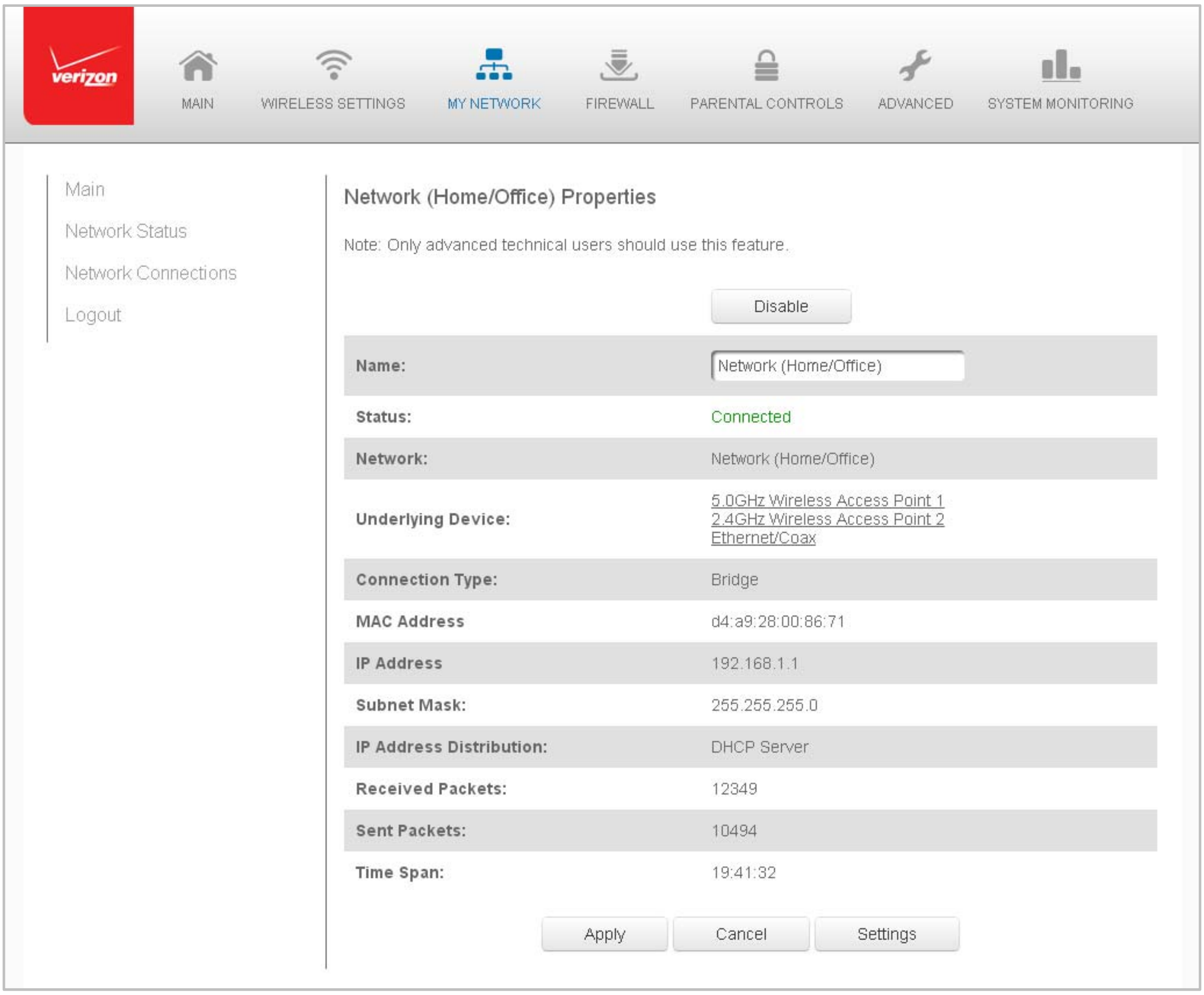
## Network (Home/Office) Connection

You can view the properties of your local network. This connection is used to combine several network devices 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 formerly underlying devices connected to it will not be able to obtain a new DHCP address from that Gateway network interface.

➢ To view the connection:

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



Network (Home/Office) Properties

Note: Only advanced technical users should use this feature.

Disable

| | |
|---|---|
| Name: | Network (Home/Office) |
| Status: | Connected |
| Network: | Network (Home/Office) |
| Underlying Device: | 5.0GHz Wireless Access Point 1<br>2.4GHz Wireless Access Point 2<br>Ethernet/Coax |
| Connection Type: | Bridge |
| MAC Address | d4:a9:28:00:86:71 |
| IP Address | 192.168.1.1 |
| Subnet Mask: | 255.255.255.0 |
| IP Address Distribution: | DHCP Server |
| Received Packets: | 12349 |
| Sent Packets: | 10494 |
| Time Span: | 19:41:32 |

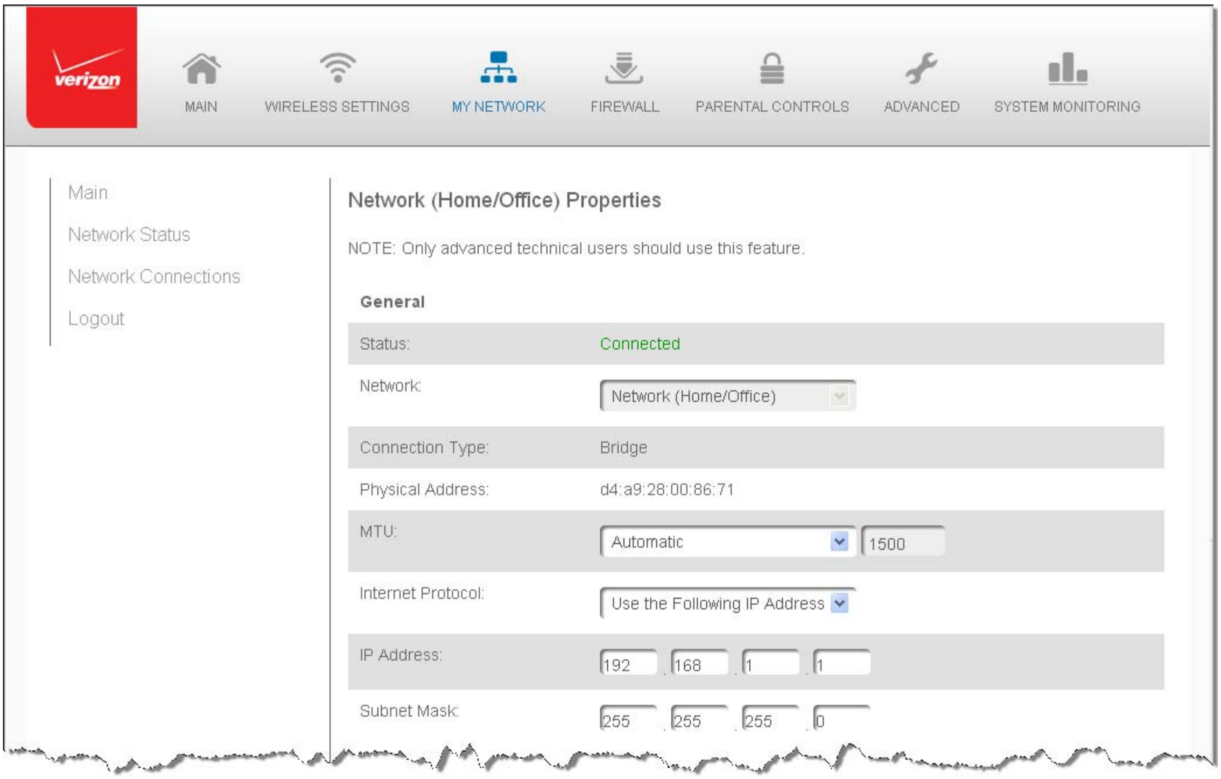
Apply Cancel Settings

2. To disable an active network connection, click **Disable**.
3. To rename a network connection, enter the new network name in the **Name** field.
4. Click **Apply** to save the changes.

## Configuring the Home/Office Network

➢ To configure a network connection:

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



Network (Home/Office) Properties

NOTE: Only advanced technical users should use this feature.

General

| | |
|---|---|
| Status: | Connected |
| Network: | Network (Home/Office) |
| Connection Type: | Bridge |
| Physical Address: | d4:a9:28:00:86:71 |
| MTU: | Automatic 1500 |
| Internet Protocol: | Use the Following IP Address |
| IP Address: | 192 . 168 . 1 . 1 |
| Subnet Mask: | 255 . 255 . 255 . 0 |

2. Configure the following sections, as needed.

### 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

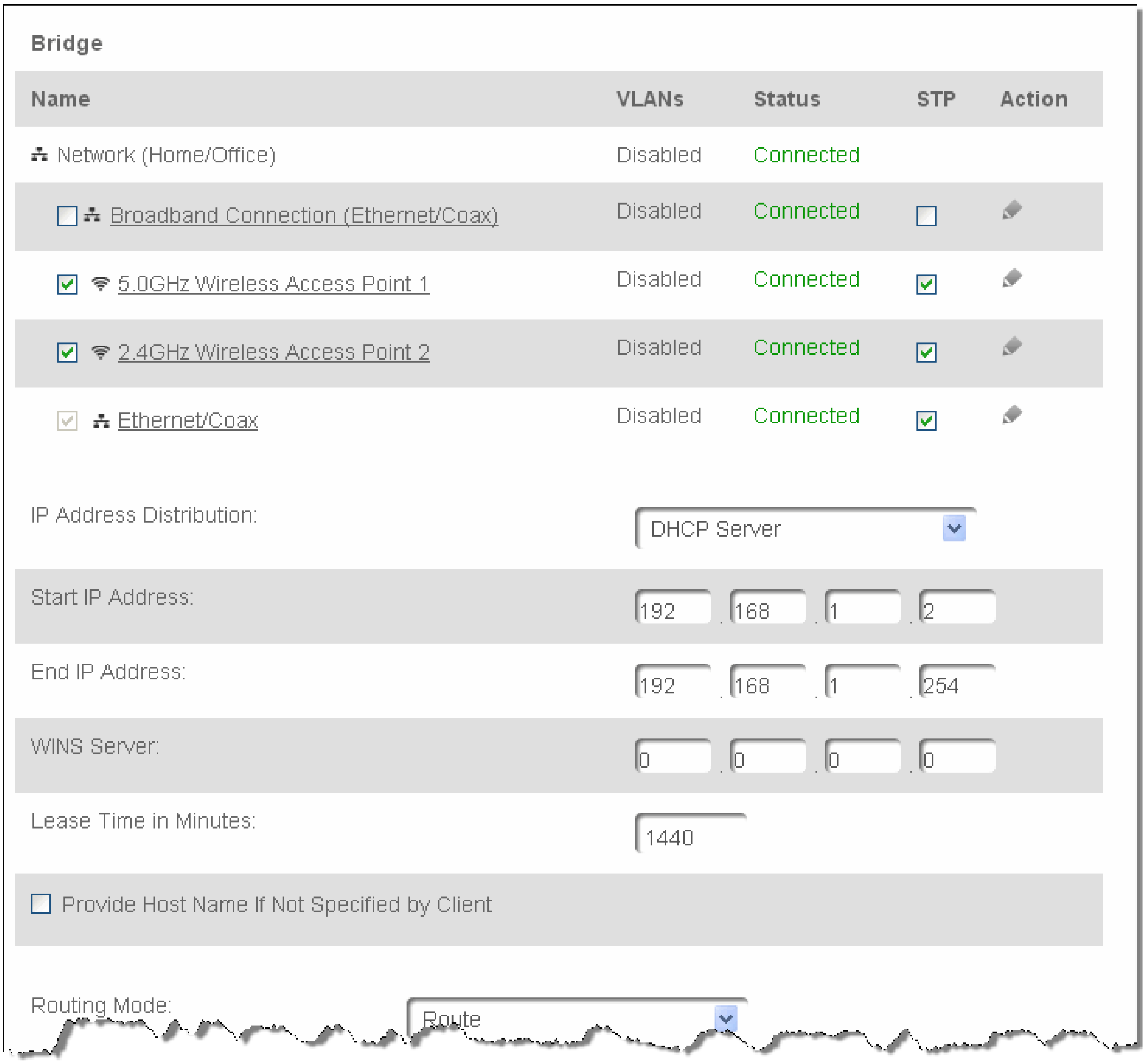
In the Internet Protocol section, specify one of the following:

- **Obtain an IP Address Automatically** – the network connection is required by Verizon to obtain an IP address automatically (default). The DHCP server assigning the IP address also assigns a subnet mask address. The subnet mask address can be overridden by entering a different subnet mask address provided by Verizon or experienced network technician.
- **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.
- **Use the Following IP Address** - the network connection uses a permanent or static IP address, then the IP address and subnet mask address.

### Bridge

In the **Bridge** section of the Configure Network (Home/Office), you can configure the various LAN interfaces. By default, the Ethernet, Coax, and Wireless Access Point connections are activated.

**Caution!** Do not change these settings unless specifically instructed to by Verizon. Changes could adversely affect the operation of your Gateway and your local network.



Bridge

| Name | VLANs | Status | STP | Action |
|---|---|---|---|---|
| Network (Home/Office) | Disabled | Connected | | |
| ☐ Broadband Connection (Ethernet/Coax) | Disabled | Connected | ☐ | ✎ |
| ☑ 5.0GHz Wireless Access Point 1 | Disabled | Connected | ☑ | ✎ |
| ☑ 2.4GHz Wireless Access Point 2 | Disabled | Connected | ☑ | ✎ |
| ☑ Ethernet/Coax | Disabled | Connected | ☑ | ✎ |

| | |
|---|---|
| IP Address Distribution: | DHCP Server |
| Start IP Address: | 192 . 168 . 1 . 2 |
| End IP Address: | 192 . 168 . 1 . 254 |
| WINS Server: | 0 . 0 . 0 . 0 |
| Lease Time in Minutes: | 1440 |

☐ Provide Host Name If Not Specified by Client

Routing Mode: Route

Verify the following information:

- **Status** – displays the connection status of a specific device.
- **STP** – enables Spanning Tree Protocol on the device. This protocol provides a path redundancy while preventing undesirable communication loops in the network.
- **Action** – contains an icon that, when clicked, generates the next lower-level configuration page for the specific network connection or network device.

For example, when you click the **Action** icon, you can configure the DNS server in the lower-level network connection properties settings for the Broadband Connection (Ethernet/Coax) network.

In addition, the DHCP and Routing actions listed below are examples of the actions that can be configured for the Broadband Connection (Ethernet/Coax) and Network (Home/Office) networks.

### DNS Server

The DNS (Domain Name System) is the naming system method by which websites or domain names are translated into IP addresses.

To configure your Gateway’s Broadband Connection (Ethernet/Coax) network to use a specific DNS server, refer to the **DNS Server** section of the Properties page.

To manually configure a DNS server using the DNS addresses provided by Verizon:

1. Specify the following DNS Server addresses: the Primary and Secondary DNS server addresses.
2. Click **Apply** to save the changes.

### DHCP Server

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

Once enabled and configure, 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 Gateway, configure the network devices as DHCP Clients. There are 2 basic options in this section: Disabled and DHCP Server.

To set up the Gateway’s network bridge to function as a DHCP server:

1. In the **IP Address Distribution** section, select the DHCP server. Once enabled, the DHCP server provides automatic IP assignments (also referred to as IP leases) based on the preset IP range defined below.
    a. **Start IP Address** – Enter the first IP address in the IP range that the Gateway will automatically begin assigning IP addresses from. Since your Gateway’s IP address is 192.168.1.1, the default Start IP Address is 192.168.1.2.

    b. **End IP Address** – Enter the last IP address in the IP range that the Gateway will automatically stop the IP address allocation at. The maximum end IP address range that can be entered is 192.168.1.254.
2. If Windows Internet Naming Service (WINS) is being used, enter the WINS server address.
3. In the **Lease Time in Minutes** field, enter the amount of time a network device is allowed to connect to the Gateway with its currently issued dynamic IP address.
4. To have the Gateway automatically assign a host name to network devices, select the **Provide Host Name if Not Specified by Client** check box.
5. Click **Apply** to save changes.

### Routing

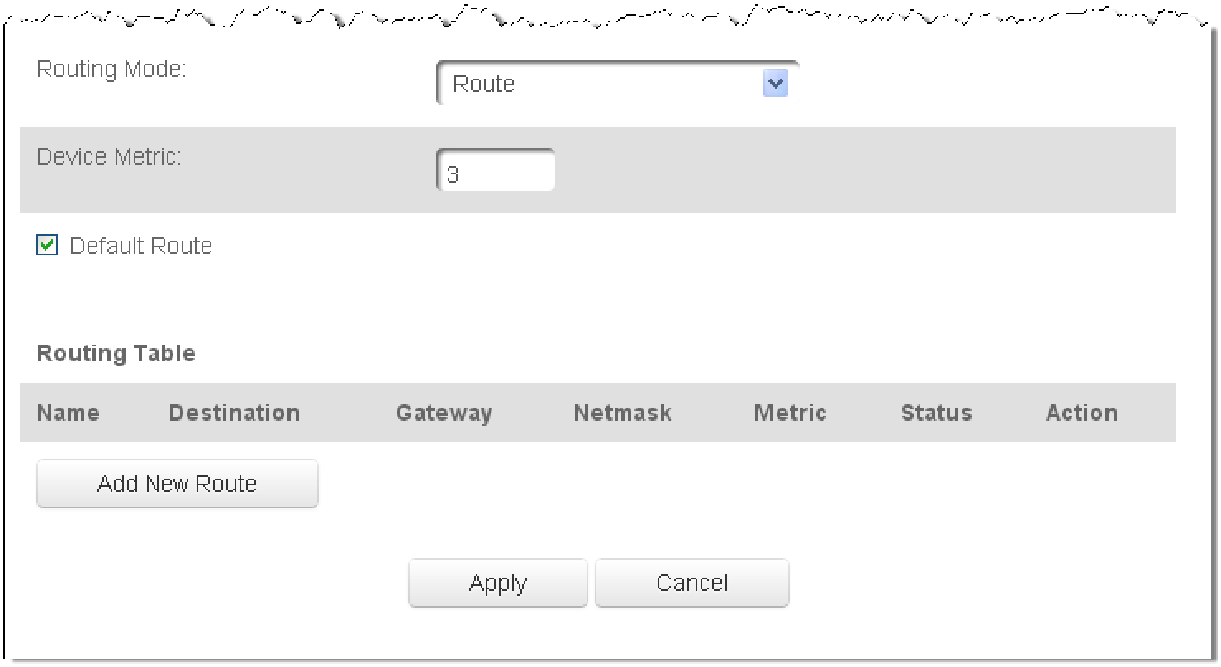
You can configure your Gateway to use static or dynamic routing.

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

To configure routing:

1. In the **Device Metric** field, enter a device metric.

   The device metric is a value used by your Gateway to determine whether one route is superior to another, based on parameters, such as bandwidth and delay time.



Routing Mode: Route

Device Metric: 3

☑ Default Route

Routing Table

| Name | Destination | Gateway | Netmask | Metric | Status | Action |
|---|---|---|---|---|---|---|

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

### Complete Network Connection Configuration Updates

- To save your changes, click **Apply**.

## Ethernet/Coax Connection

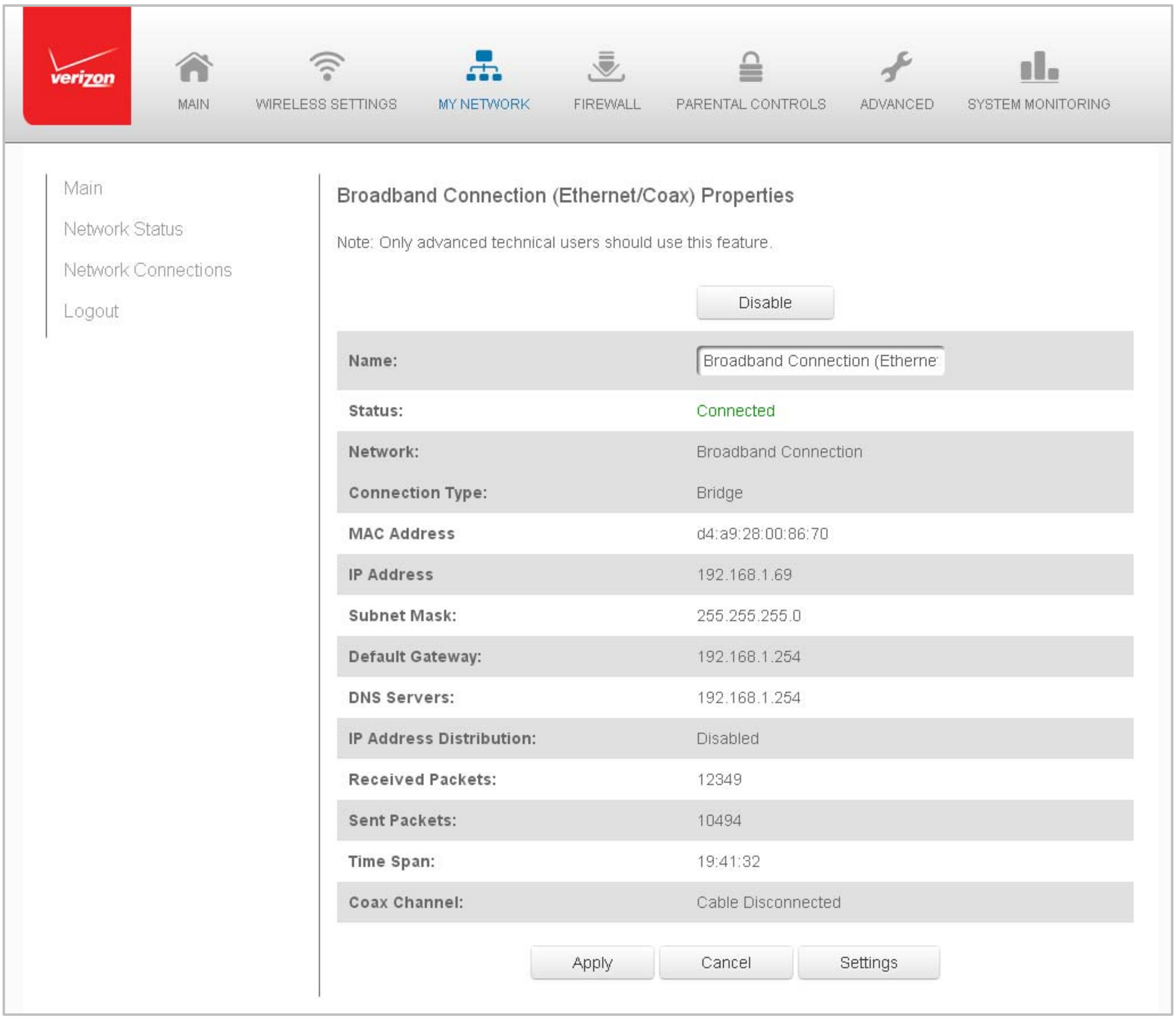
An Ethernet connection connects computers to your Gateway using Ethernet cables. The connections are either direct or use network hubs and switches.

A Coax connection connects devices, such as set-top boxes, to your Gateway using a coaxial cable.

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

➢ To view the connection:

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



Broadband Connection (Ethernet/Coax) Properties

Note: Only advanced technical users should use this feature.

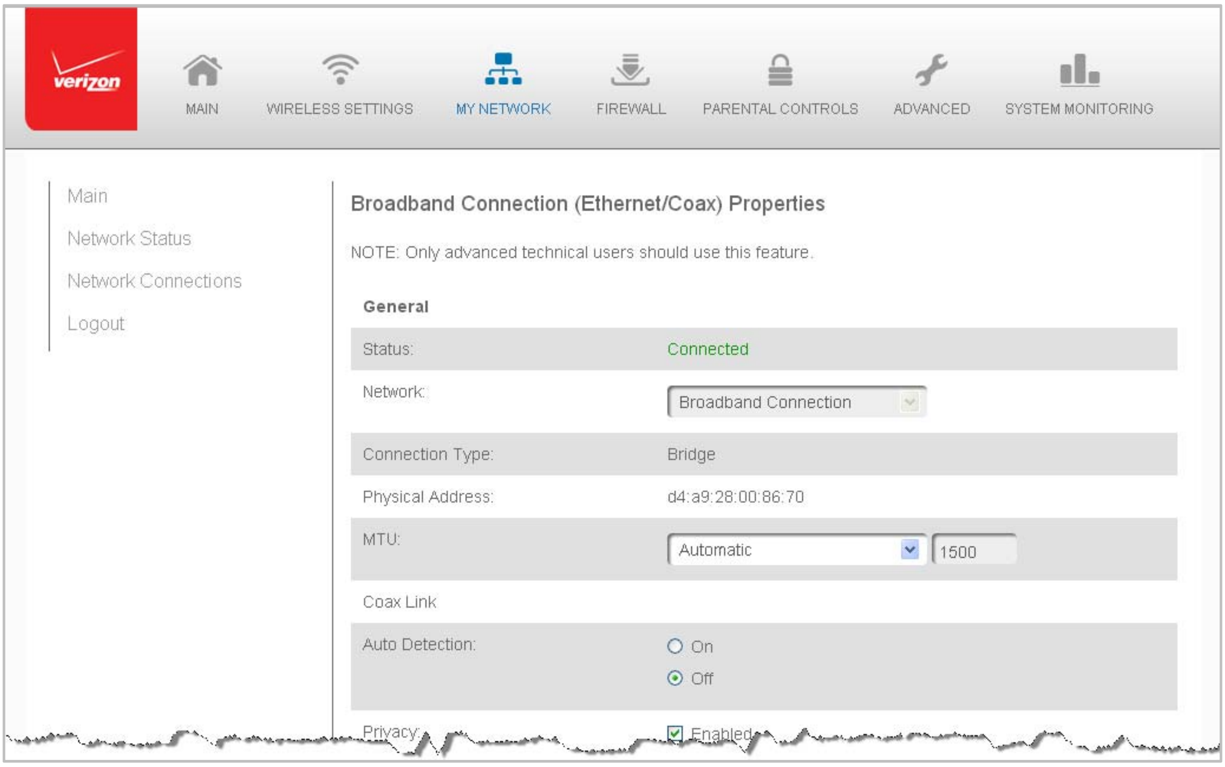
| | |
|---|---|
| Name: | Broadband Connection (Etherne |
| Status: | Connected |
| Network: | Broadband Connection |
| Connection Type: | Bridge |
| MAC Address | d4:a9:28:00:86:70 |
| IP Address | 192.168.1.69 |
| Subnet Mask: | 255.255.255.0 |
| Default Gateway: | 192.168.1.254 |
| DNS Servers: | 192.168.1.254 |
| IP Address Distribution: | Disabled |
| Received Packets: | 12349 |
| Sent Packets: | 10494 |
| Time Span: | 19:41:32 |
| Coax Channel: | Cable Disconnected |

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

### 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) Properties

NOTE: Only advanced technical users should use this feature.

General

| | |
|---|---|
| Status: | Connected |
| Network: | Broadband Connection |
| Connection Type: | Bridge |
| Physical Address: | d4:a9:28:00:86:70 |
| MTU: | Automatic 1500 |

Coax Link

| | |
|---|---|
| Auto Detection: | ○ On<br>● Off |
| Privacy: | ☑ Enabled |

2. Configure the following settings, as needed.

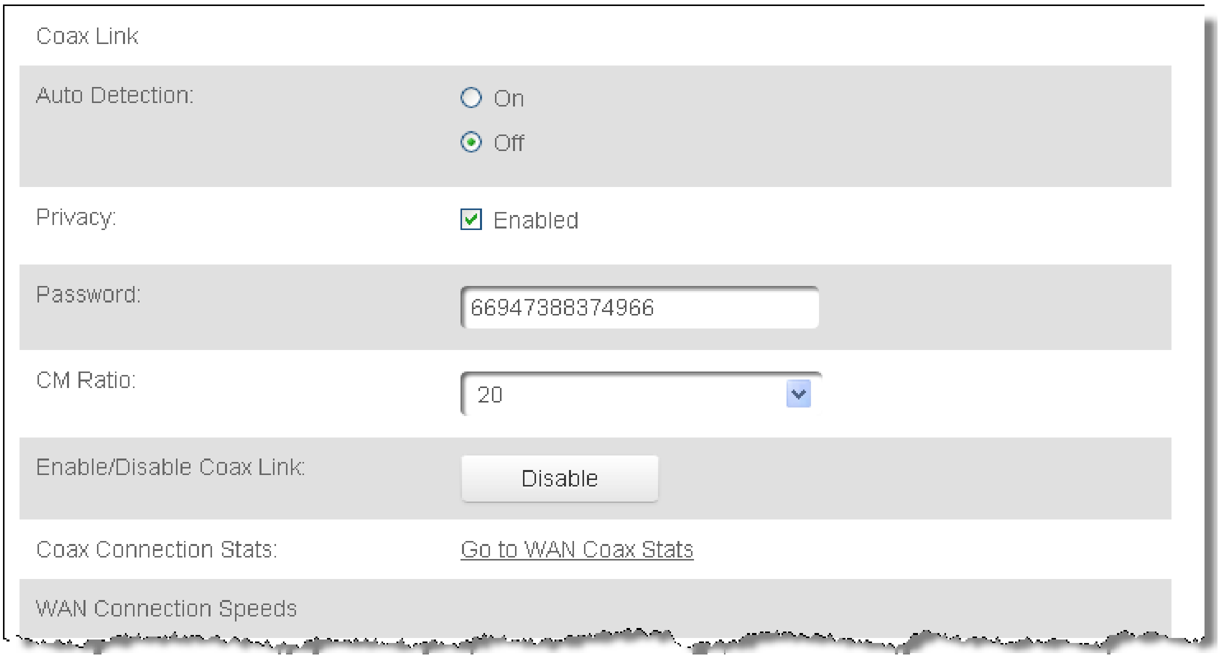
### General

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:
  - **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

### Coax Link

1. To set the Channel, select the coax link channel as 1 to 3.



Coax Link

| | |
|---|---|
| Auto Detection: | ○ On<br>● Off |
| Privacy: | ☑ Enabled |
| Password: | 66947388374966 |
| CM Ratio: | 20 |
| Enable/Disable Coax Link: | Disable |
| Coax Connection Stats: | Go to WAN Coax Stats |

WAN Connection Speeds

2. Select the **On** or **Off** radio button in the **Auto Detection** field.
3. 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.
4. To set the password, enter the Coax Link password in the **Password** field.
5. To set the CM ratio, select the CM ratio in drop down.
6. To enable or disable the Coax link, click **Disable** or **Enable**.
7. To view the devices connected using the coaxial cable, click the **Go to WAN Coax Stats** link.

#### HW Switch Ports

➢ To generate the Port Settings page and set the HW Switch Ports:

1. In the **HW Switch Ports** section, verify the connection status of the 4 Ethernet ports and 1 coax port.
2. To edit network traffic policies, click the **Action** icon.

#### Complete all Ethernet/Coax Connection Configuration Updates

➢ To save your changes:

1. Click **Apply**.

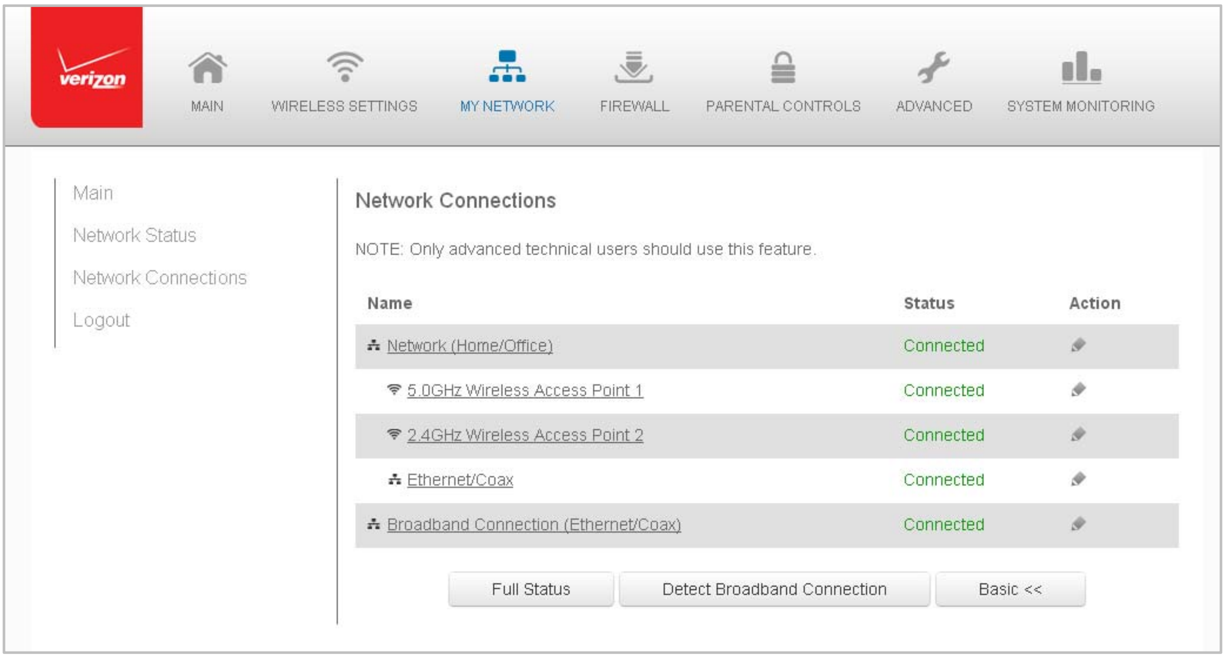
## Wireless Access Point Connection

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.

➢ To view the connection:

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

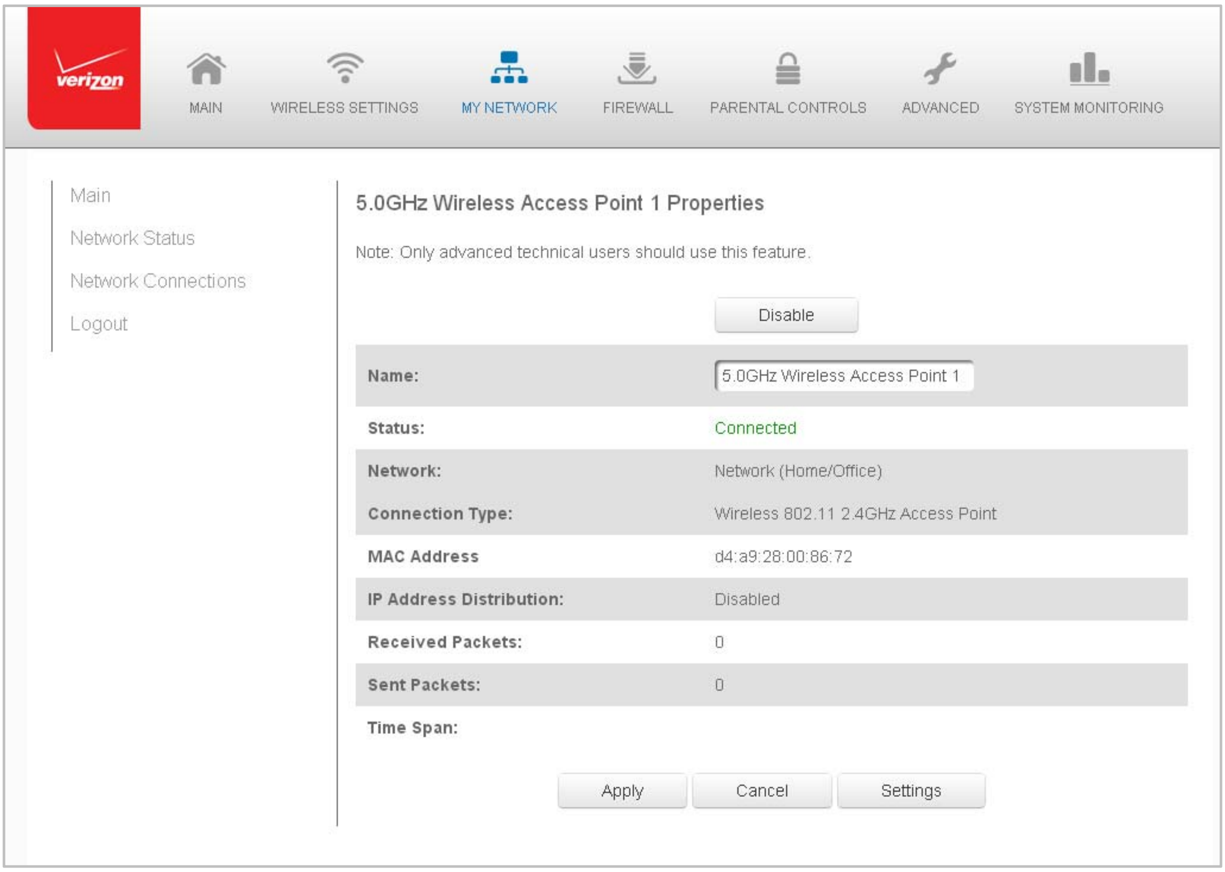


Network Connections

NOTE: Only advanced technical users should use this feature.

| Name | Status | Action |
|---|---|---|
| Network (Home/Office) | Connected | ✎ |
| 5.0GHz Wireless Access Point 1 | Connected | ✎ |
| 2.4GHz Wireless Access Point 2 | Connected | ✎ |
| Ethernet/Coax | Connected | ✎ |
| Broadband Connection (Ethernet/Coax) | Connected | ✎ |

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



5.0GHz Wireless Access Point 1 Properties

Note: Only advanced technical users should use this feature.

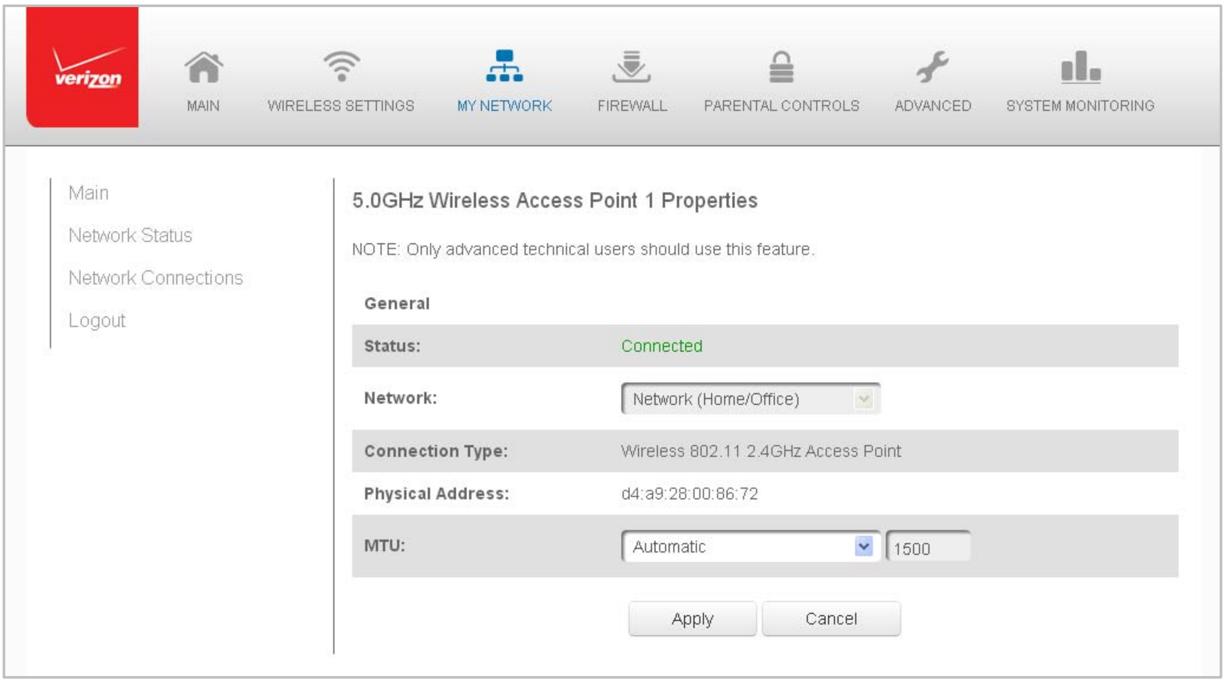
| | |
|---|---|
| Name: | 5.0GHz Wireless Access Point 1 |
| Status: | Connected |
| Network: | Network (Home/Office) |
| Connection Type: | Wireless 802.11 2.4GHz Access Point |
| MAC Address | d4:a9:28:00:86:72 |
| IP Address Distribution: | Disabled |
| Received Packets: | 0 |
| Sent Packets: | 0 |
| Time Span: | |

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 Gateway.

### Configuring the Wireless Access Point Properties

➢ To configure the connection:

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



5.0GHz Wireless Access Point 1 Properties

NOTE: Only advanced technical users should use this feature.

General

| | |
|---|---|
| Status: | Connected |
| Network: | Network (Home/Office) |
| Connection Type: | Wireless 802.11 2.4GHz Access Point |
| Physical Address: | d4:a9:28:00:86:72 |
| MTU: | Automatic 1500 |

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.

## Broadband Ethernet/Coax Connection

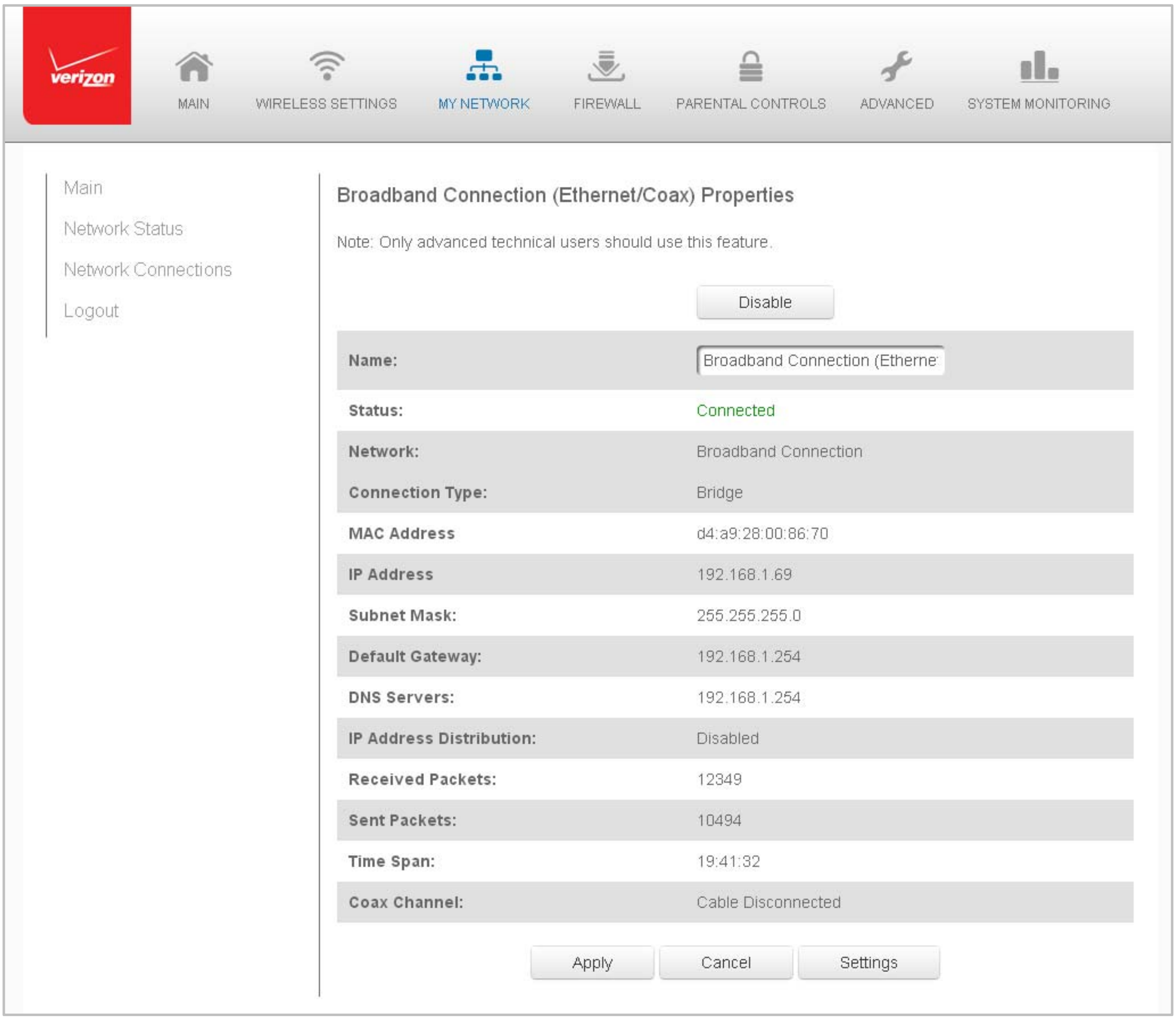
A Broadband Ethernet connection connects computers to your Gateway using Ethernet cables. The connections are either direct or use network hubs and switches.

A Coax connection connects devices, such as set-top boxes, to your Gateway using a coaxial cable.

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

➢ To view the connection:

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



Broadband Connection (Ethernet/Coax) Properties

Note: Only advanced technical users should use this feature.

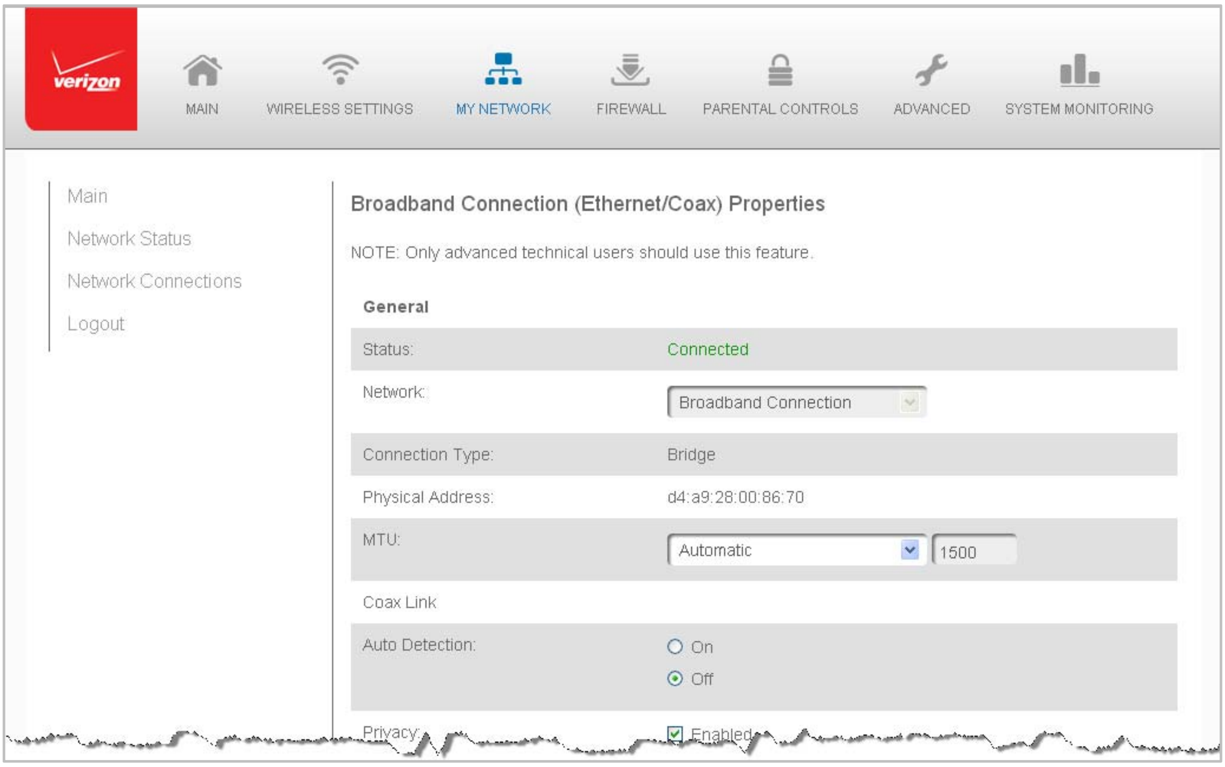
| | |
|---|---|
| Name: | Broadband Connection (Etherne |
| Status: | Connected |
| Network: | Broadband Connection |
| Connection Type: | Bridge |
| MAC Address | d4:a9:28:00:86:70 |
| IP Address | 192.168.1.69 |
| Subnet Mask: | 255.255.255.0 |
| Default Gateway: | 192.168.1.254 |
| DNS Servers: | 192.168.1.254 |
| IP Address Distribution: | Disabled |
| Received Packets: | 12349 |
| Sent Packets: | 10494 |
| Time Span: | 19:41:32 |
| Coax Channel: | Cable Disconnected |

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

## 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) Properties

NOTE: Only advanced technical users should use this feature.

General

| | |
|---|---|
| Status: | Connected |
| Network: | Broadband Connection |
| Connection Type: | Bridge |
| Physical Address: | d4:a9:28:00:86:70 |
| MTU: | Automatic 1500 |
| Coax Link | |
| Auto Detection: | ○ On<br>● Off |
| Privacy: | ☑ Enabled |

2. Configure the following settings, as needed.

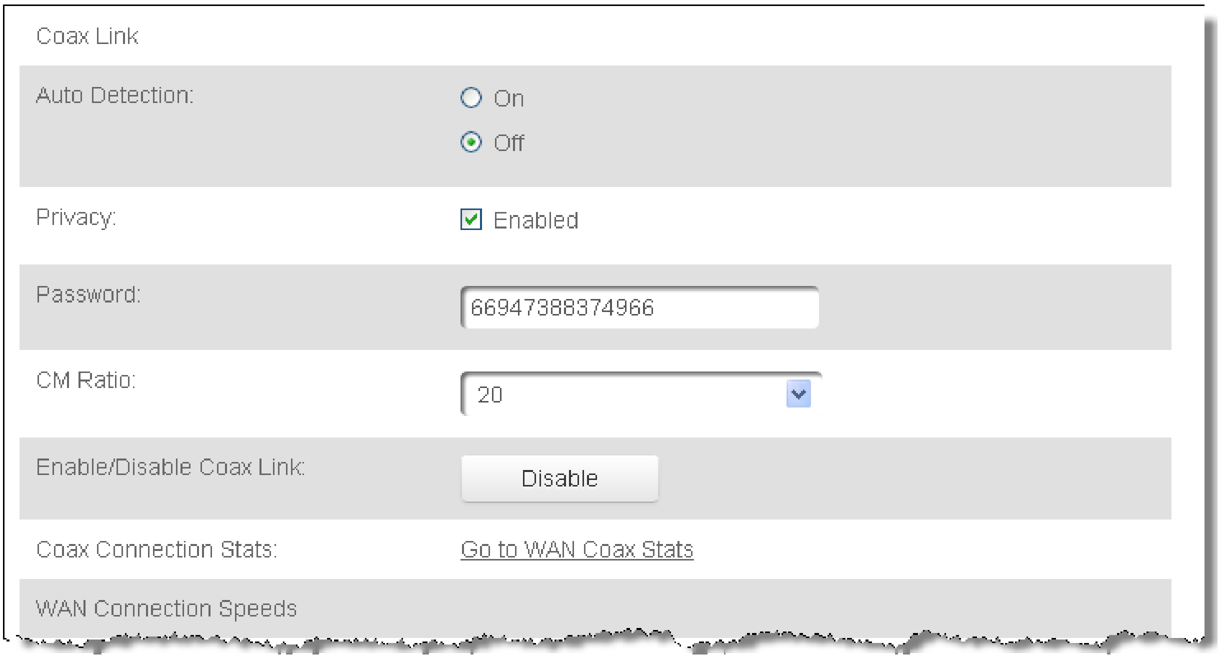
### General

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:
  - **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

### Coax Link

1. To set the Channel, select the coax link channel as 1 to 3.



Coax Link

| | |
|---|---|
| Auto Detection: | ○ On<br>● Off |
| Privacy: | ☑ Enabled |
| Password: | 66947388374966 |
| CM Ratio: | 20 |
| Enable/Disable Coax Link: | Disable |
| Coax Connection Stats: | Go to WAN Coax Stats |

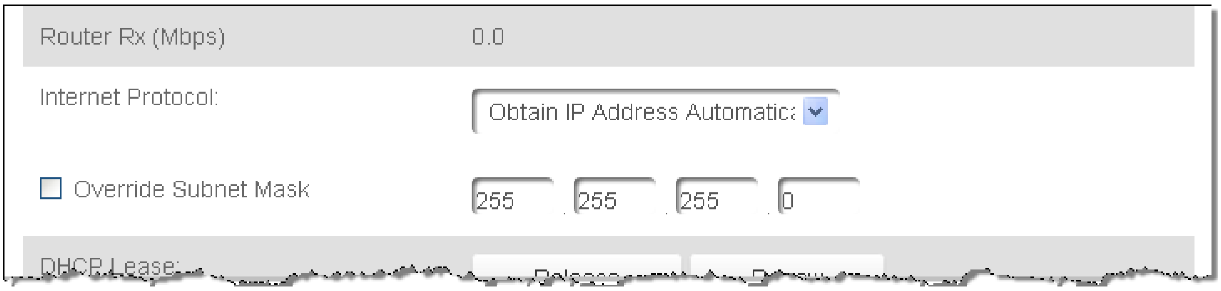
WAN Connection Speeds

2. Select the **On** or **Off** radio button in the **Auto Detection** field.
3. 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.
4. To set the password, enter the Coax Link password in the **Password** field.
5. To set the CM ratio, select the CM ratio in drop down.
6. To enable or disable the Coax link, click **Disable** or **Enable**.
7. To view the devices connected using the coaxial cable, click the **Go to WAN Coax Stats** link.

### 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.



Router Rx (Mbps) 0.0

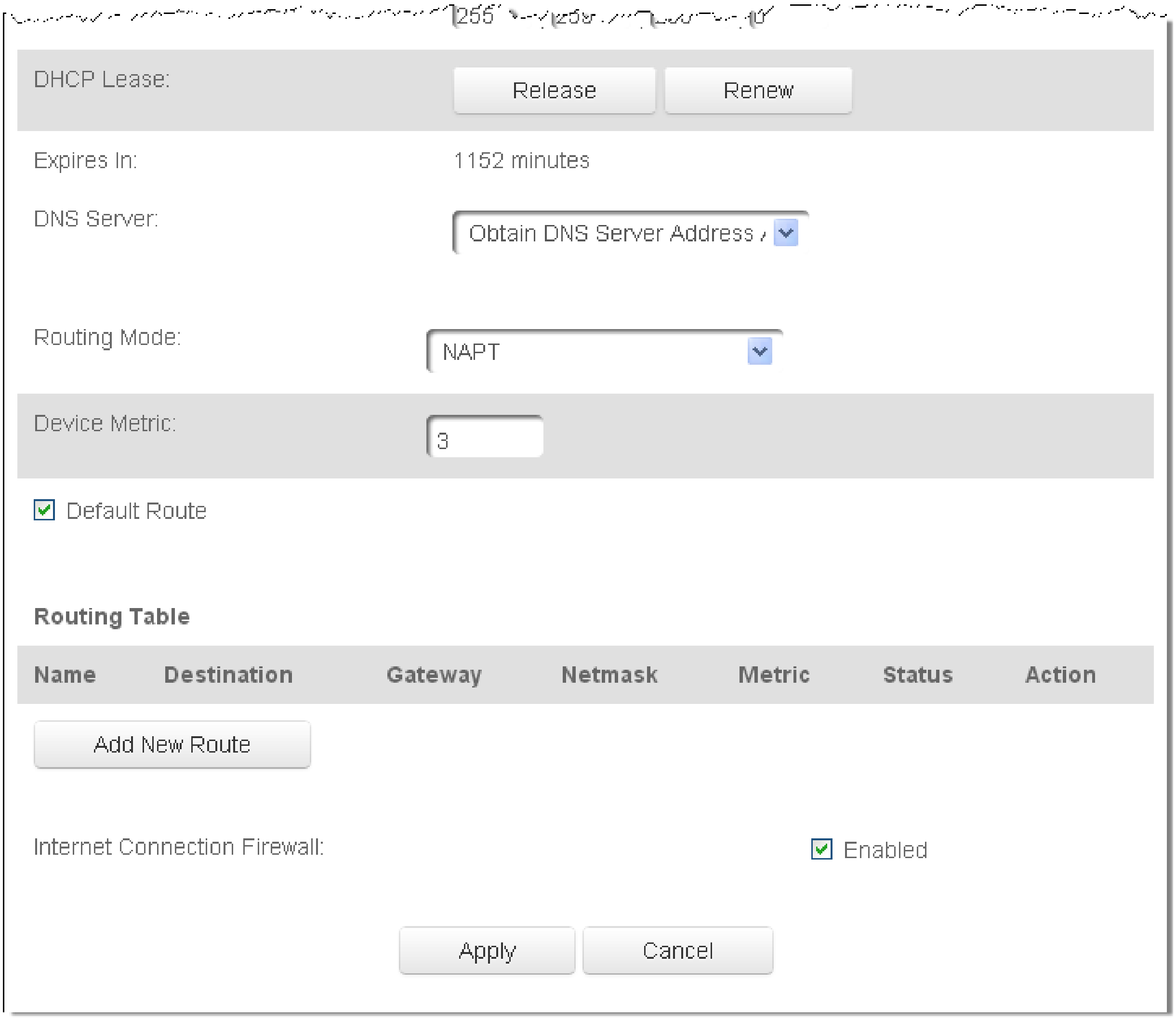
Internet Protocol: Obtain IP Address Automatic

☐ Override Subnet Mask 255 . 255 . 255 . 0

DHCP Lease:

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

**Routing Mode**



DHCP Lease: Release Renew

Expires In: 1152 minutes

DNS Server: Obtain DNS Server Address

Routing Mode: NAPT

Device Metric: 3

☑ Default Route

Routing Table

| Name | Destination | Gateway | Netmask | Metric | Status | Action |
|---|---|---|---|---|---|---|

Add New Route

Internet Connection Firewall: ☑ Enabled

Apply Cancel

### Complete all Ethernet/Coax Connection Configuration Updates

➢ To save your changes:

1. Click **Apply**.

# Chapter 6 Configuring Security Settings

Your Gateway’s security suite includes comprehensive and robust security services, such as stateful packet inspection, firewall security, user authentication protocols, and password protection mechanisms. These features help protect your computers from security threats on the Internet.

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 specific services provided by computers on the local network
- **Port Triggering** – define port triggering entries to dynamically open the firewall for specific protocols or ports
- **Remote Administration** – enable remote configuration of your Gateway 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

## Firewall

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

The firewall provides both the security and flexibility 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 Gateway or rejected and barred from passing through your Gateway, according to a flexible and configurable set of rules. These rules are designed to prevent unwanted intrusions from the outside, while allowing local network users access to Internet services.

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

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 Gateway, the firewall identifies the request type and origin, such as HTTP and a specific computer in the local network. Unless your Gateway is configured to block requests of this type from this computer, the firewall allows this type of request to pass to the Internet.

When the website is returned from the web server, the firewall associates the website with this session and allows it to pass; regardless HTTP access from the Internet to the local network is blocked or permitted.

It is the origin of the request, not subsequent responses to this request, which determines whether a session can be established.

## 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<br>Incoming Traffic | Local Network Requests<br>Outgoing Traffic |
|---|---|---|
| Maximum | Blocked | Limited |
| Typical | Blocked | Unrestricted |
| Minimum | Unrestricted | Unrestricted |

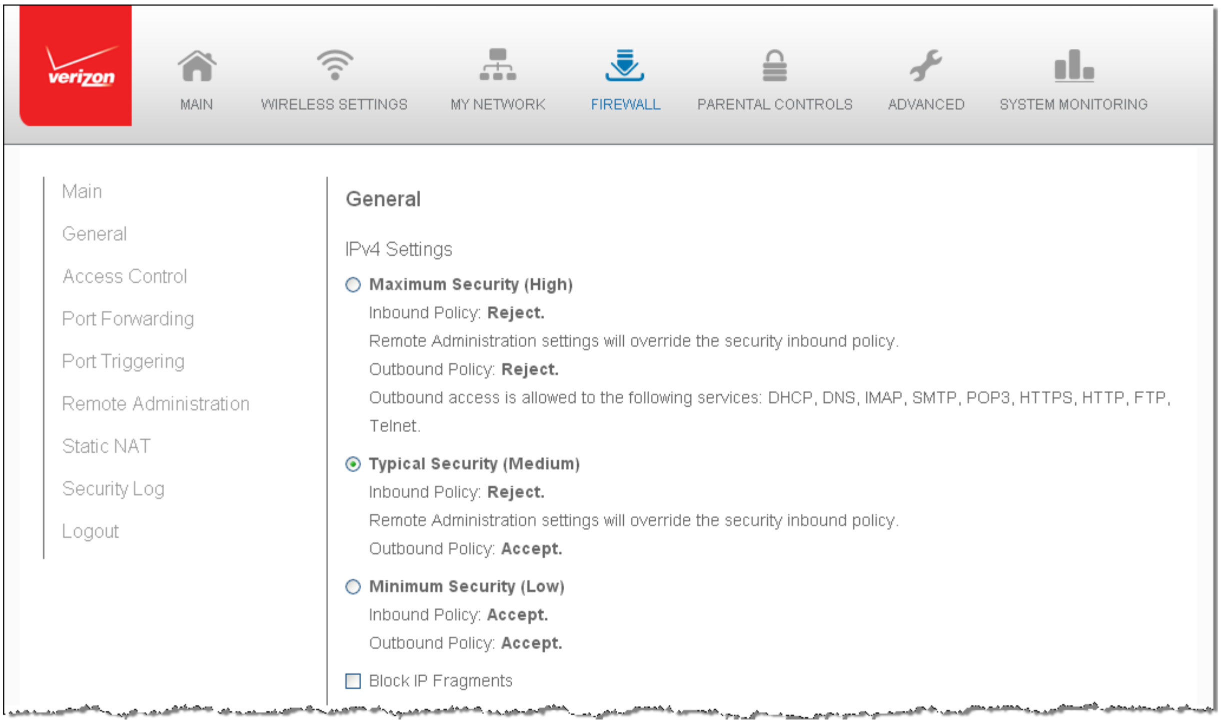
The request access is defined as:

- **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

## Specifying General Settings for IPv4 or IPv6

➢ To set your firewall configuration:

1. Click the **Firewall Settings** icon. The General Settings page displays.



General

IPv4 Settings

○ **Maximum Security (High)**

Inbound Policy: **Reject.**

Remote Administration settings will override the security inbound policy.

Outbound Policy: **Reject.**

Outbound access is allowed to the following services: DHCP, DNS, IMAP, SMTP, POP3, HTTPS, HTTP, FTP, Telnet.

● **Typical Security (Medium)**

Inbound Policy: **Reject.**

Remote Administration settings will override the security inbound policy.

Outbound Policy: **Accept.**

○ **Minimum Security (Low)**

Inbound Policy: **Accept.**

Outbound Policy: **Accept.**

□ Block IP Fragments

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. To protect the local network from a common type of hacker attack that uses fragmented data packets to sabotage the network, select the **Block IP Fragments** check box.

   VPN over IPSec and some UDP-based services make legitimate use of IP fragments. IP fragments must be allowed to pass into the local network to use these services.

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

## Access Control

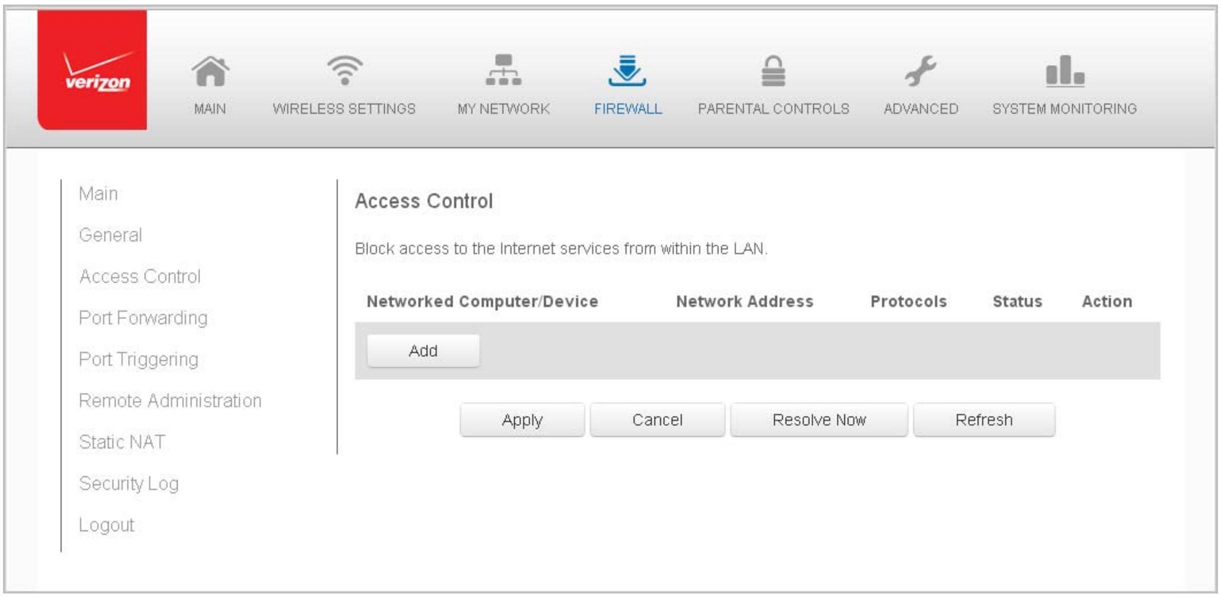
You can block individual computers on your local network from accessing specific services on the Internet. For example, you could block one computer from accessing the Internet, then block a second computer from transferring files using FTP as well as prohibit the computer from receiving incoming email.

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

### Allow or Restrict Services

➢ To allow or restrict services:

1. From the 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.

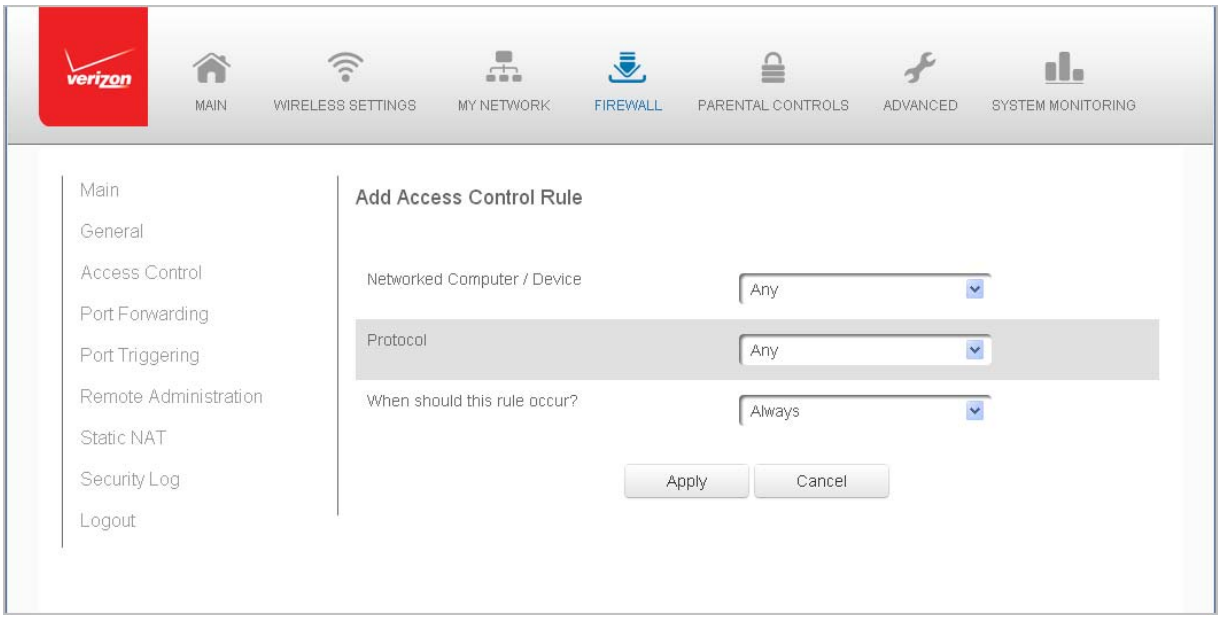


Access Control

Block access to the Internet services from within the LAN.

| Networked Computer/Device | Network Address | Protocols | Status | Action |
|---|---|---|---|---|

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



Add Access Control Rule

| | |
|---|---|
| Networked Computer / Device | Any |
| Protocol | Any |
| When should this rule occur? | Always |

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.

## 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.

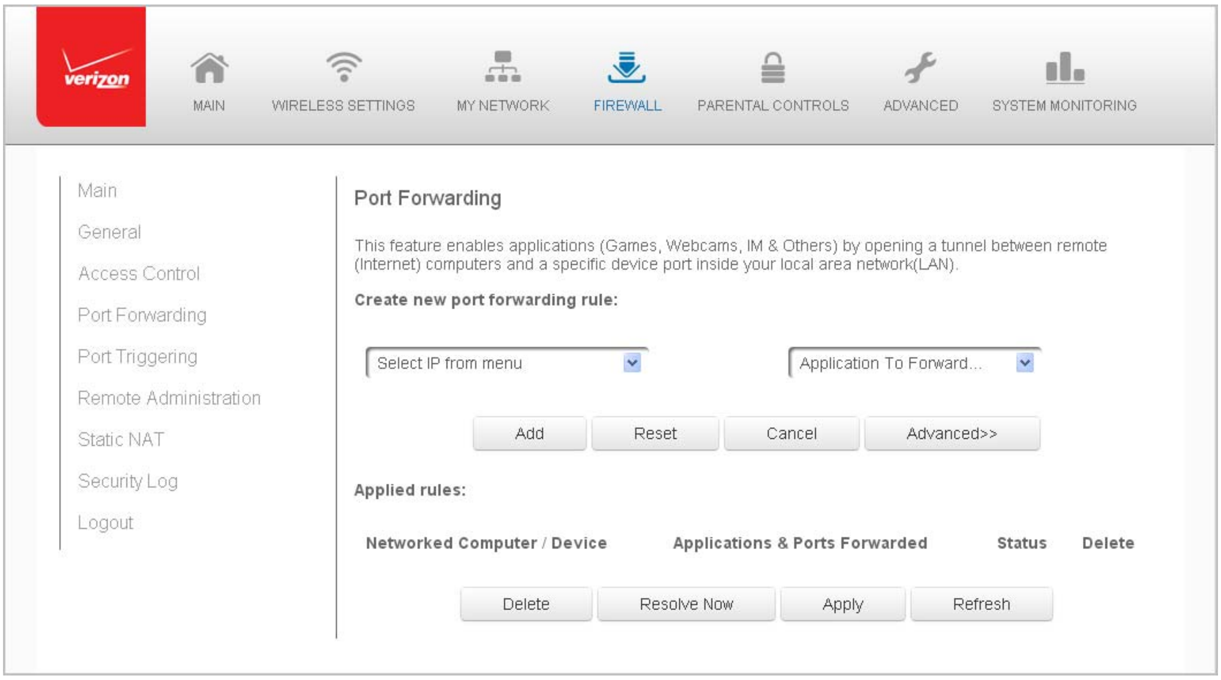
- To disable an access control, clear the check box next to the service name.
- To reinstate the restriction, select the check box next to the service name.
- To remove an access restriction, select the service and click Remove. The service is removed from the Access Control table.

## 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.



Port Forwarding

This feature enables applications (Games, Webcams, IM & Others) by opening a tunnel between remote (Internet) computers and a specific device port inside your local area network(LAN).

**Create new port forwarding rule:**

**Applied rules:**

| Networked Computer / Device | Applications & Ports Forwarded | Status | Delete |
|---|---|---|---|

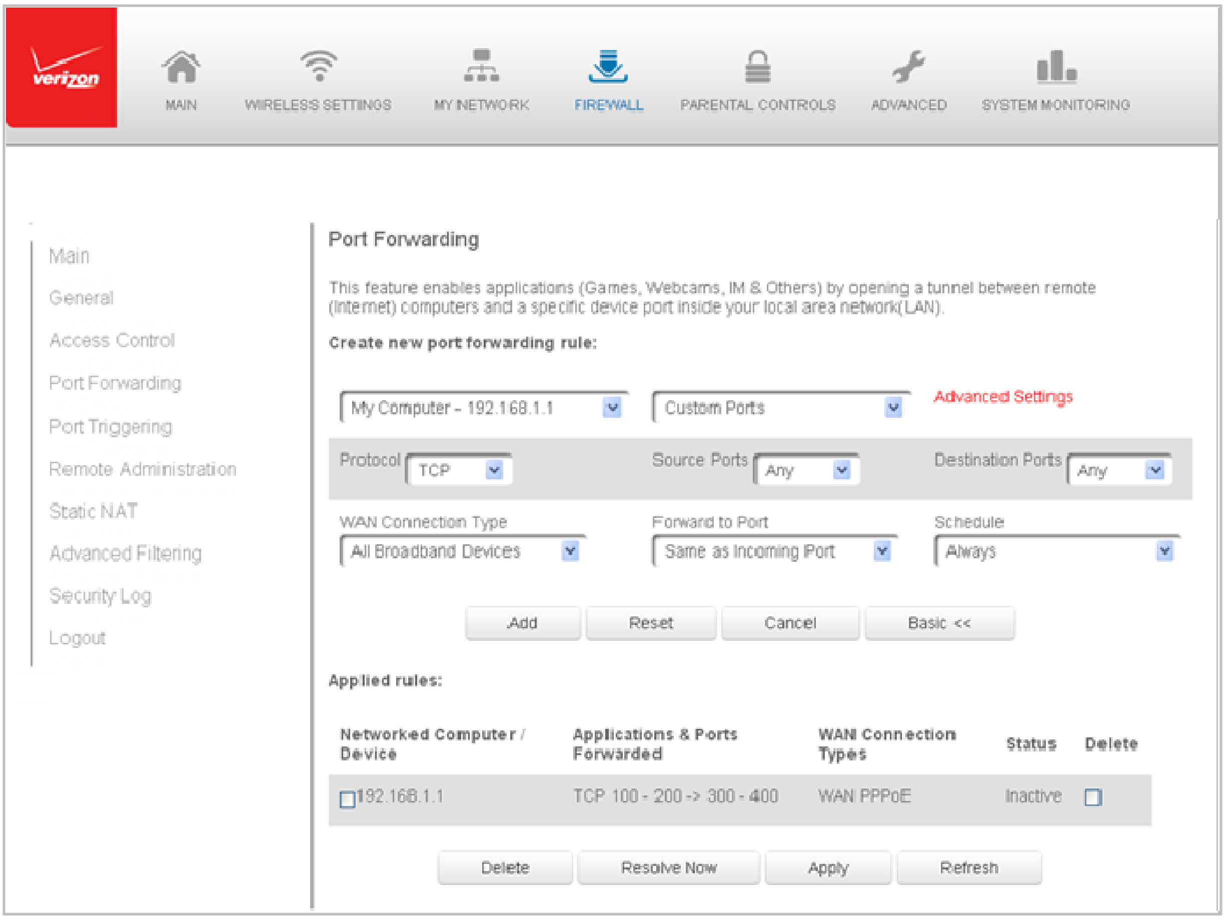
2. To create a new rule, select the IP address in the **Select IP from Menu** drop down.
3. Select the application in the **Application to Forward** drop down.
4. Click **Add**. The rule displays in the **Applied Rules** section.
5. Click **Apply** to save changes.

## Advanced Port Forwarding Rules

You can configure advanced port forwarding rules.

➢ To configure the rules:

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



Port Forwarding

This feature enables applications (Games, Webcams, IM & Others) by opening a tunnel between remote (Internet) computers and a specific device port inside your local area network(LAN).

Create new port forwarding rule:

My Computer - 192.168.1.1 | Custom Ports

Protocol: TCP | Source Ports: Any | Destination Ports: Any

WAN Connection Type: All Broadband Devices | Forward to Port: Same as Incoming Port | Schedule: Always

Applied rules:

| Networked Computer / Device | Applications & Ports Forwarded | WAN Connection Types | Status | Delete |
|---|---|---|---|---|
| □192.168.1.1 | TCP 100 - 200 -> 300 - 400 | WAN PPPoE | Inactive | □ |

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.

## 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.

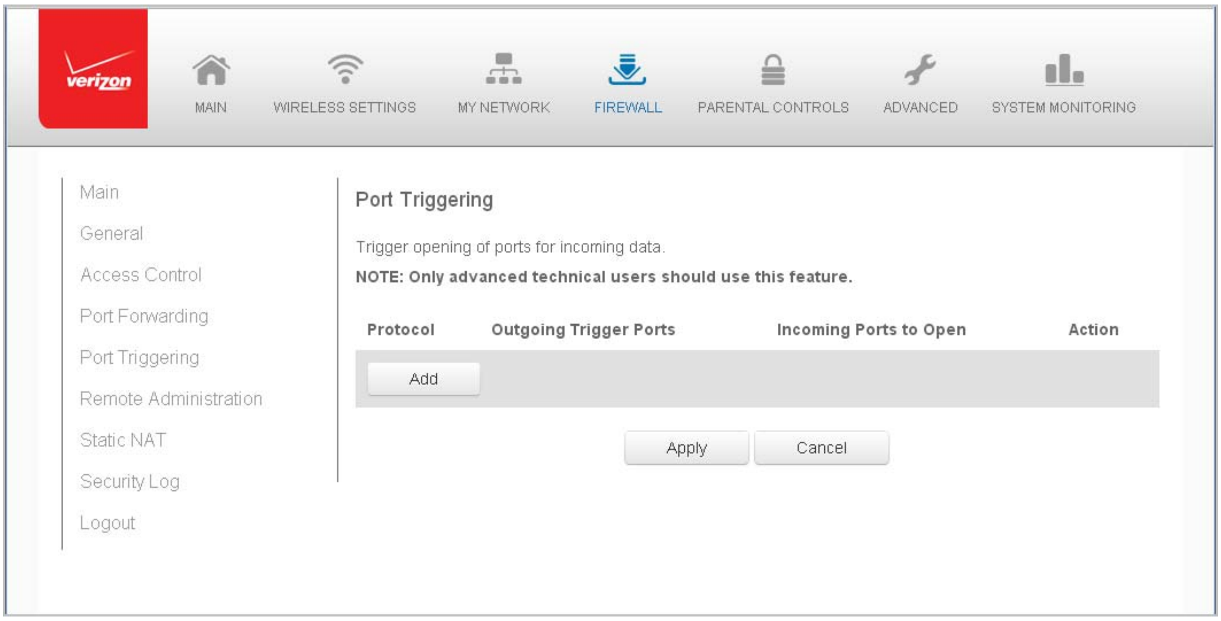
In this case, port triggering must be used since it conflicts with the following default firewall settings:

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

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

➢ To configure port triggering:

1. Select **Port Triggering**.



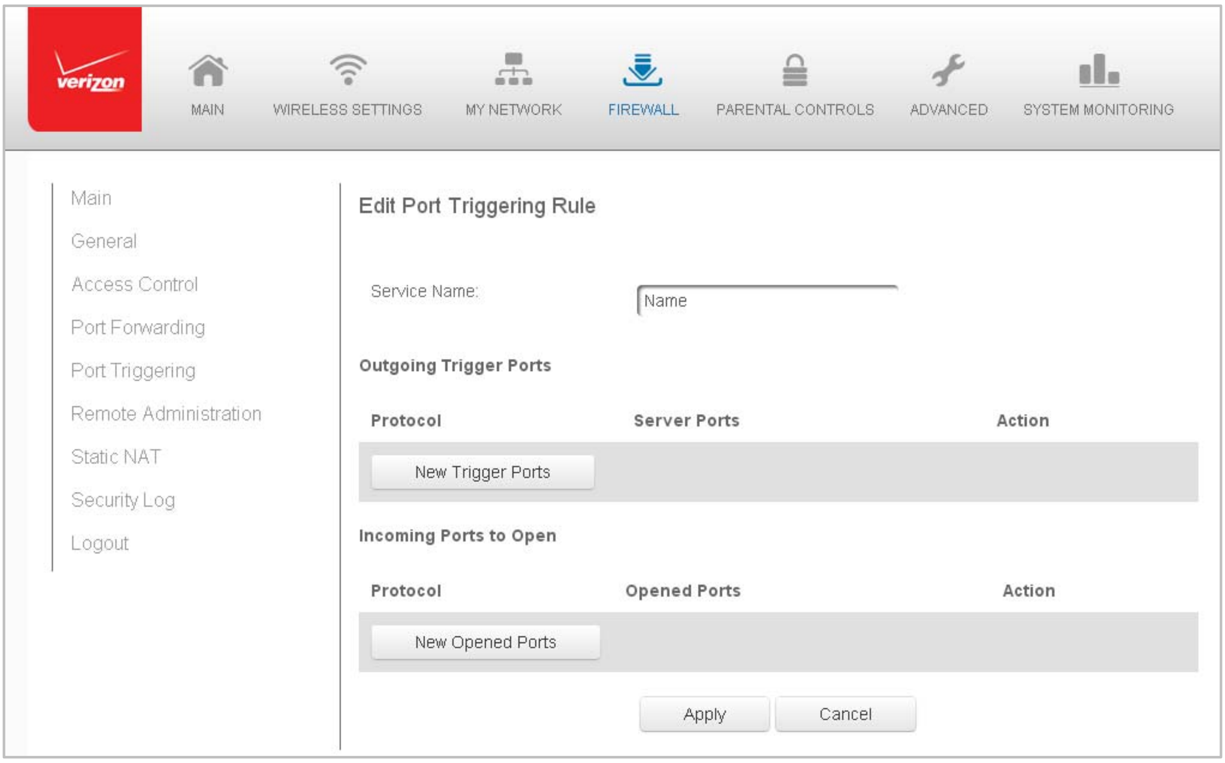
Port Triggering

Trigger opening of ports for incoming data.

**NOTE: Only advanced technical users should use this feature.**

| Protocol | Outgoing Trigger Ports | Incoming Ports to Open | Action |
|---|---|---|---|

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



Edit Port Triggering Rule

Service Name: Name

Outgoing Trigger Ports

| Protocol | Server Ports | Action |
|---|---|---|

Incoming Ports to Open

| Protocol | Opened Ports | Action |
|---|---|---|

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.

## Remote Administration

**Caution!** Enabling Remote Administration places your Gateway network at risk from outside attacks.

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

You can allow incoming access to the following:

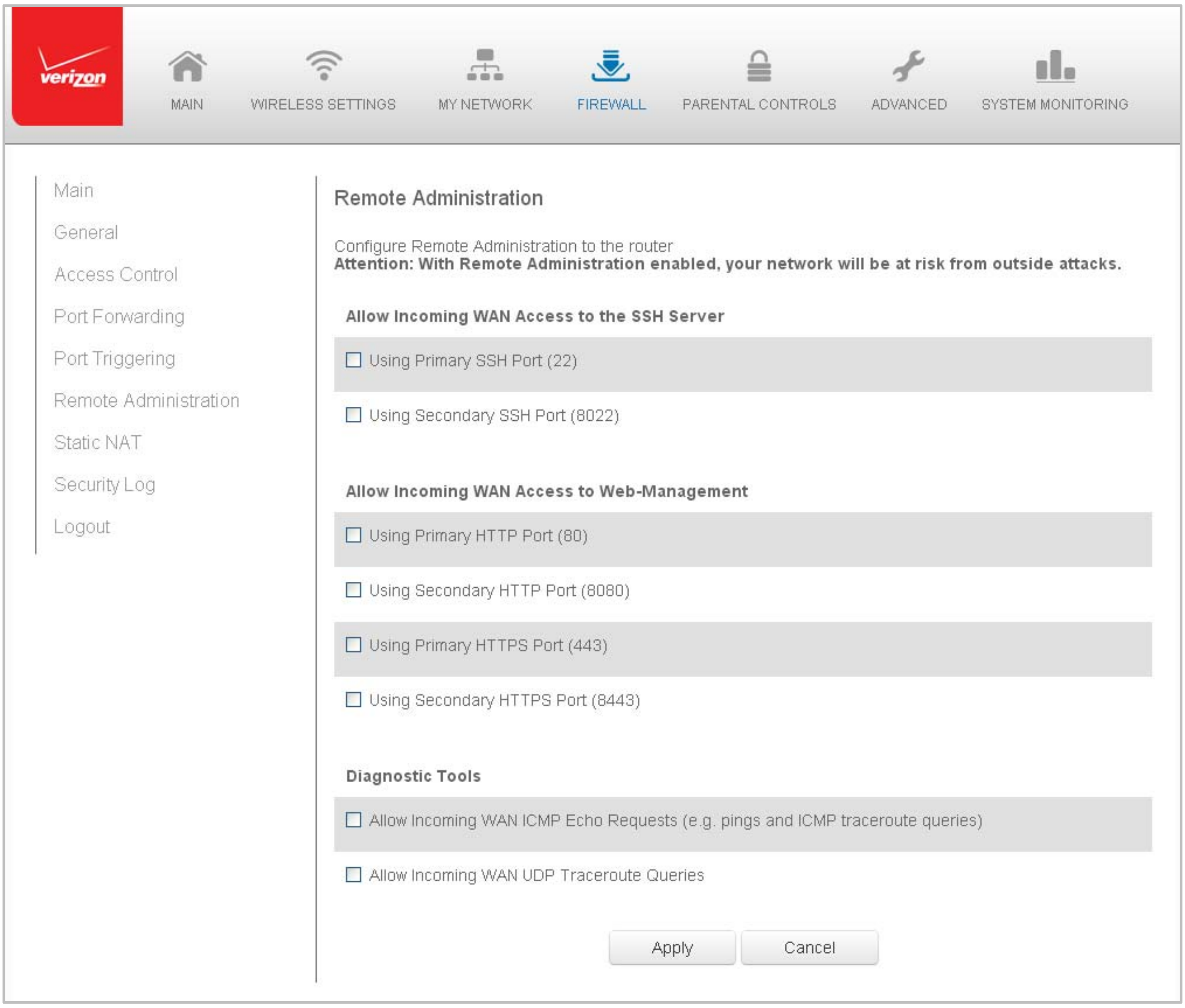
- **SSH Access** – used to create a command-line session and gain access to all system settings and parameters using a text-based terminal.
- **Web Management** – used to obtain access to your Gateway's GUI and gain access to all settings and parameters through a web browser. Both secure HTTPS and non-secure HTTP access is available.
- **Diagnostic Tools** – used for troubleshooting and remote system management by a user or Verizon.

SSH and 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 Gateway 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 Gateway for the first time using encrypted remote administration, a warning page opens with a certificate authentication message displayed. This is due to your Gateway 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.

➢ To enable remote administration:

1. Select **Remote Administration**.



Remote Administration

Configure Remote Administration to the router
**Attention: With Remote Administration enabled, your network will be at risk from outside attacks.**

**Allow Incoming WAN Access to the SSH Server**

☐ Using Primary SSH Port (22)

☐ Using Secondary SSH Port (8022)

**Allow Incoming WAN Access to Web-Management**

☐ Using Primary HTTP Port (80)

☐ Using Secondary HTTP Port (8080)

☐ Using Primary HTTPS Port (443)

☐ Using Secondary HTTPS Port (8443)

**Diagnostic Tools**

☐ Allow Incoming WAN ICMP Echo Requests (e.g. pings and ICMP traceroute queries)

☐ Allow Incoming WAN UDP Traceroute Queries

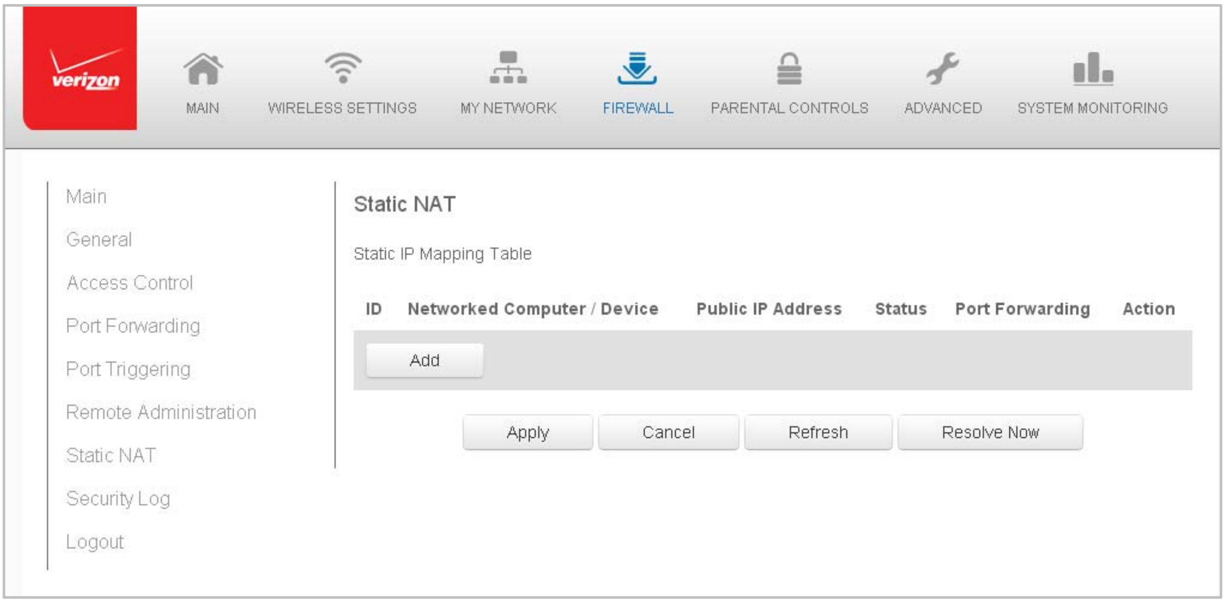
2. To enable access, select the check box.
3. Click **Apply** to save changes.
4. To remove access, clear the check box.
5. Click **Apply** again to save changes.

## 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.

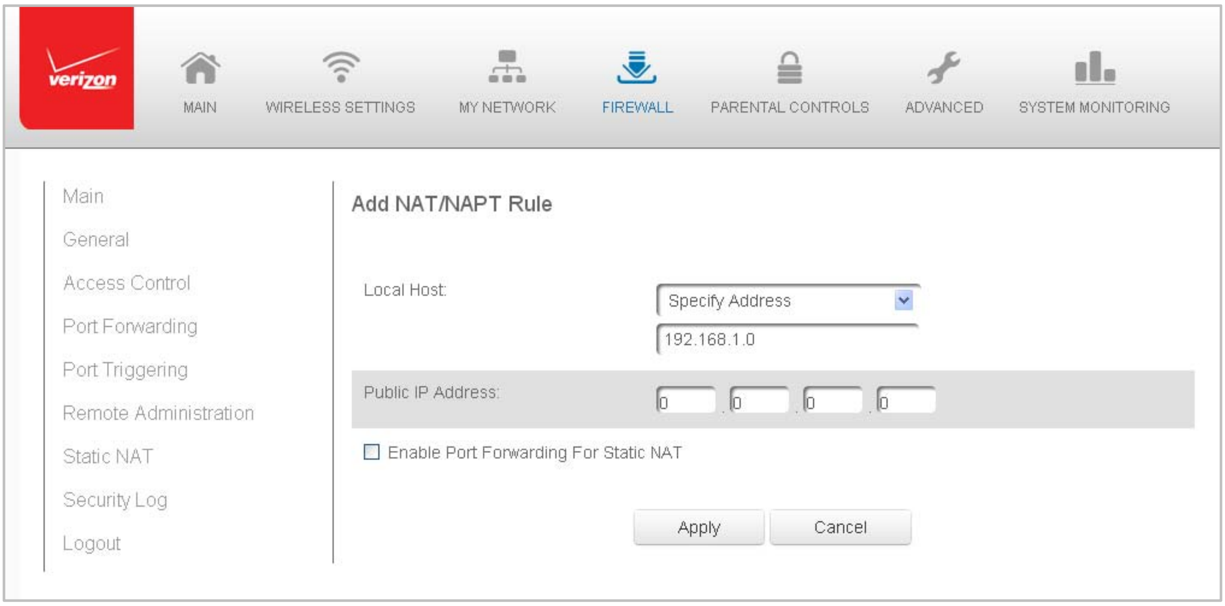


Static NAT

Static IP Mapping Table

| ID | Networked Computer / Device | Public IP Address | Status | Port Forwarding | Action |
|---|---|---|---|---|---|

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



Add NAT/NAPT Rule

Local Host: Specify Address 192.168.1.0

Public IP Address: 0 . 0 . 0 . 0

□ Enable Port Forwarding For Static NAT

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.

## Security Log

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

The security log reports the following information:

- **Time** – based on the date and time in your Gateway
- **Event** – consists of firewall information, firewall setup, and system log
- **Event Type** – 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 control.

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.

## Event Types

The security logs records the following event types:

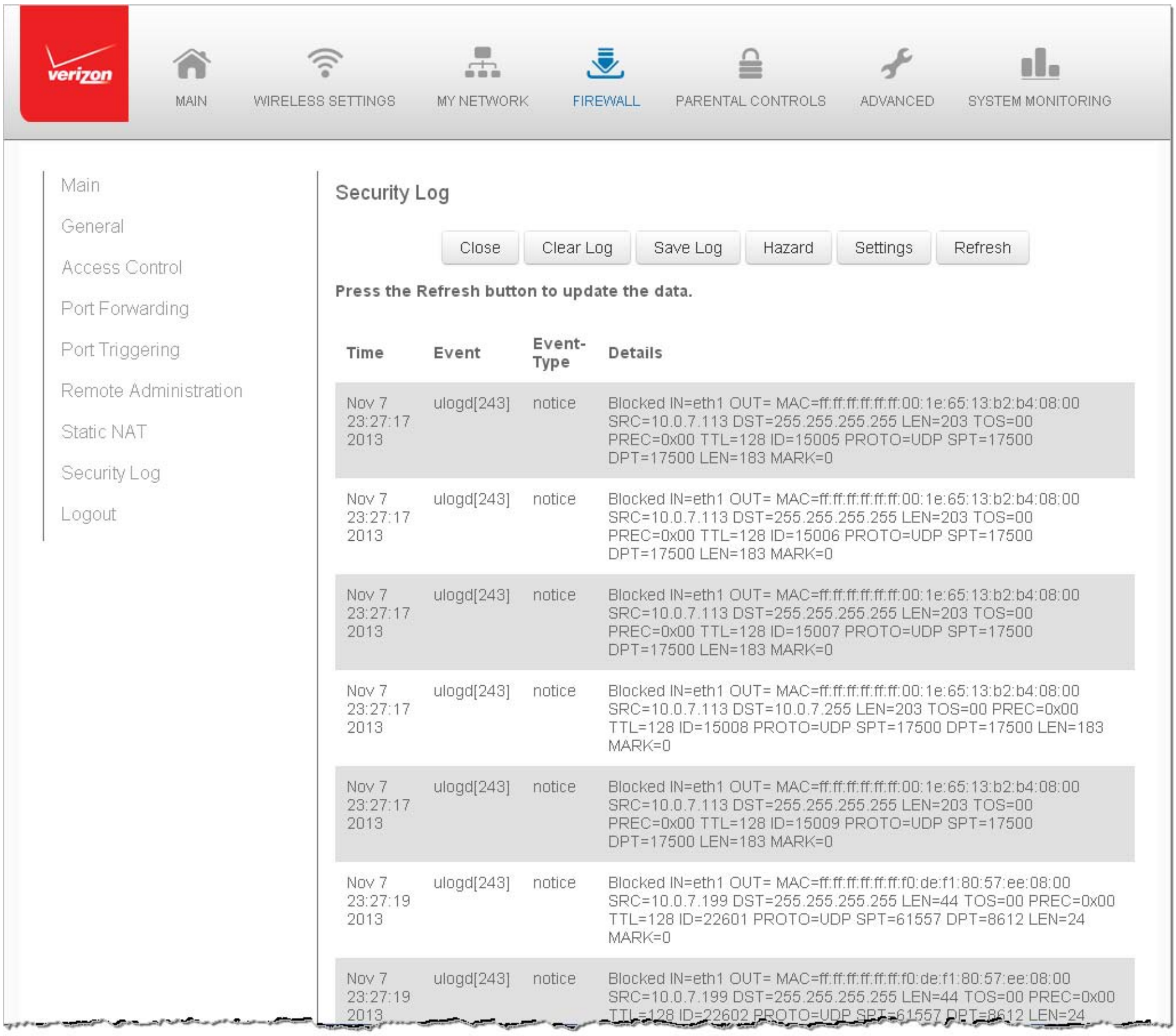
- **Access control** – a packet has been accepted/blocked due to an access control rule.
- **Advance filter rule** – a packet has been accepted/blocked due to an advanced filter rule.
- **ARP** – an ARP packet has been accepted.
- **AUTH:113 request** - an outbound packet for AUTH protocol has been accepted (for maximum security level).
- **Broadcast/Multicast protection** – a packet with a broadcast/multicast source IP has been blocked.
- **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 Gateway sent a DHCP request (depends on the distribution).
- **DHCP response** - your Gateway 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.
- **Malformed packet: Failed parsing** – a packed has been blocked because it is malformed.
- **Maximum security enabled service** – a packet has been accepted because it belongs to a permitted service in the maximum security level.
- **Multicast IGMP connection** – a multicast packet has been accepted.
- **NAT Error: Connection pool is full** - No connection created – a connection has not been created because the connection pool is full.
- **NAT Error: Conflict mapping already exists** – a conflict occurred because the NAT mapping already exists, so NAT failed.
- **NAT Error: No free NAT IP** – no free NAT IP, so NAT has failed.
- **NAT out failed** – NAT failed for this packet.
- **Outbound Auth1X** – an outbound Auth1X packet has been accepted.
- **Packet invalid in connection** – an invalid connection packet has been blocked.
- **Parental control** – a package has been block because of parental control.
- **Passive attack on ftp-server: Client attempted to open Server ports** – a packet has been blocked.
- **Service** – a packet has been accepted because of a certain service, as specified in the event type.
- **Spoofing protection** – a packet from the Internet with a source IP belong to the local network has been blocked.
- **STP packet** – STP (Spanning Tree Protocol) packet has been accepted/rejected.
- **SynCookies protection** – a SynCookies packet has been blocked.

- **Trusted device** – a packet from a trusted device has been accepted.
- **UDP flood protection** – a packed has been blocked, stopping a UDP flood.
- **User authentication** – a message arrived during login time, including both successful and failed authentication.
- **Wildcard connection hooked** – debug message regarding connection.
- **Wildcard connection opened** - debug message regarding connection.
- **WinNuke protection** – a WinNuke attack has been blocked.

➢ To view the security log:

1. Select **Security Log**.

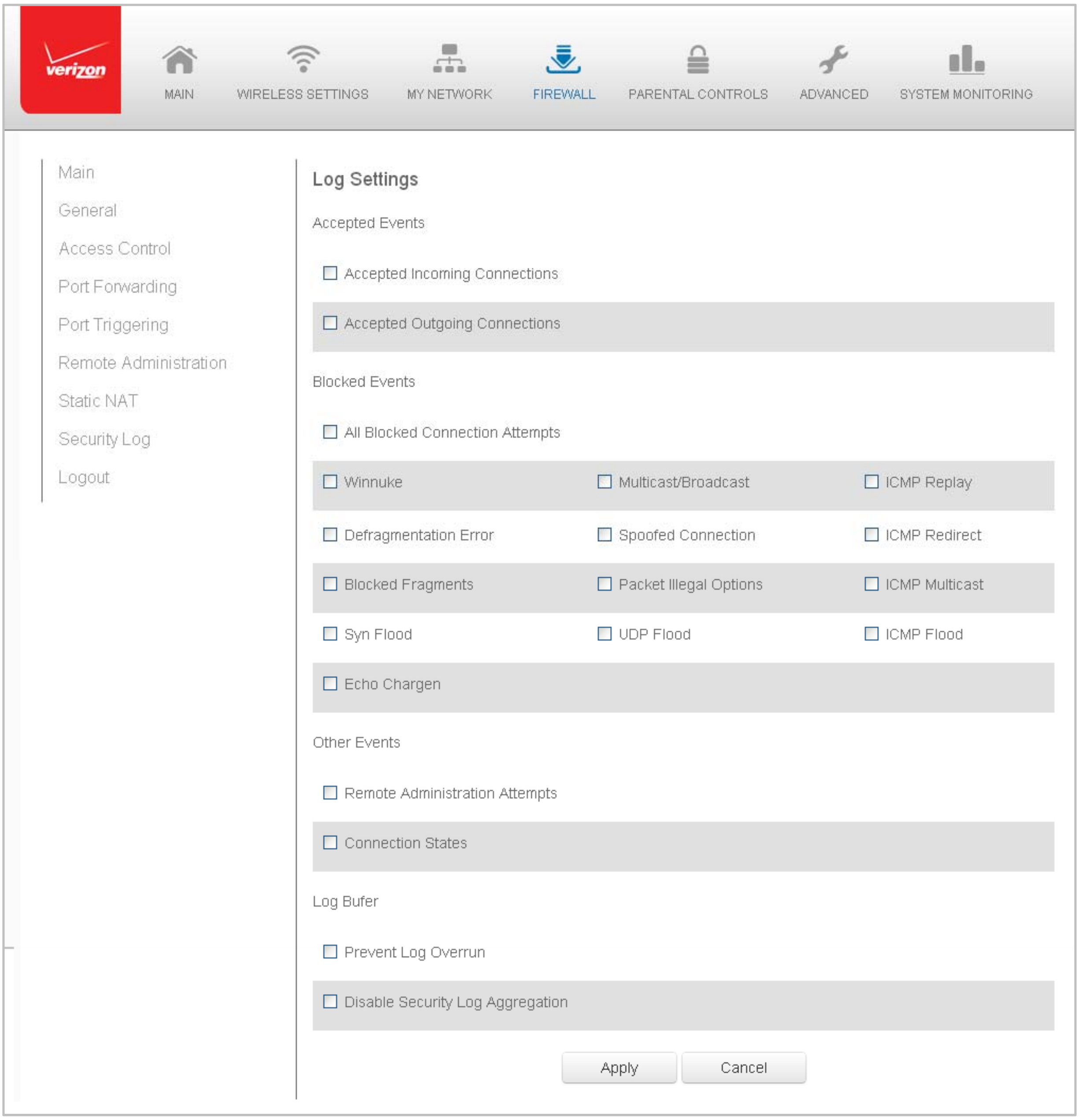


Security Log

Press the Refresh button to update the data.

| Time | Event | Event-Type | Details |
|---|---|---|---|
| Nov 7 23:27:17 2013 | ulogd[243] | notice | Blocked IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:1e:65:13:b2:b4:08:00 SRC=10.0.7.113 DST=255.255.255.255 LEN=203 TOS=00 PREC=0x00 TTL=128 ID=15005 PROTO=UDP SPT=17500 DPT=17500 LEN=183 MARK=0 |
| Nov 7 23:27:17 2013 | ulogd[243] | notice | Blocked IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:1e:65:13:b2:b4:08:00 SRC=10.0.7.113 DST=255.255.255.255 LEN=203 TOS=00 PREC=0x00 TTL=128 ID=15006 PROTO=UDP SPT=17500 DPT=17500 LEN=183 MARK=0 |
| Nov 7 23:27:17 2013 | ulogd[243] | notice | Blocked IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:1e:65:13:b2:b4:08:00 SRC=10.0.7.113 DST=255.255.255.255 LEN=203 TOS=00 PREC=0x00 TTL=128 ID=15007 PROTO=UDP SPT=17500 DPT=17500 LEN=183 MARK=0 |
| Nov 7 23:27:17 2013 | ulogd[243] | notice | Blocked IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:1e:65:13:b2:b4:08:00 SRC=10.0.7.113 DST=10.0.7.255 LEN=203 TOS=00 PREC=0x00 TTL=128 ID=15008 PROTO=UDP SPT=17500 DPT=17500 LEN=183 MARK=0 |
| Nov 7 23:27:17 2013 | ulogd[243] | notice | Blocked IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:1e:65:13:b2:b4:08:00 SRC=10.0.7.113 DST=255.255.255.255 LEN=203 TOS=00 PREC=0x00 TTL=128 ID=15009 PROTO=UDP SPT=17500 DPT=17500 LEN=183 MARK=0 |
| Nov 7 23:27:19 2013 | ulogd[243] | notice | Blocked IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:f0:de:f1:80:57:ee:08:00 SRC=10.0.7.199 DST=255.255.255.255 LEN=44 TOS=00 PREC=0x00 TTL=128 ID=22601 PROTO=UDP SPT=61557 DPT=8612 LEN=24 MARK=0 |
| Nov 7 23:27:19 2013 | ulogd[243] | notice | Blocked IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:f0:de:f1:80:57:ee:08:00 SRC=10.0.7.199 DST=255.255.255.255 LEN=44 TOS=00 PREC=0x00 TTL=128 ID=22602 PROTO=UDP SPT=61557 DPT=8612 LEN=24 |

2. To modify the types of events that display in the log, click **Settings**.



Log Settings

Accepted Events

☐ Accepted Incoming Connections

☐ Accepted Outgoing Connections

Blocked Events

☐ All Blocked Connection Attempts

☐ Winnuke ☐ Multicast/Broadcast ☐ ICMP Replay

☐ Defragmentation Error ☐ Spoofed Connection ☐ ICMP Redirect

☐ Blocked Fragments ☐ Packet Illegal Options ☐ ICMP Multicast

☐ Syn Flood ☐ UDP Flood ☐ ICMP Flood

☐ Echo Chargen

Other Events

☐ Remote Administration Attempts

☐ Connection States

Log Bufer

☐ Prevent Log Overrun

☐ Disable Security Log Aggregation

3. In the **Accepted Events** section, select the type of activities that generates a log message:

   - **Accepted Incoming Connections** – generates a log message for each successful attempt to establish an inbound connection to the local network.

   - **Accepted Outgoing Connections** - generates a log message for each successful attempt to establish an outbound connection to the public network.

4. In the **Blocked Events** section, select the type of blocked events you want logged.

5. To log a message for each remote administration connection attempt, click the **Remote Administration Attempts** check box.

6. To log the connection for handling by the firewall and application level Gateways, click the **Connection States** check box.

7. Click **Apply** to save changes. The Security Log page displays.

# Chapter 7 Setting Parental Controls

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

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

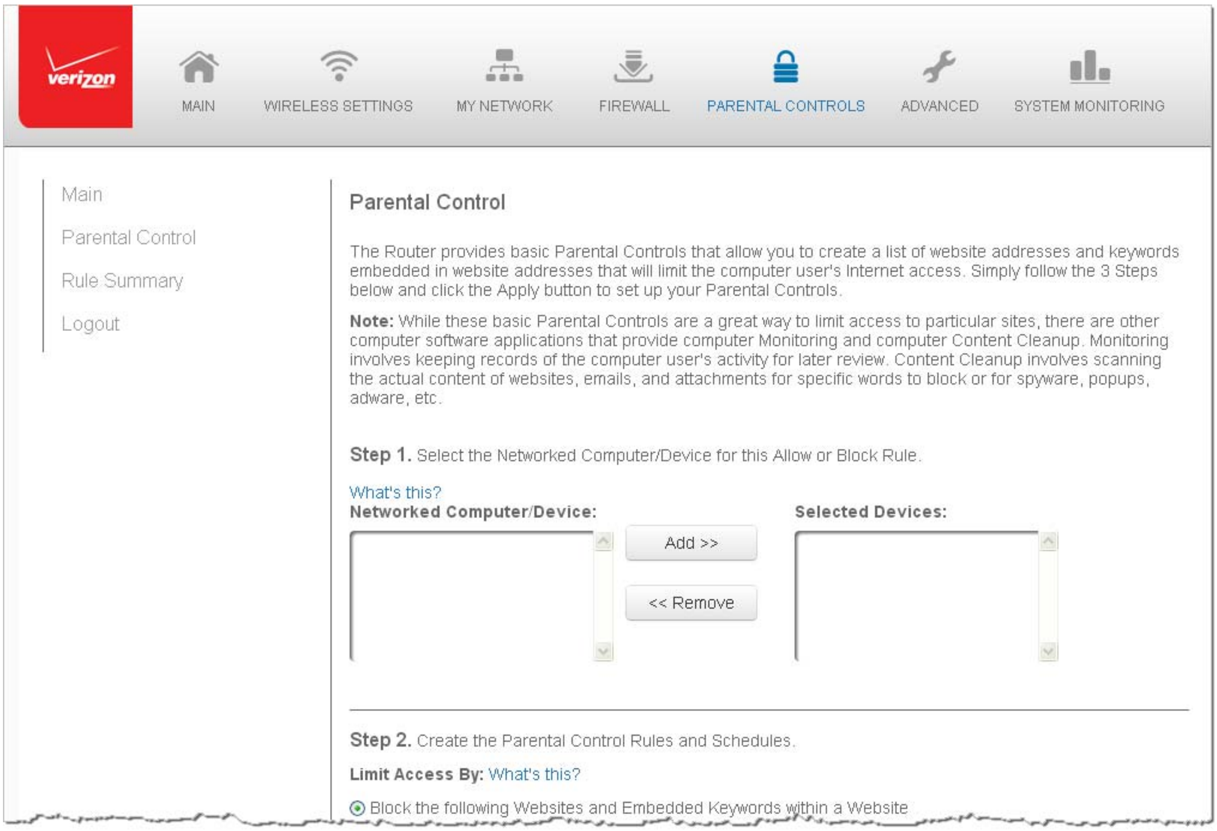
## Activating Parental Controls

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

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

➢ To limit computer access:

1. Select **Parental Control**.



Parental Control

The Router provides basic Parental Controls that allow you to create a list of website addresses and keywords embedded in website addresses that will limit the computer user's Internet access. Simply follow the 3 Steps below and click the Apply button to set up your Parental Controls.

**Note:** While these basic Parental Controls are a great way to limit access to particular sites, there are other computer software applications that provide computer Monitoring and computer Content Cleanup. Monitoring involves keeping records of the computer user's activity for later review. Content Cleanup involves scanning the actual content of websites, emails, and attachments for specific words to block or for spyware, popups, adware, etc.

Step 1. Select the Networked Computer/Device for this Allow or Block Rule.

What's this?
Networked Computer/Device:

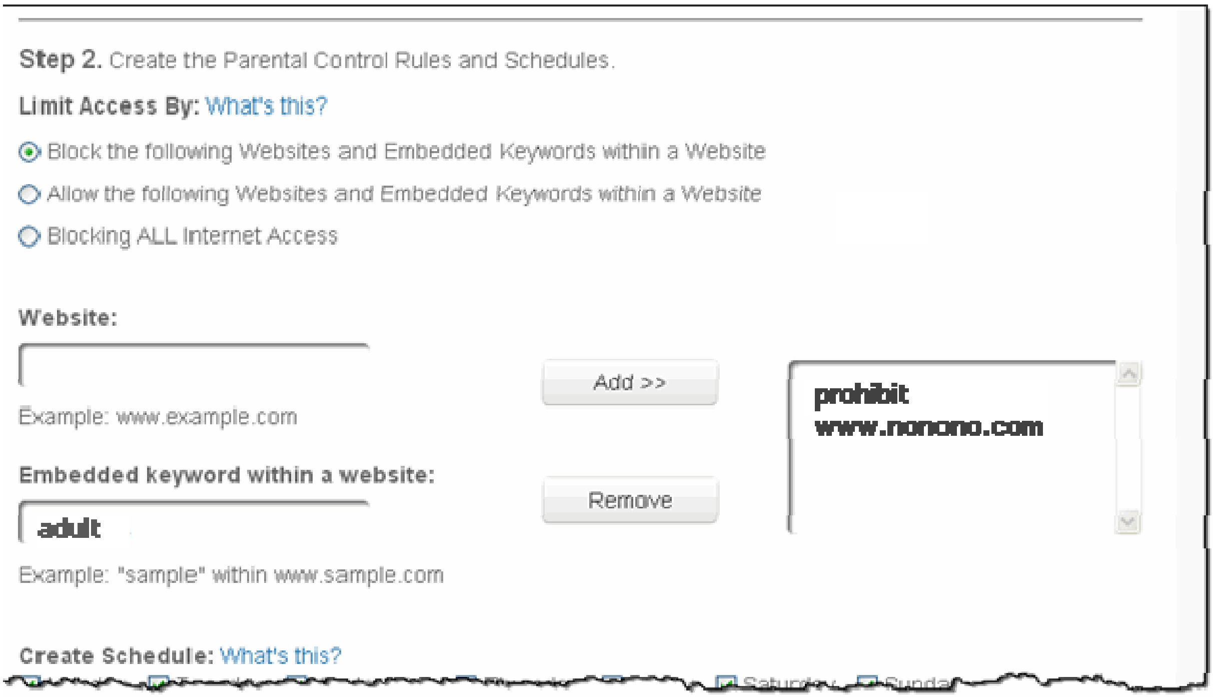
Selected Devices:

Step 2. Create the Parental Control Rules and Schedules.

Limit Access By: What's this?

● Block the following Websites and Embedded Keywords within a Website

2. In **Step 1**, select the computers or device where you are limiting access in the **Networked Computer/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 **Networked Computer/Device** 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 Website** – blocks the specified websites and websites with names contained the specified keyword.
   - **Allow the following Websites and Embedded Keywords within a Website** – allows the specified websites and websites with names contained the specified keyword.
   - **Block ALL Internet Access** – will not allow the device to access the Internet.
5. Enter the name of the website or keyword, then click **Add**.



**Step 2.** Create the Parental Control Rules and Schedules.

**Limit Access By:** What's this?

● Block the following Websites and Embedded Keywords within a Website

○ Allow the following Websites and Embedded Keywords within a Website

○ Blocking ALL Internet Access

**Website:**

Example: www.example.com

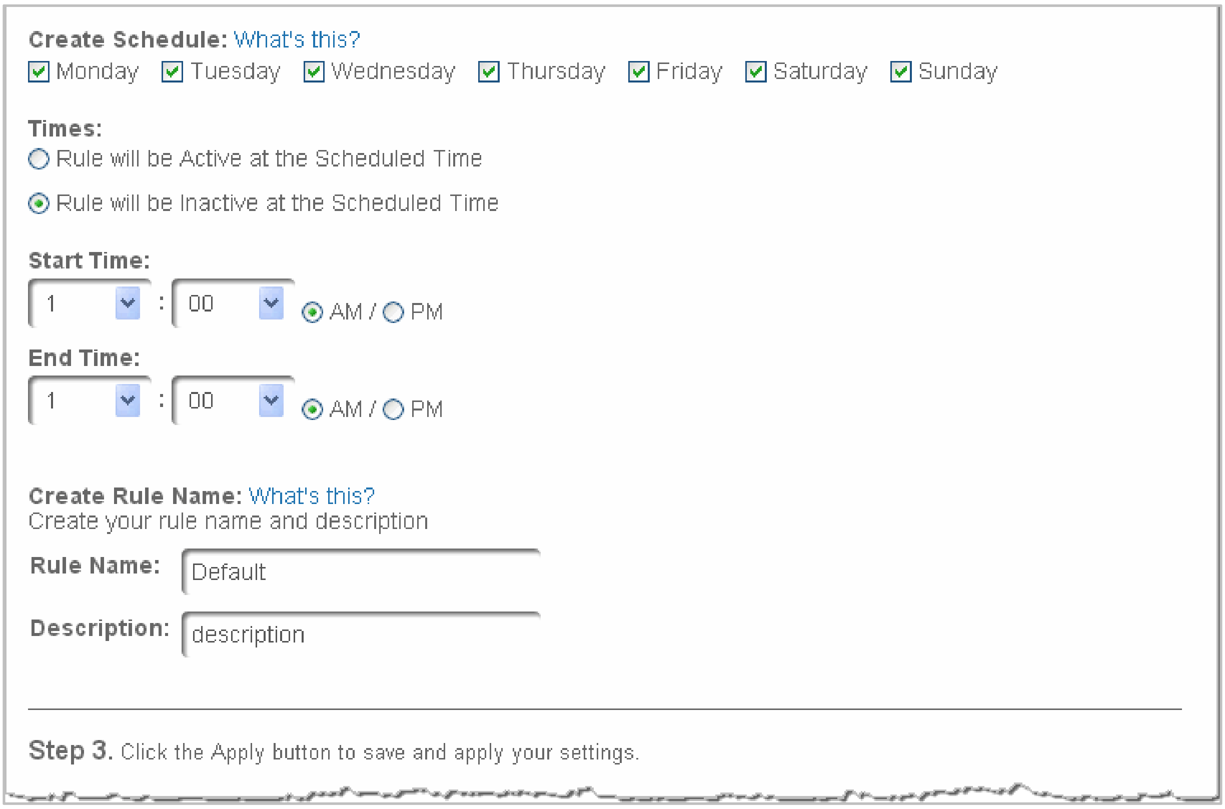
**Embedded keyword within a website:** adult

Example: "sample" within www.sample.com

prohibit
www.nonono.com

**Create Schedule:** What's this?

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.



**Create Schedule:** What's this?

☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

**Times:**

○ Rule will be Active at the Scheduled Time

● Rule will be Inactive at the Scheduled Time

**Start Time:**

1 : 00 ● AM / ○ PM

**End Time:**

1 : 00 ● AM / ○ PM

**Create Rule Name:** What's this?

Create your rule name and description

**Rule Name:** Default

**Description:** description

Step 3. Click the Apply button to save and apply your settings.

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.

## Rule Summary

You can view the rules created for your Gateway.

- 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 view, edit, or delete the rule.

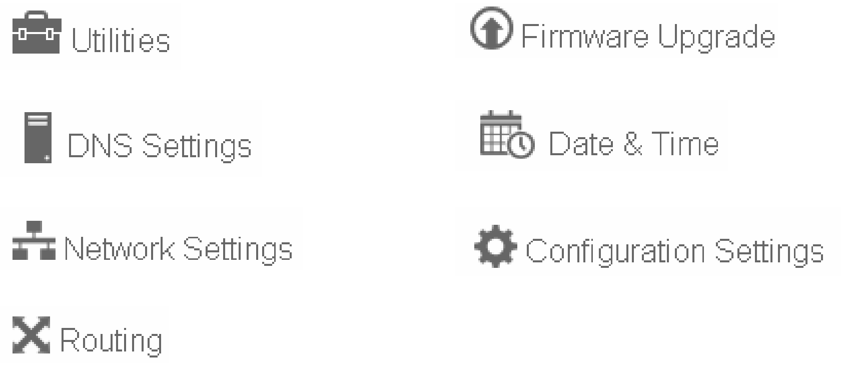
# Chapter 8 Configuring Advanced Settings

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

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

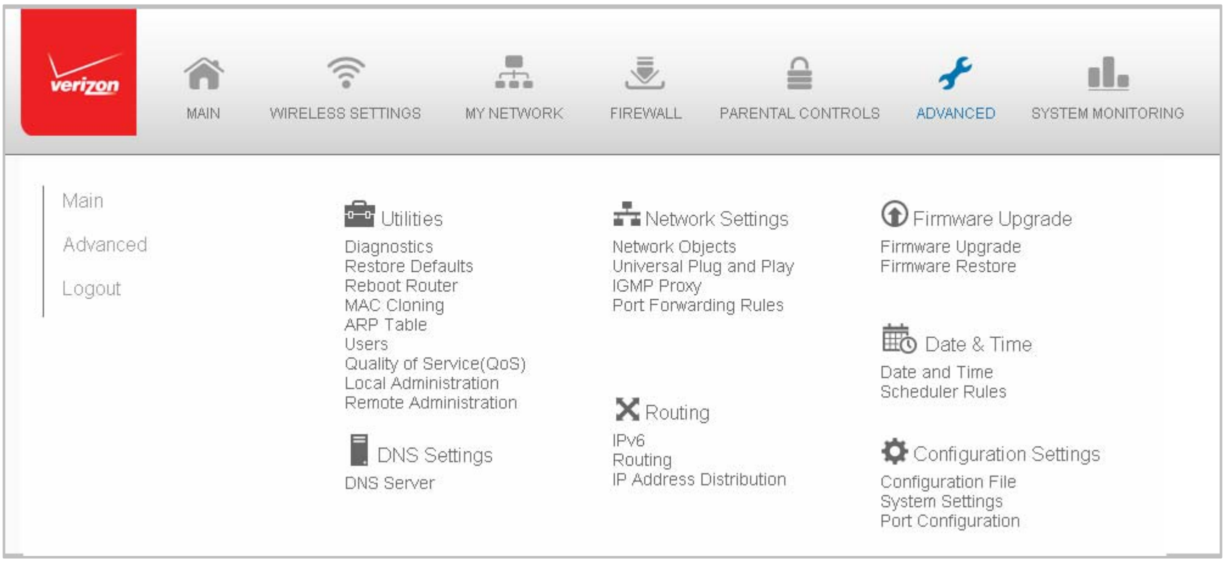
## Using Advanced Settings

You can access the following settings:



➢ To access the advanced settings:

1. Select **Advanced**. A warning page displays, asking if you want to proceed.
2. Click **Yes**. The Advanced page displays.



Utilities
Diagnostics
Restore Defaults
Reboot Router
MAC Cloning
ARP Table
Users
Quality of Service(QoS)
Local Administration
Remote Administration

DNS Settings
DNS Server

Network Settings
Network Objects
Universal Plug and Play
IGMP Proxy
Port Forwarding Rules

Routing
IPv6
Routing
IP Address Distribution

Firmware Upgrade
Firmware Upgrade
Firmware Restore

Date & Time
Date and Time
Scheduler Rules

Configuration Settings
Configuration File
System Settings
Port Configuration

3. Select a topic by clicking the topic name.

## Utilities

You can access the following advanced settings:

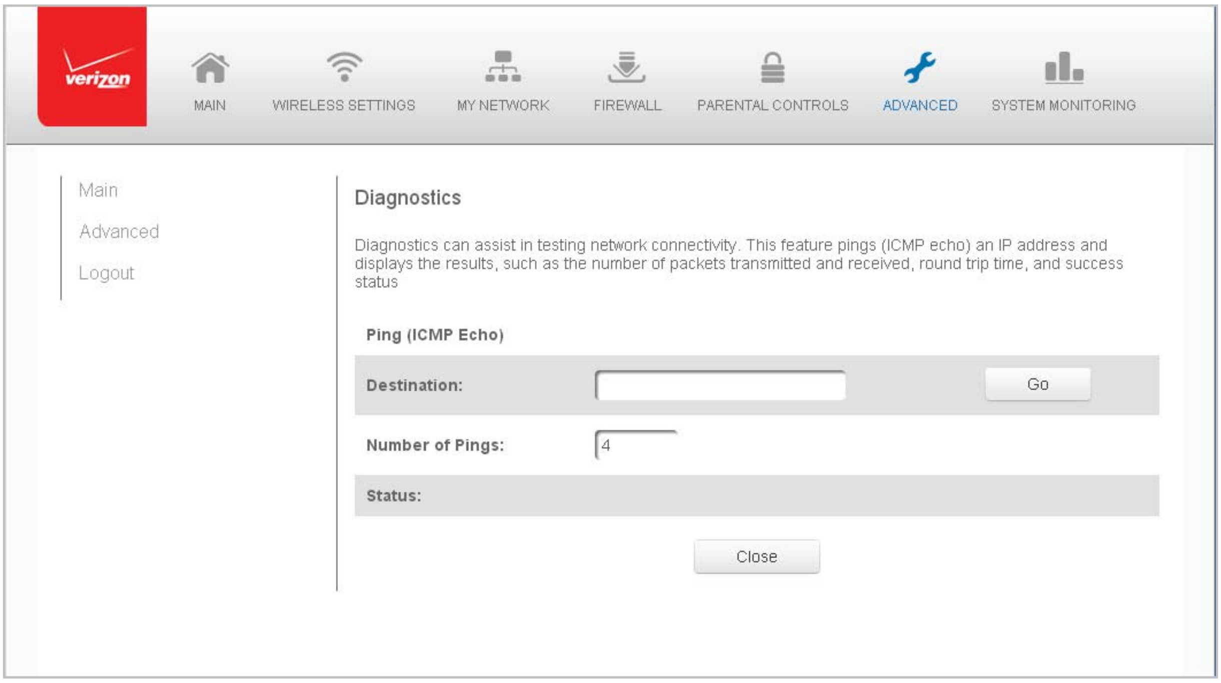
- **Diagnostics** – performs diagnostic tests
- **Restore Defaults** – resets your Gateway to it default settings
- **Reboot Router** – restarts your Gateway
- **MAC Cloning** – clones the MAC address
- **ARP Table** – displays active devices with their IP and MAC addresses
- **Users** – creates and manages remote users
- **Quality of Service (QoS)** – contact Technical Support for detailed information
- **Local Administration** – allows you to grant local SSH access
- **Remove Administration** – detailed in **Chapter 6 Configuring Your Network Settings**

## Diagnostics

You can use diagnostics to test network connectivity.

➢ To diagnose network connectivity:

1. Select **Diagnostics** in the Advanced page.



Diagnostics

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

Ping (ICMP Echo)

Destination: Go

Number of Pings: 4

Status:

Close

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.

## Restore Defaults

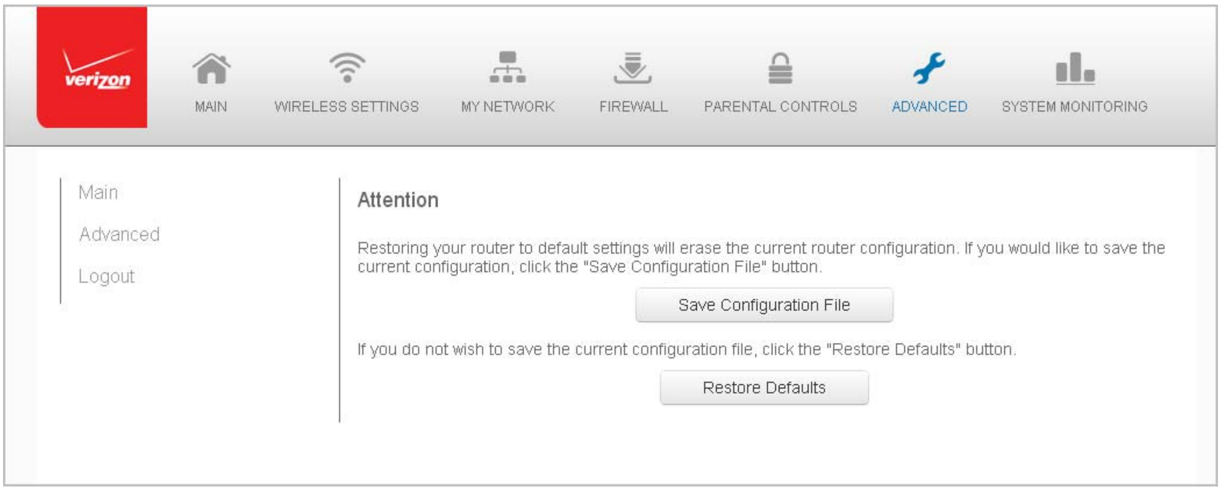
You can restore your configuration settings to your Gateway factory default settings. Restoring the default settings erases the current configuration, including user defined settings and network connections. All connected DHCP client must request new IP addresses. Your Gateway must restart.

Prior to restoring the factory defaults, you may want to save your current configuration to a file. This allows you to reapply your current settings and parameters to the default settings, as needed. For additional information, refer to the **Configuration File** section.

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

➢ To restore your Gateway's factory default settings:

1. Select **Restore Defaults** in the Advanced page.



Attention

Restoring your router to default settings will erase the current router configuration. If you would like to save the current configuration, click the "Save Configuration File" button.

If you do not wish to save the current configuration file, click the "Restore Defaults" button.

2. To save your current configuration file, click **Save Configuration File**.
3. To restore the factory default settings, click **OK**.

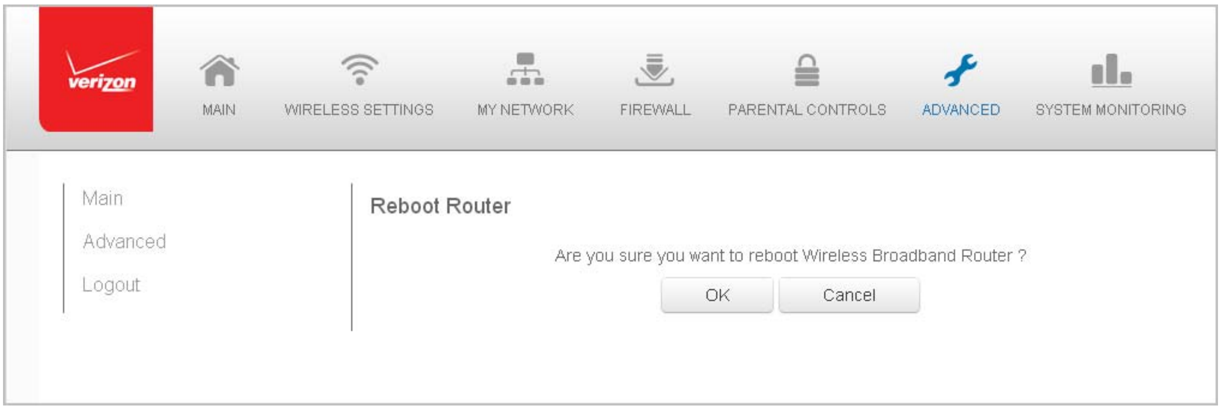
   The factory default settings are applied and your Gateway restarts. Once complete, the Login page for the First Time Easy Setup Wizard displays.

## Reboot Gateway

You can reboot your Gateway using the Reboot Router feature as well as pressing and holding the WPS button on the front of the Gateway for at least 10 seconds.

➢ To reboot your Gateway:

1. Select **Reboot Router** in the Advanced page.



Reboot Router

Are you sure you want to reboot Wireless Broadband Router ?

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

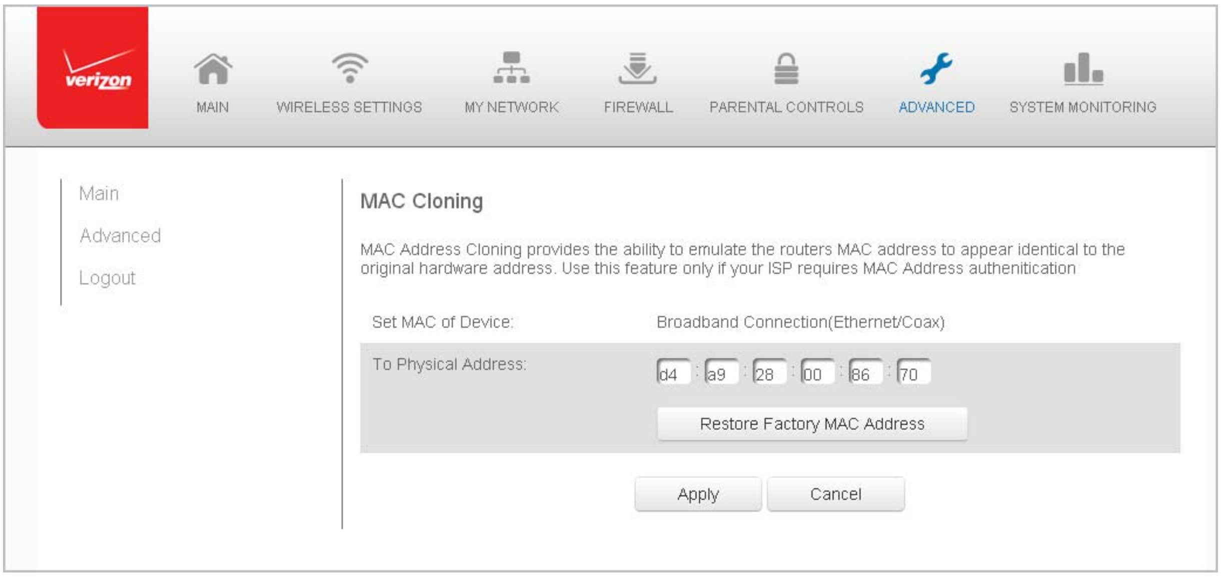
## MAC Cloning

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 Gateway, you can simplify the installation process by copying the MAC address of the existing device to your Gateway.

➢ To copy the MAC address of the existing device:

1. Select **MAC Cloning** in the Advanced page.



MAC Cloning

MAC Address Cloning provides the ability to emulate the routers MAC address to appear identical to the original hardware address. Use this feature only if your ISP requires MAC Address authenitication

Set MAC of Device: Broadband Connection(Ethernet/Coax)

To Physical Address: d4 : a9 : 28 : 00 : 86 : 70

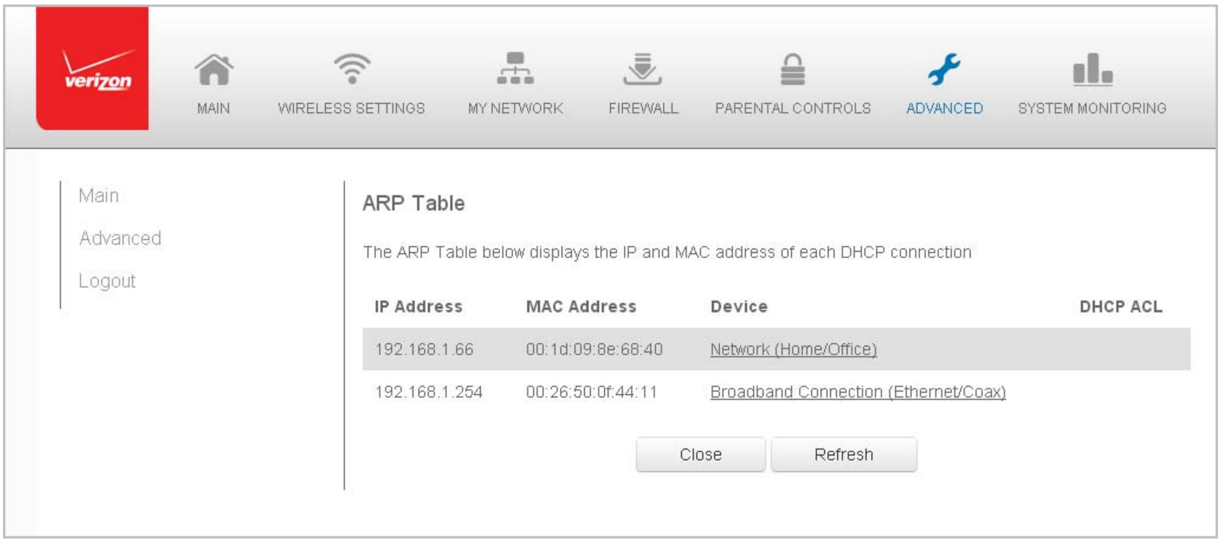
2. In the **To Physical Address** field, enter the MAC address of your new device.
3. To locate the MAC address, refer to the documentation from the device manufacturer.
4. Click **Apply** to save changes.

## ARP Table

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

➢ To view the addresses:

1. Select **ARP Table** in the Advanced page.



ARP Table

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

| IP Address | MAC Address | Device | DHCP ACL |
|---|---|---|---|
| 192.168.1.66 | 00:1d:09:8e:68:40 | Network (Home/Office) | |
| 192.168.1.254 | 00:26:50:0f:44:11 | Broadband Connection (Ethernet/Coax) | |

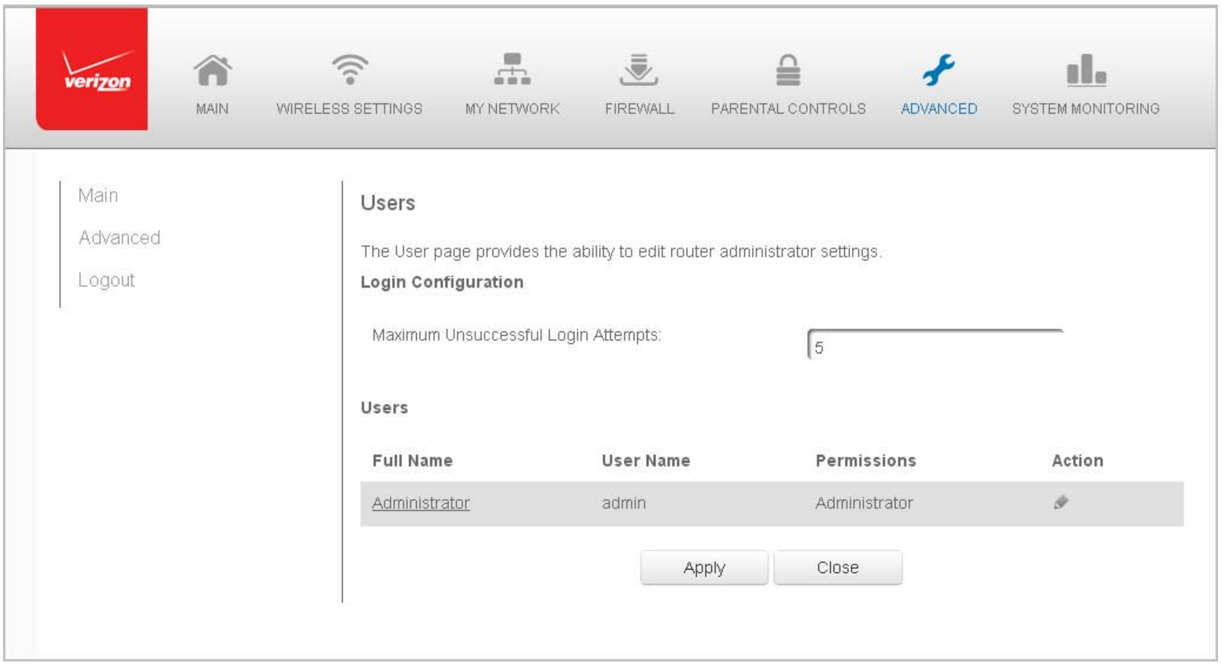
2. Review the IP and MAC address for each device.
3. When complete, click **Close**.

## Users

You can view the users that can currently access your wireless 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 Gateway temporarily denies all further login attempts by that user.

➢ To view users:

1. Select **Users** in the Advanced page.



Users

The User page provides the ability to edit router administrator settings.

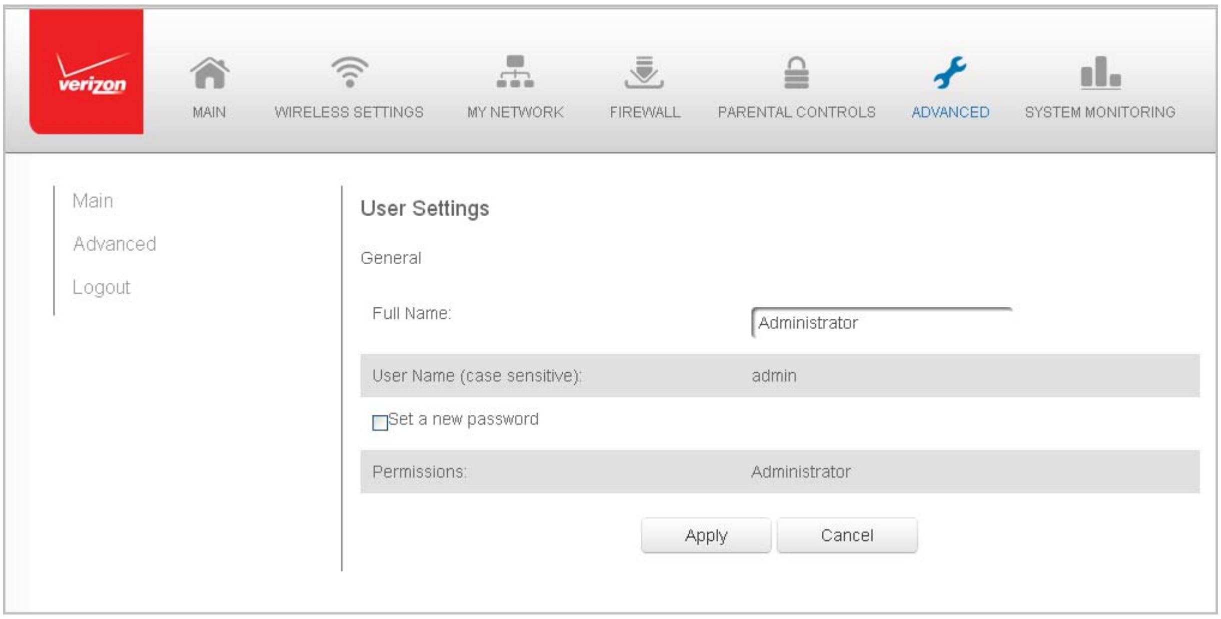
Login Configuration

Maximum Unsuccessful Login Attempts: 5

Users

| Full Name | User Name | Permissions | Action |
|---|---|---|---|
| Administrator | admin | Administrator | ✎ |

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



User Settings

General

| | |
|---|---|
| Full Name: | Administrator |
| User Name (case sensitive): | admin |

□ Set a new password

| | |
|---|---|
| Permissions: | Administrator |

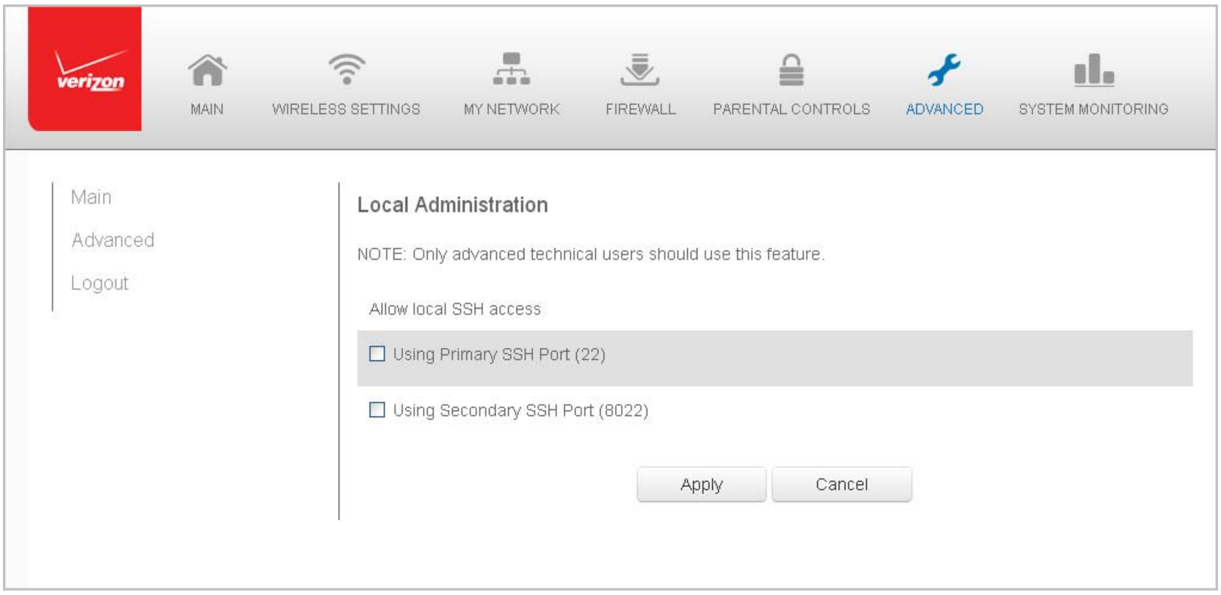
4. To edit the username and set a new password, as needed.
5. To add a new user, specify the following parameters:
   - **Full Name** – name of the user.
   - **User Name** – name the user enters to remotely access the home or office network. This field is case-sensitive.
6. To set a new Password, select 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.

## Local Administration

You can grant local access on a specific port.

➢ To grant access:

1. Select **Local Administration** in the Advanced page.



Local Administration

NOTE: Only advanced technical users should use this feature.

Allow local SSH access

□ Using Primary SSH Port (22)

□ Using Secondary SSH Port (8022)

2. To grant access, select the check box for the specific SSH access.
3. Click **Apply** to save changes. Local access is granted.
4. To remove access, clear the checkbox, then click **Apply**. No local access is granted.

### Remote Administration

The Remote Administration parameters are detailed in **Chapter 4 Configuring Your Network Settings.**

## DNS Settings

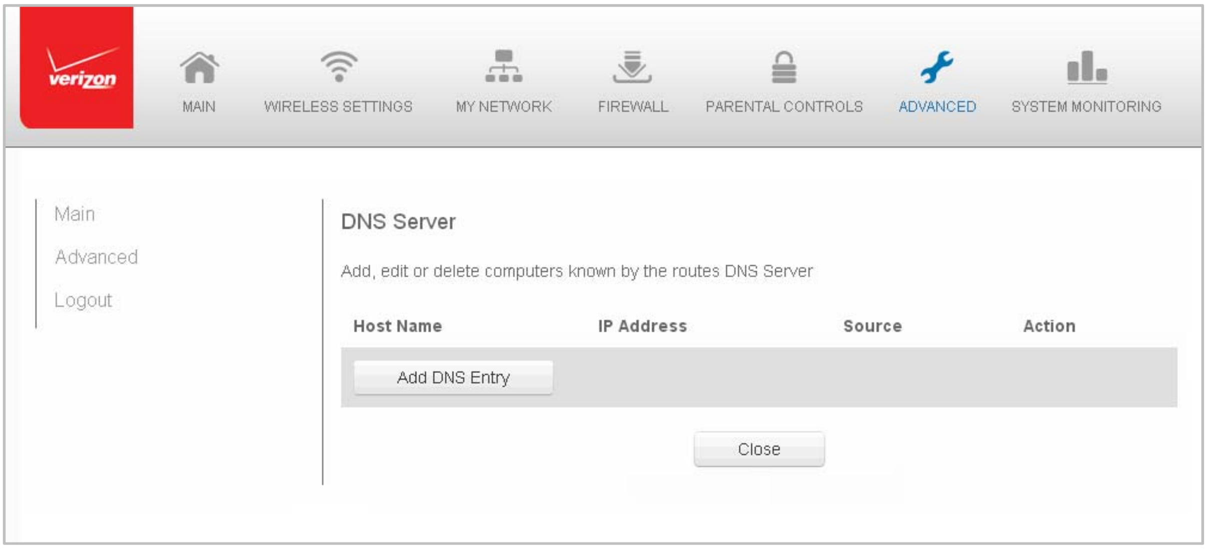
You can view and manage the DNS server host name and IP address as well as add a new computer. The DNS server does not require configuration.

### 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 Advanced page.



DNS Server

Add, edit or delete computers known by the routes DNS Server

| Host Name | IP Address | Source | Action |
|---|---|---|---|

2. To view and add computers stored in the DNS table, click **Add DNS Entry**. The Add DNS Entry page displays.
3. In the **Host Name** field, enter the name of the computer, then enter the IP address and click **Apply** to save changes. The DNS Server page displays.
4. 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.
5. To remove a host from the DNS table, click the **Delete** icon in the **Action** column.

## Network Settings

You can configure the following network settings:

- **Network Objects** – define a group, such as a group of computers
- **UPnP** – checks the validity of all UPnP services and rules
- **IGMP Proxy** – enables IGMP proxy
- **Port Forwarding Rules** – displays port forwarding rules

### Network Objects

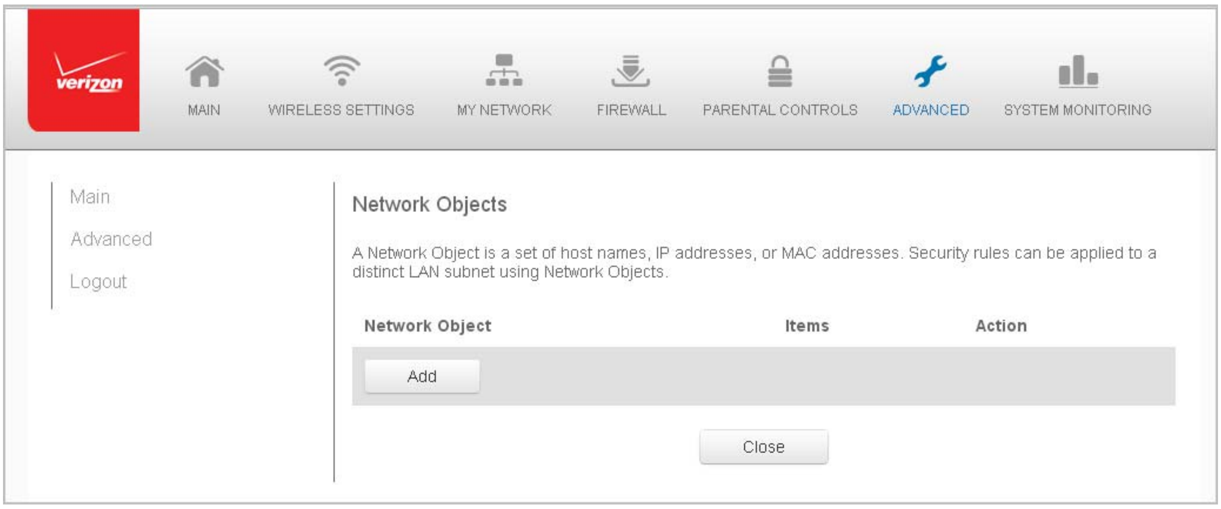
Network objects define a group, such as a group of computers, on your Gateway network by MAC address, IP address, and /or host name. The defined group becomes a network object. You can apply settings, such as configuring system rules, to all devices defined in the network object.

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

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

➢ To define a network object:

1. Select **Network Objects** in the Advanced page.

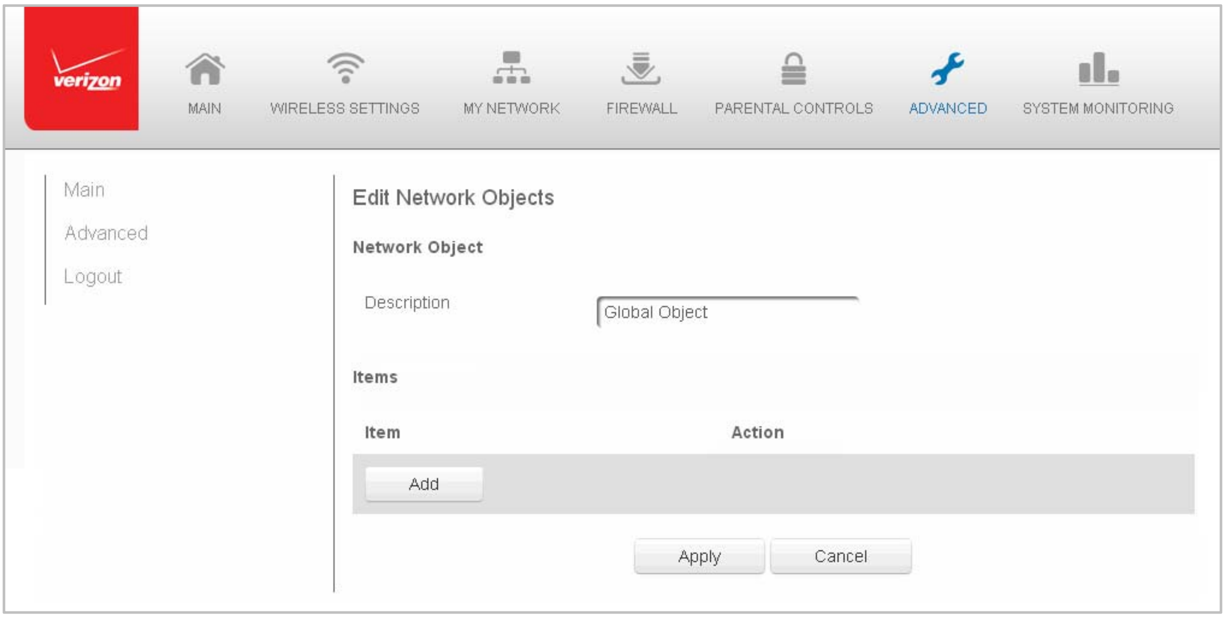


Network Objects

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

| Network Object | Items | Action |
|---|---|---|
| Add | | |

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



Edit Network Objects

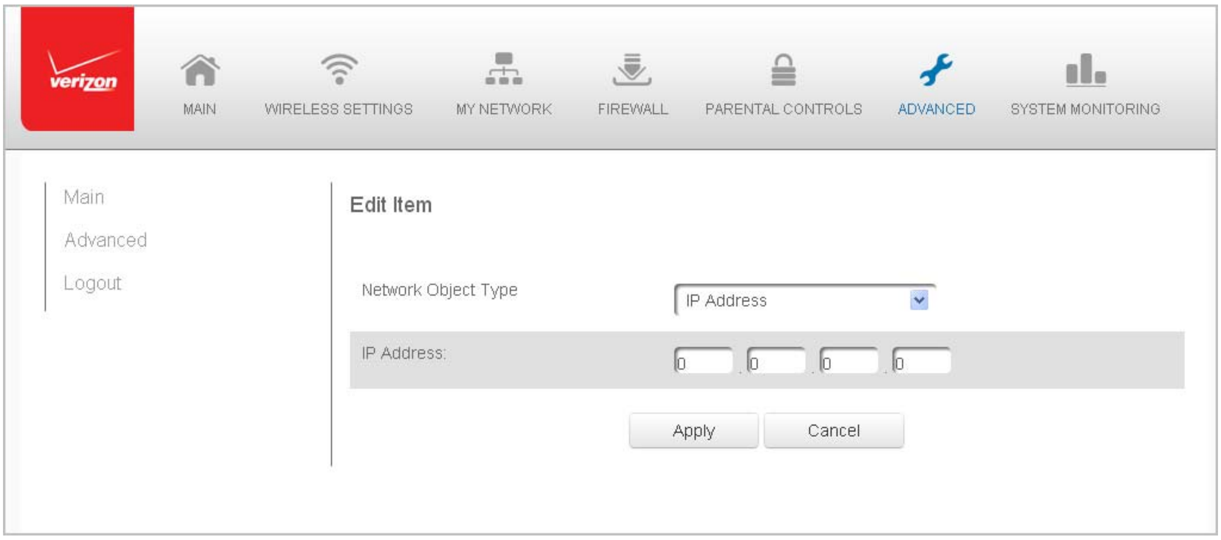
Network Object

Description: Global Object

Items

| Item | Action |
|---|---|
| Add | |

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



Edit Item

Network Object Type: IP Address

IP Address: 0 . 0 . 0 . 0

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

## Universal Plug and Play

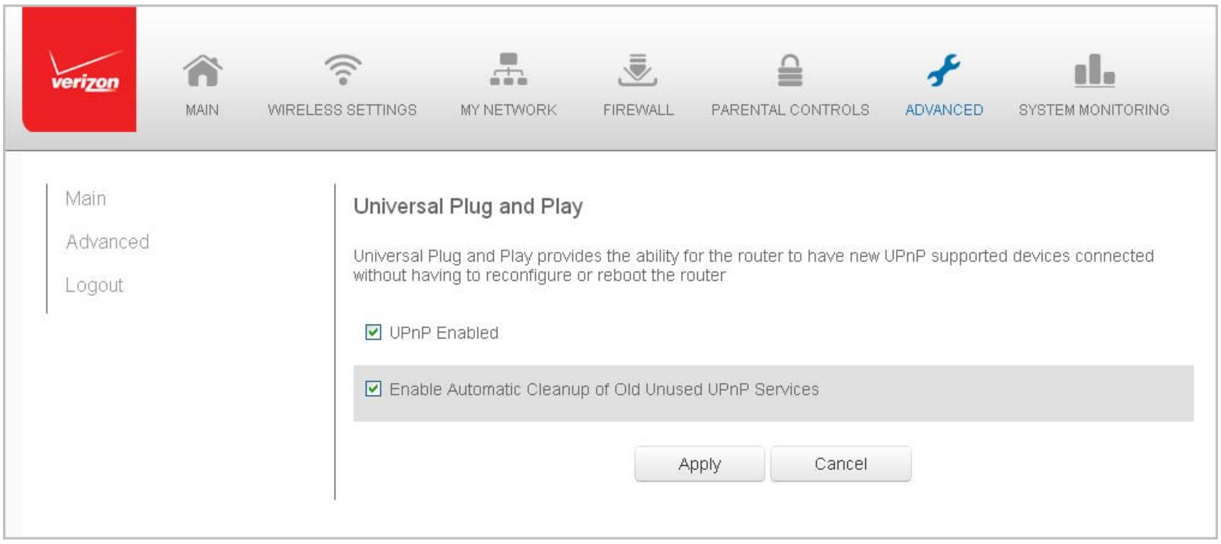
You can use Universal Plug and Play (UPnP) to support new devices without configuring or rebooting your Gateway.

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, and no new services can be define. The cleanup feature locates the invalid services and removes them, preventing services exhaustion.

➢ To access this setting:

1. Select **Universal Plug and Play** in the Advanced page.



Universal Plug and Play

Universal Plug and Play provides the ability for the router to have new UPnP supported devices connected without having to reconfigure or reboot the router

☑ UPnP Enabled

☑ Enable Automatic Cleanup of Old Unused UPnP Services

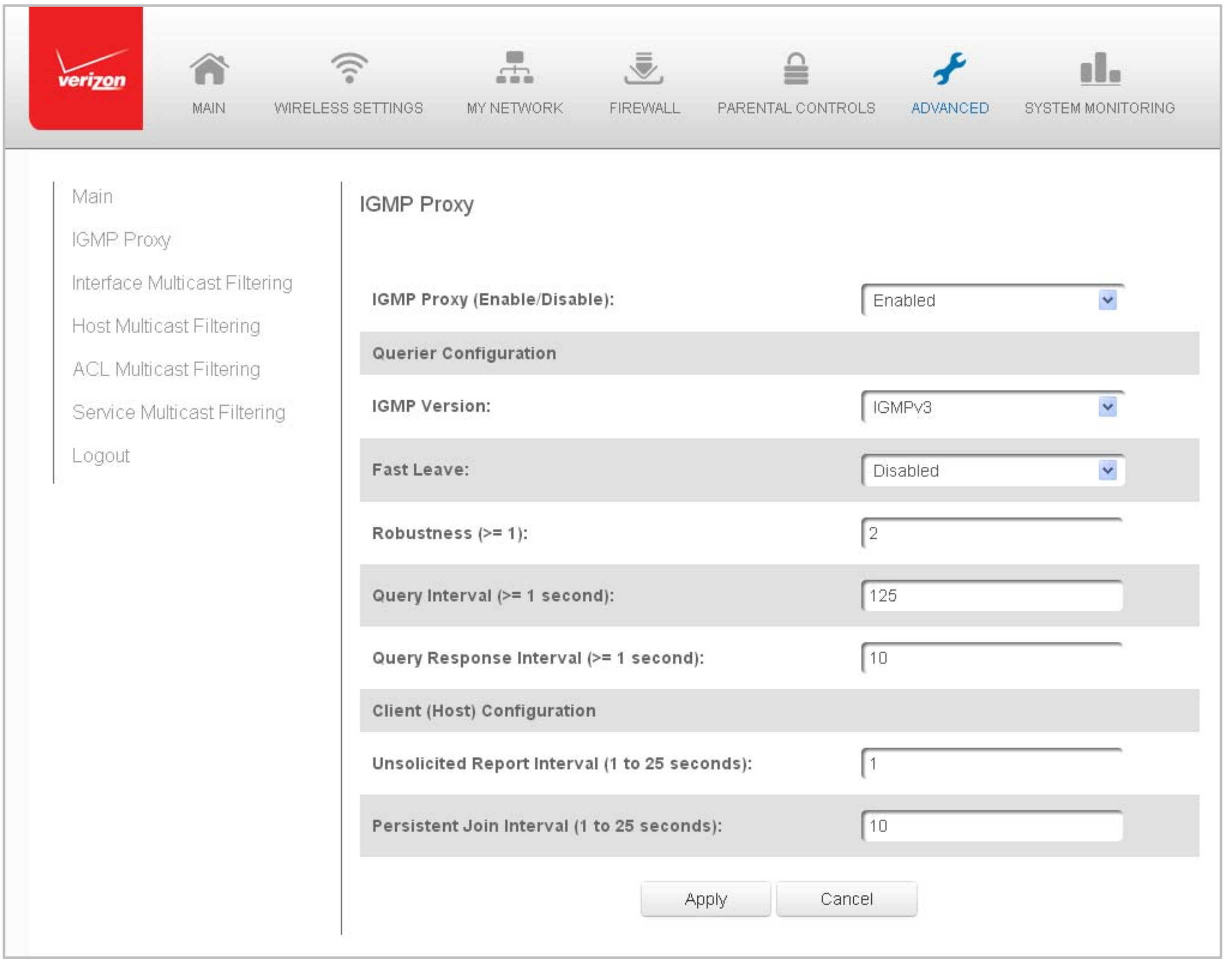
2. To enable UPnP and allow UPnP services to be defined on any network hosts, select the **UPnP Enabled** check box.
3. To enable automatic cleanup of invalid rules, select **Enable Automatic Cleanup of Old Unused UPnP Services** check box.
4. Click **Apply** to save changes.

## IGMP Proxy

You can configure IGMP proxy settings, as needed.

➢ To define the settings:

1. Select **ICMP Proxy** in the Advanced page.



IGMP Proxy

| | |
|---|---|
| IGMP Proxy (Enable/Disable): | Enabled |
| Querier Configuration | |
| IGMP Version: | IGMPv3 |
| Fast Leave: | Disabled |
| Robustness (>= 1): | 2 |
| Query Interval (>= 1 second): | 125 |
| Query Response Interval (>= 1 second): | 10 |
| Client (Host) Configuration | |
| Unsolicited Report Interval (1 to 25 seconds): | 1 |
| Persistent Join Interval (1 to 25 seconds): | 10 |

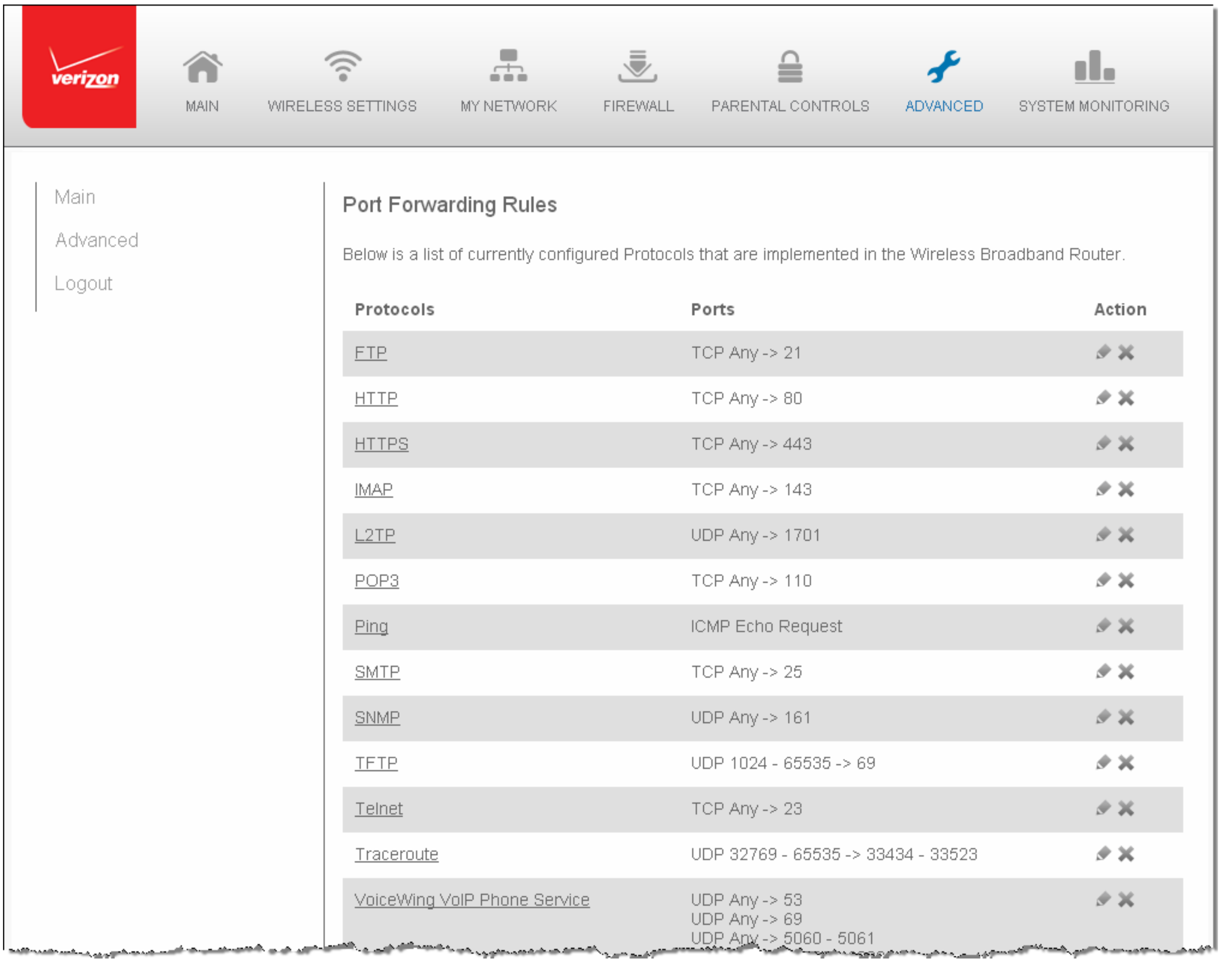
2. In the **IGMP Proxy** field, verify IGMP Proxy is enabled.
3. In the **Querier Configuration** section, define the following fields, as needed:
   - **IGMP Version** - select the IGMP Proxy version as IGMP, IGMPv2, or IGMPv3.
   - **Fast Leave** - activate or deactivate Fast.
   - **Robustness** - select the level of robustness by entering a number greater than or equal to 1.
   - **Query Interval** - set the query interval in seconds. The interval must be greater than or equal to 1.
   - **Query Response Interval** - set the query response interval in seconds. The interval must be greater than or equal to 1.
4. In the **Client (Host) Configuration** section, define the following fields, as needed:
   - **Unsolicited Report Interval** - set the unsolicited report in seconds. The interval must be between 1 and 25.
   - **Persistent Join Interval** - set the persistent join interval in seconds. The interval must be between 1 and 25.
5. Click **Apply** to save changes.

## Port Forwarding Rules

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

➢ To access the rules:

1. Select **Port Forwarding Rules** in the Advanced page.

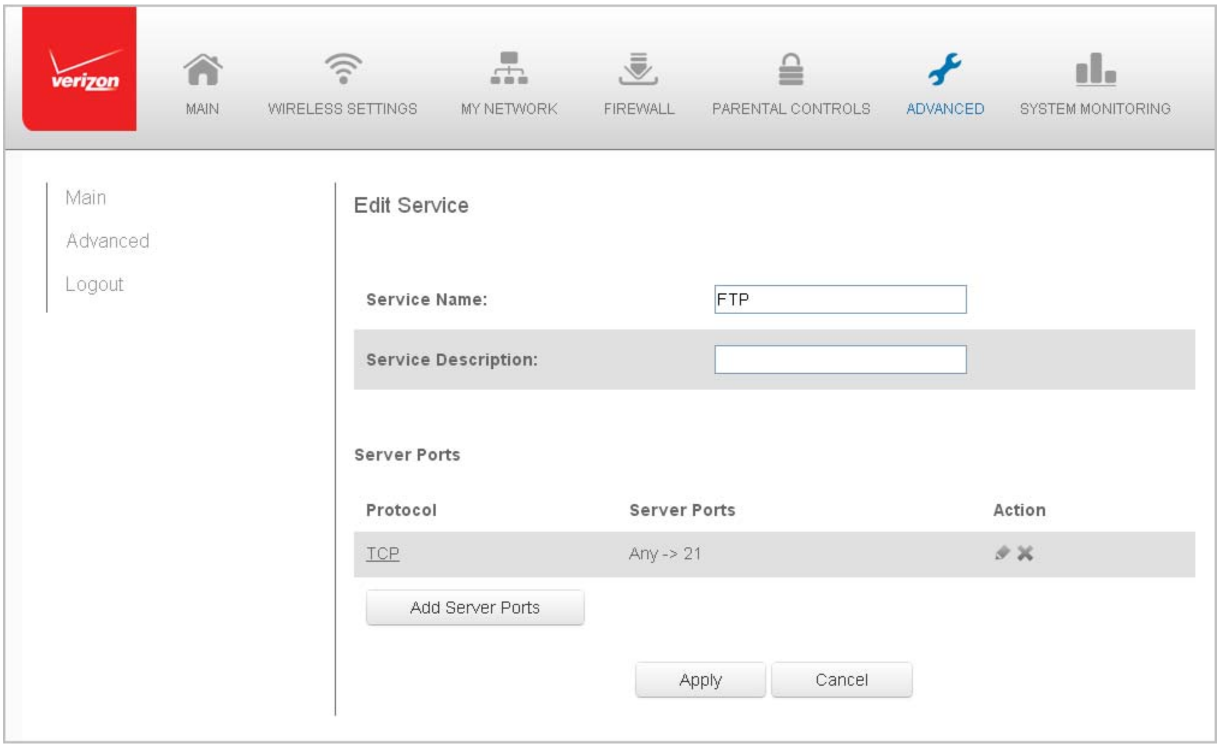


Port Forwarding Rules

Below is a list of currently configured Protocols that are implemented in the Wireless Broadband Router.

| Protocols | Ports | Action |
|---|---|---|
| FTP | TCP Any -> 21 | ✎ ✖ |
| HTTP | TCP Any -> 80 | ✎ ✖ |
| HTTPS | TCP Any -> 443 | ✎ ✖ |
| IMAP | TCP Any -> 143 | ✎ ✖ |
| L2TP | UDP Any -> 1701 | ✎ ✖ |
| POP3 | TCP Any -> 110 | ✎ ✖ |
| Ping | ICMP Echo Request | ✎ ✖ |
| SMTP | TCP Any -> 25 | ✎ ✖ |
| SNMP | UDP Any -> 161 | ✎ ✖ |
| TFTP | UDP 1024 - 65535 -> 69 | ✎ ✖ |
| Telnet | TCP Any -> 23 | ✎ ✖ |
| Traceroute | UDP 32769 - 65535 -> 33434 - 33523 | ✎ ✖ |
| VoiceWing VoIP Phone Service | UDP Any -> 53<br>UDP Any -> 69<br>UDP Any -> 5060 - 5061 | ✎ ✖ |

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



Edit Service

|  |  |
|---|---|
| Service Name: | FTP |
| Service Description: |  |

Server Ports

| Protocol | Server Ports | Action |
|---|---|---|
| TCP | Any -> 21 | ✎ ✖ |

3. Modify the **Service Name** and **Service Description**, as needed.
4. To modify the current protocol, click the **Edit** icon in the Action column.
5. To add server ports, click **Add Server Ports**.
6. Click **Apply** to save changes.

## Routing

You can configure the following settings:

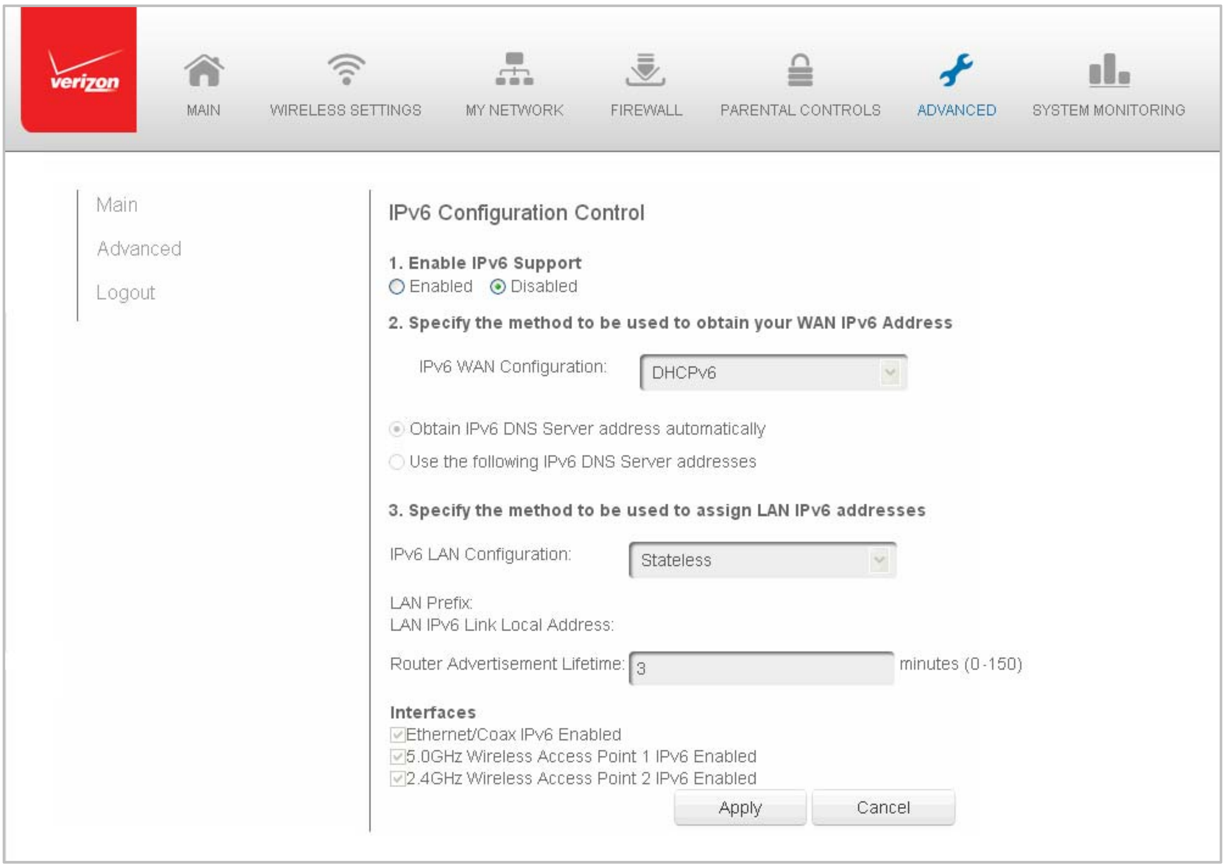
- **IPv6** – enables IPv6 support.
- **Routing** – manages the routing and IP address distribution rules.
- **IP Address Distribution** - adds computers configured as DHCP clients to the network

### IPv6 Configuration Control

You can configure IPv6 on your wireless network.

➢ To configure IPv6:

1. Select **IPv6** from the Advanced page.



IPv6 Configuration Control

**1. Enable IPv6 Support**

○ Enabled ● Disabled

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

IPv6 WAN Configuration: DHCPv6

● Obtain IPv6 DNS Server address automatically

○ Use the following IPv6 DNS Server addresses

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

IPv6 LAN Configuration: Stateless

LAN Prefix:
LAN IPv6 Link Local Address:

Router Advertisement Lifetime: 3 minutes (0-150)

**Interfaces**

☑ Ethernet/Coax IPv6 Enabled
☑ 5.0GHz Wireless Access Point 1 IPv6 Enabled
☑ 2.4GHz Wireless Access Point 2 IPv6 Enabled

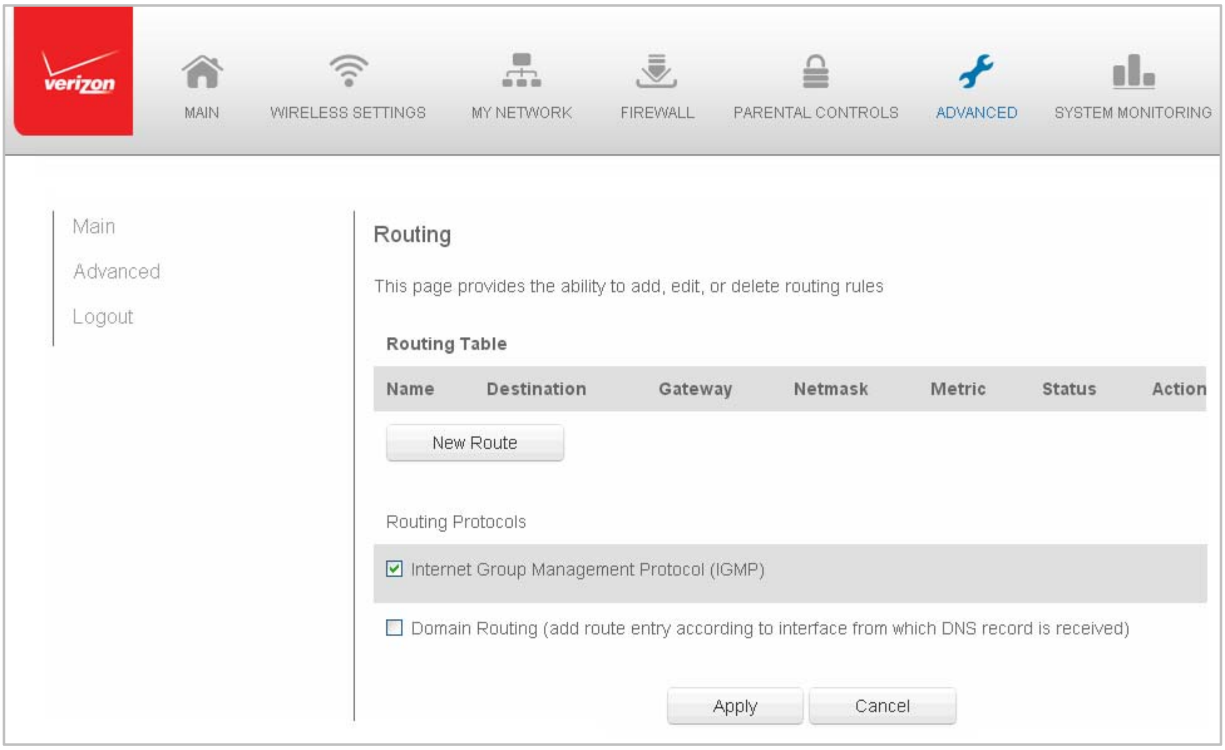
2. Enable IPv6 support.
3. Obtain IPv6 DNS Server address automatically or specify the server address.
4. Specify method for assigning LAN IPv6 addresses.
5. In the **Interfaces** section, select the enabled interfaces.
6. Click **Apply** to save changes.

## Routing Settings

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

➢ To view the rules:

1. Select **Routing** in the Advanced page.



Routing

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

Routing Table

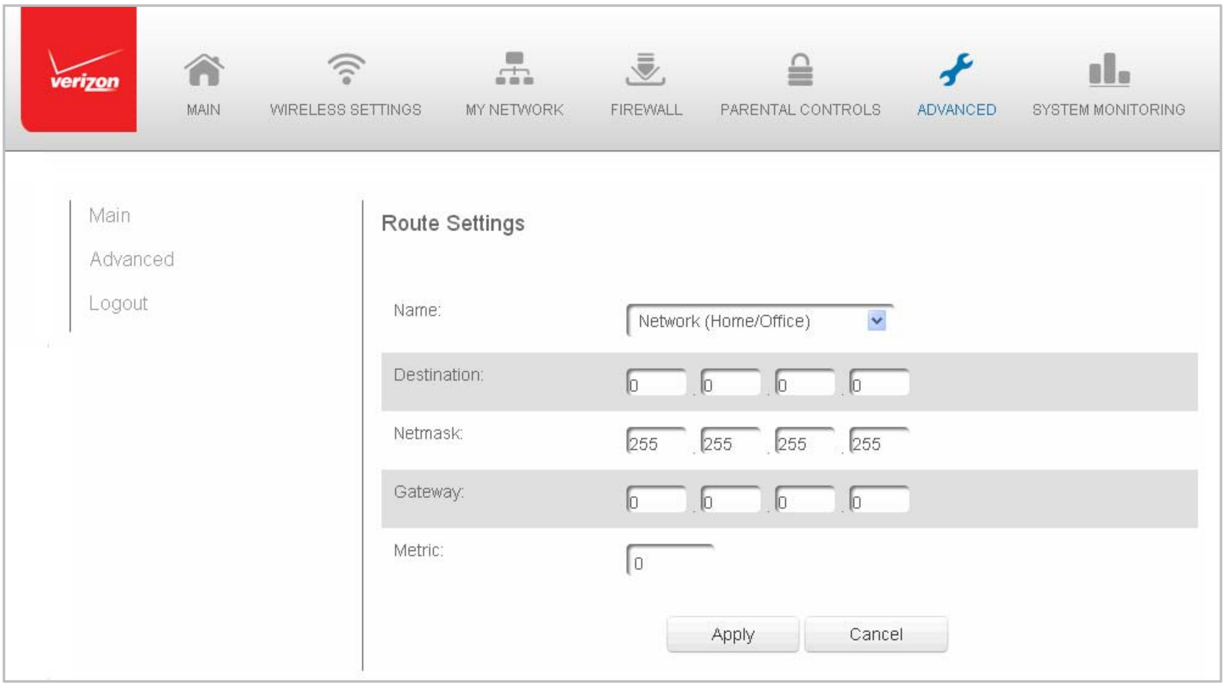
| Name | Destination | Gateway | Netmask | Metric | Status | Action |
|---|---|---|---|---|---|---|

Routing Protocols

☑ Internet Group Management Protocol (IGMP)

☐ Domain Routing (add route entry according to interface from which DNS record is received)

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



Route Settings

| | |
|---|---|
| Name: | Network (Home/Office) |
| Destination: | 0 . 0 . 0 . 0 |
| Netmask: | 255 . 255 . 255 . 255 |
| Gateway: | 0 . 0 . 0 . 0 |
| Metric: | 0 |

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

## IP 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.

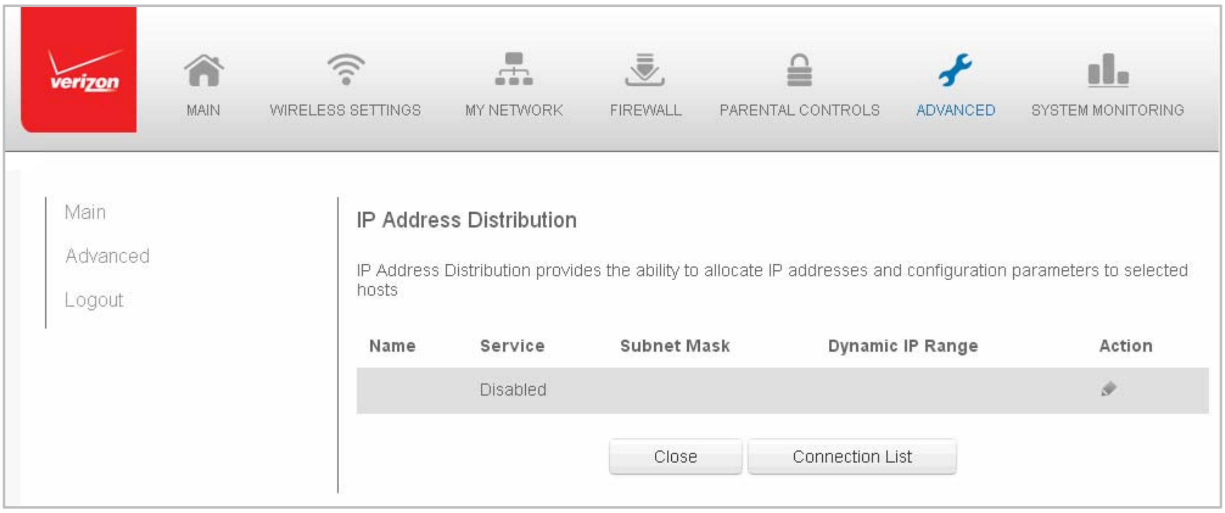
If the host wishes to terminate a lease before its expiration, it sends a release message to the DHCP server. This makes the IP address available for use by other hosts.

The DHCP server performs the following functions:

- Displays a list of all DHCP host devices connected to your Gateway
- Defines the range of IP addresses that can be allocated in the network
- Defines the length of time the dynamic P 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 **IP Address Distribution** in the Advanced page.



IP Address Distribution

IP Address Distribution provides the ability to allocate IP addresses and configuration parameters to selected hosts

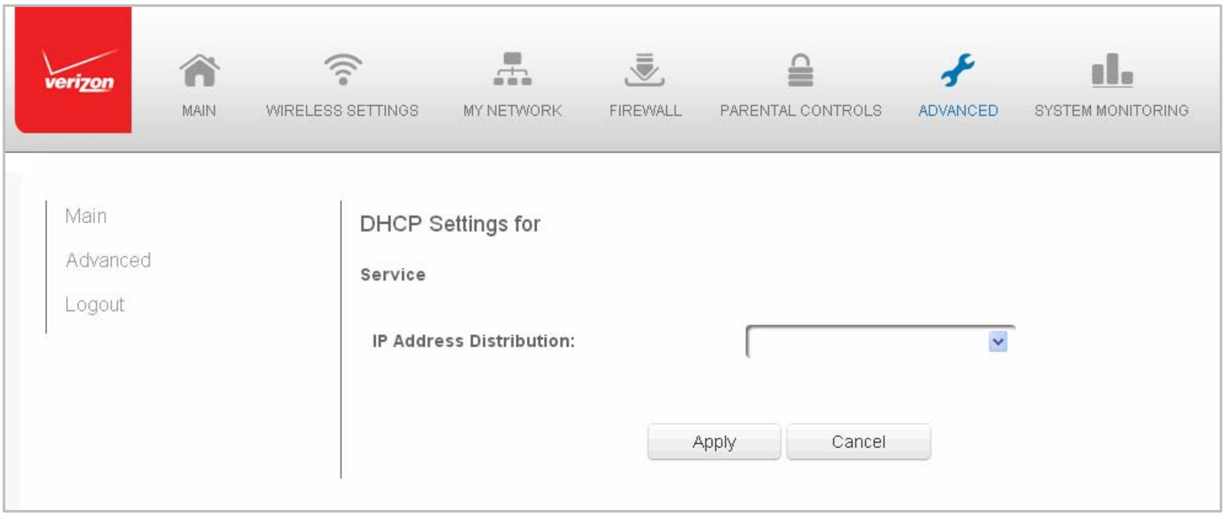
| Name | Service | Subnet Mask | Dynamic IP Range | Action |
|---|---|---|---|---|
| | Disabled | | | ✎ |

### DHCP Server Settings

You can edit the DHCP server settings for a device.

- ➢ To edit the settings:

  1. On the IP Address Distribution page, click the **Edit** icon in the **Action** column. The DHCP Settings page opens with the device information displayed.



DHCP Settings for

Service

IP Address Distribution:

2. To enable the DHCP server, select **DHCP Server** in the **IP Address Distribution** field.

   Once enabled, the DHCP server provides automatic IP assignments (IP leases) based on the preset IP range defined below.

3. To configure the DHCP server complete the following fields:

   - **Start IP Address** – enter the first IP address that your Gateway will automatically begin assigning IP addresses from. Since your Gateway's default IP address is 192.168.1.1, the default start IP address should be 192.162.1.2.
   - **End IP Address** – enter the last IP address that your Gateway will automatically stop 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.
   - **Provide Host Name if Not Specified by Client** – when activated, your Gateway assigns a default name to the client, if the DHCP client has no host name.

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

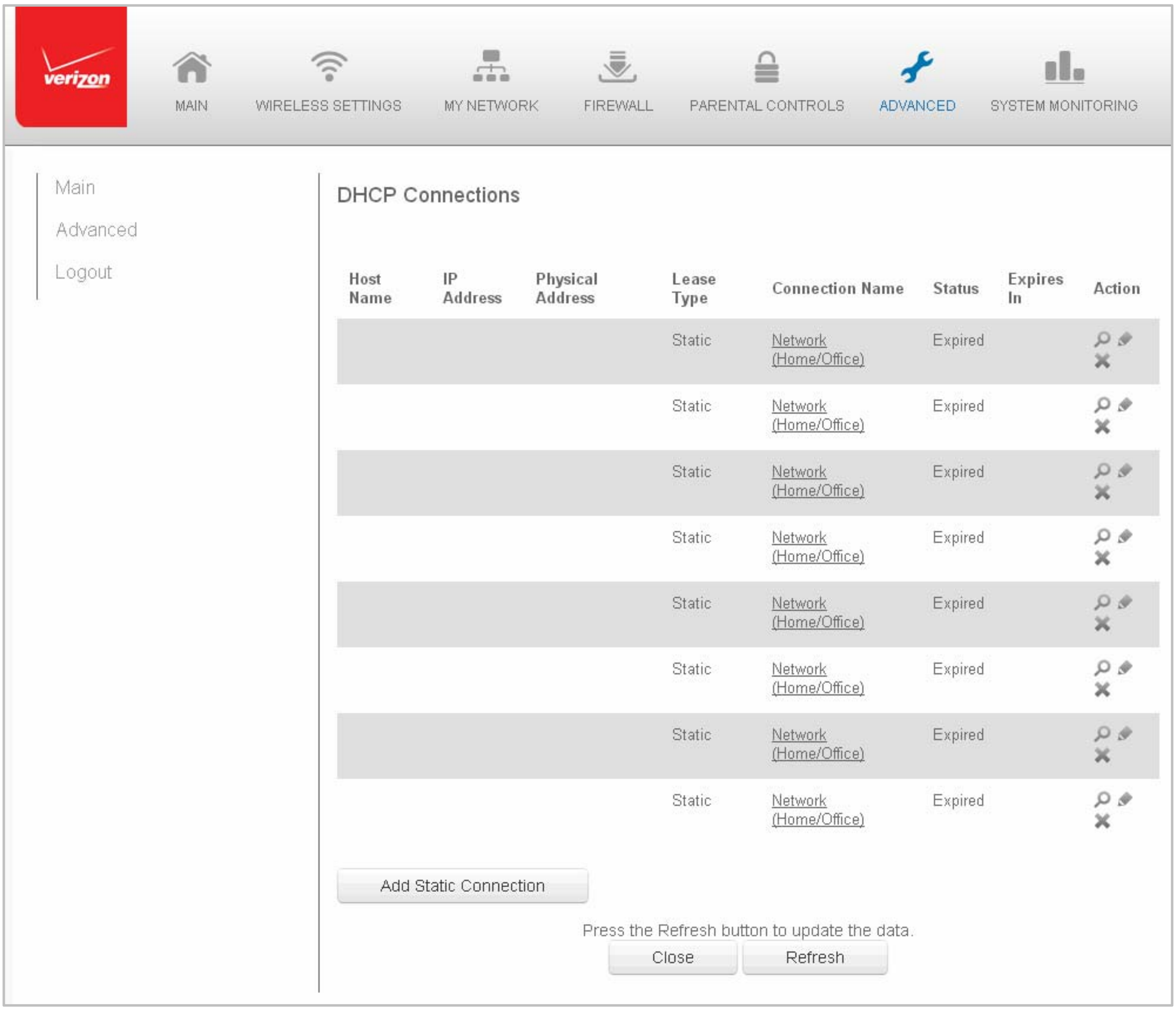
### DHCP Connections

You can view a list of the connections currently assigned and recognized by the DHCP server. In addition, you can add a new connection with a fixed IP address.

**Note:** The fixed IP address of a device is assigned to the MAC address of the network card installed on the network computer. If this network card is replaced, you must update the device entry in the DHCP Connections list with the MAC address of the new network card.

➢ To view a list of computers:

1. On the IP Address page, click **Connection List.**

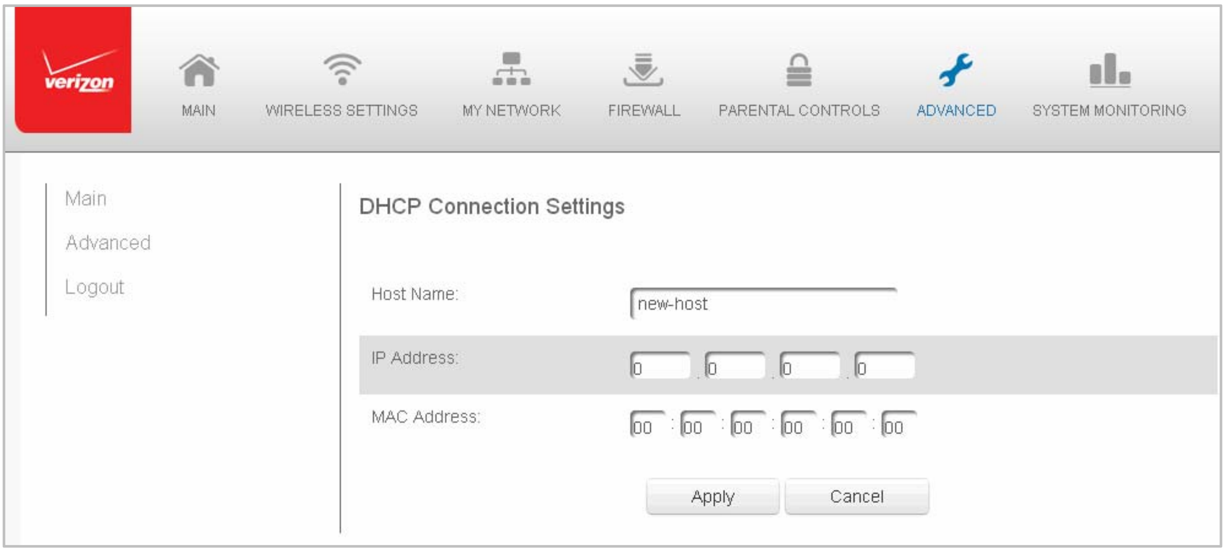


DHCP Connections

| Host Name | IP Address | Physical Address | Lease Type | Connection Name | Status | Expires In | Action |
|---|---|---|---|---|---|---|---|
| | | | Static | Network (Home/Office) | Expired | | |
| | | | Static | Network (Home/Office) | Expired | | |
| | | | Static | Network (Home/Office) | Expired | | |
| | | | Static | Network (Home/Office) | Expired | | |
| | | | Static | Network (Home/Office) | Expired | | |
| | | | Static | Network (Home/Office) | Expired | | |
| | | | Static | Network (Home/Office) | Expired | | |
| | | | Static | Network (Home/Office) | Expired | | |

Press the Refresh button to update the data.

2. To define a new Static Connection with a fixed IP address, click **Add Static Connection**.



DHCP Connection Settings

Host Name: new-host

IP Address: 0 . 0 . 0 . 0

MAC Address: 00 : 00 : 00 : 00 : 00 : 00

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.

## Firmware Upgrade

You can perform the following functions:

- **Firmware Upgrade** – upgrades using the Internet or a local computer.
- **Firmware Restore** – rollbacks your firmware to a previous version.

### Firmware Upgrade

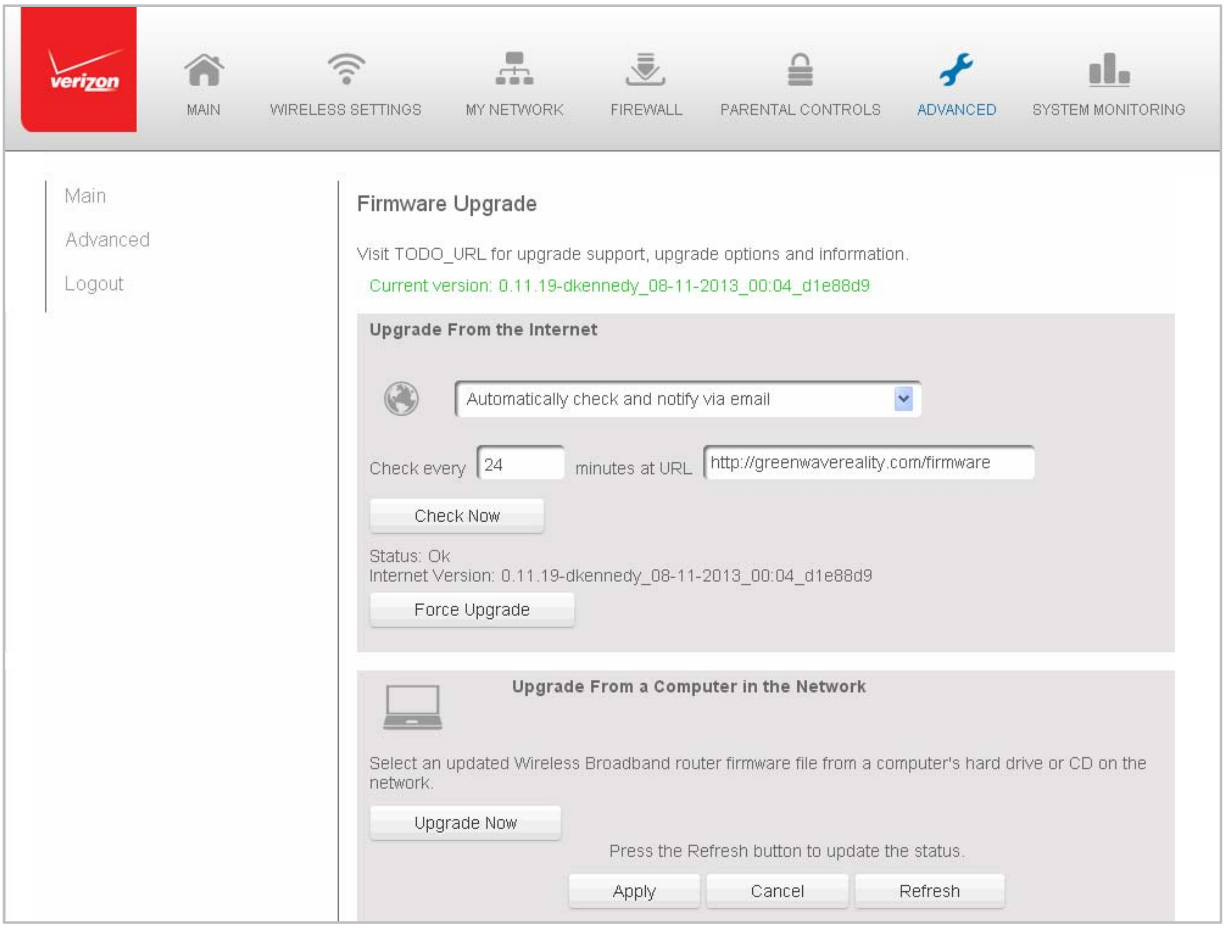
Your Gateway offers a built-in mechanism for upgrading or restoring its firmware without losing custom configuration and settings.

You can use either of the following methods:

- **Upgrading from the Internet** – upgrades your Gateway's firmware by remotely downloading an updated software image file.
- **Upgrading from a local computer** – use a software image file pre-downloaded to the computer's disk drive for upgrades

➢ To upgrade the firmware:

1. Select **Firmware Upgrade** in the Advanced page.



Firmware Upgrade

Visit TODO_URL for upgrade support, upgrade options and information.

Current version: 0.11.19-dkennedy_08-11-2013_00:04_d1e88d9

Upgrade From the Internet

Automatically check and notify via email

Check every 24 minutes at URL http://greenwavereality.com/firmware

Status: Ok
Internet Version: 0.11.19-dkennedy_08-11-2013_00:04_d1e88d9

Upgrade From a Computer in the Network

Select an updated Wireless Broadband router firmware file from a computer's hard drive or CD on the network.

Press the Refresh button to update the status.

2. Select either **Upgrade from the Internet** or **Upgrade from a Computer in the Network**.

## Automatically Upgrade from the Internet

➢ To automatically upgrade:

1. Select from the following options in the Firmware Upgrade page:
   - **Automatically Check for New Version and Upgrade Wireless Broadband Gateway** – enter the period of time and URL at which to receive the upgrade. Your Gateway checks each time interval for an upgrade and, if an upgrade is available, upgrades the firmware.
   - **Automatically Check for New Version and Notify via Email** – enter the period of time and URL at which to receive the upgrade. Your Gateway checks each time interval for an upgrade and, if an upgrade is available, sends an email to the email address listed in the System Settings.
   - **Automatically Check Disabled** – Your Gateway does not automatically check for firmware upgrades. You must manually upgrade the firmware.

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

### Manually Upgrade from the Internet

➢ To manually upgrade:

1. Click the **Check Now** button in the Firmware Upgrade page.
2. If a new version is available, click **Force Upgrade**. A download process begins.

   When completed, a confirmation page displays, asking whether to upgrade to the new version.
3. Click **Apply** to save changes. The upgrade process begins and should require no more than a minute to complete the process.

   When the upgrade process completes, your Gateway automatically reboots. The new firmware runs, maintaining any custom configurations and settings.

### Upgrade from Local Computer

Only use files with a rmt extension when performing the firmware upgrade procedure.

➢ To upgrade from a local computer:

1. To utilize the **Upgrade from a Computer in the Network** option, first obtain a valid firmware image (file) for your Gateway.
2. In the **Upgrade from a Computer in the Network** section of the Firmware Upgrade page, click **Browse** to locate the downloaded firmware file and click Open.
3. Click **Upgrade Now** to begin the update process. The Firmware Upgrade in process page displays.

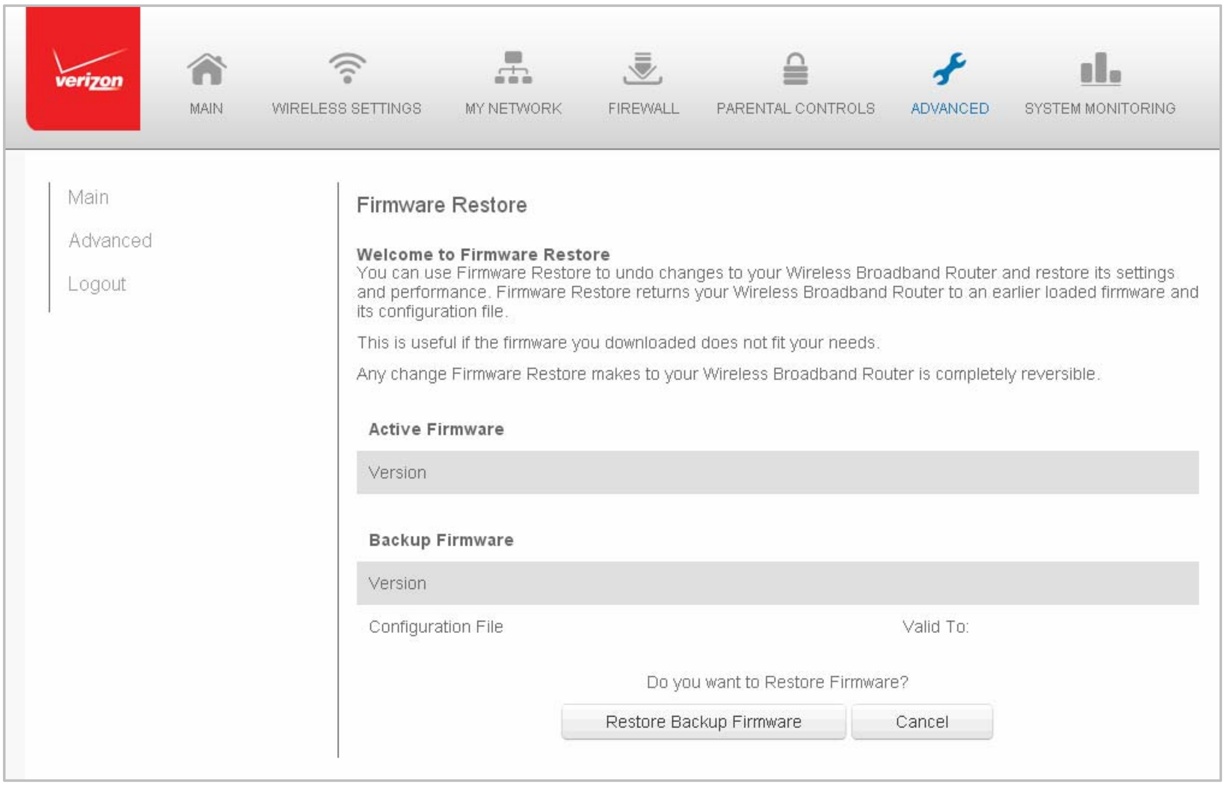
   When the upgrade process completes, your Gateway automatically reboots. The new firmware runs, maintaining any custom configuration and settings.

## Firmware Restore

Firmware Restore allows you to undo changes to your Gateway and restore previous settings. For example, you can use firmware restore if a firmware update does not fit your needs.

➢ To restore firmware to a previous version:

1. Select **Firmware Restore** in the Advanced page.



Firmware Restore

**Welcome to Firmware Restore**
You can use Firmware Restore to undo changes to your Wireless Broadband Router and restore its settings and performance. Firmware Restore returns your Wireless Broadband Router to an earlier loaded firmware and its configuration file.

This is useful if the firmware you downloaded does not fit your needs.

Any change Firmware Restore makes to your Wireless Broadband Router is completely reversible.

**Active Firmware**

Version

**Backup Firmware**

Version

Configuration File    Valid To:

Do you want to Restore Firmware?

2. Click **Restore Backup Firmware**.

## Date and Time

You can configure the following settings:

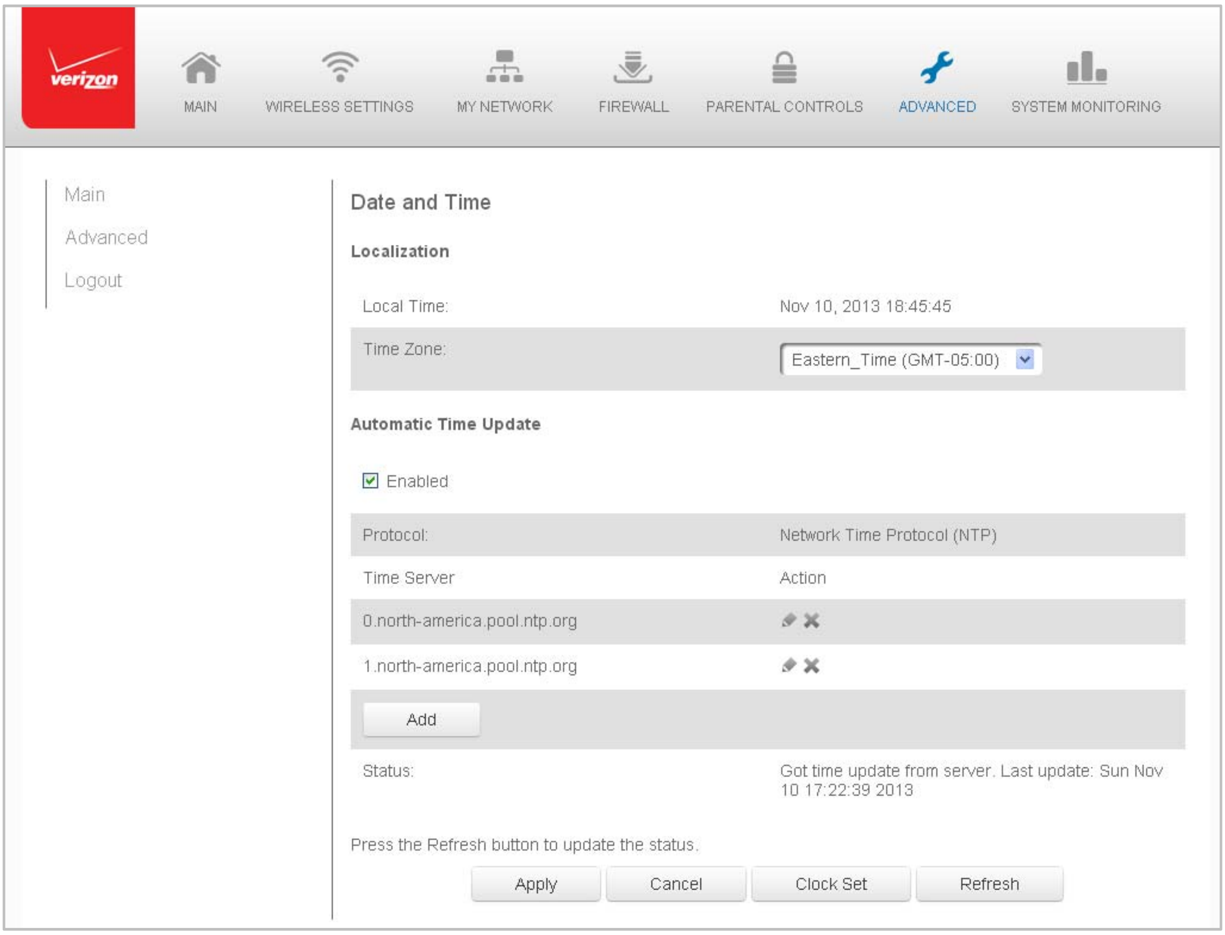
- **Date and Time Settings** – sets the time zone and enables automatic time updates.
- **Scheduler Rules** – limits the activation of firewall rules to specific time periods.

### 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 Advanced page.



Date and Time

Localization

| | |
|---|---|
| Local Time: | Nov 10, 2013 18:45:45 |
| Time Zone: | Eastern_Time (GMT-05:00) |

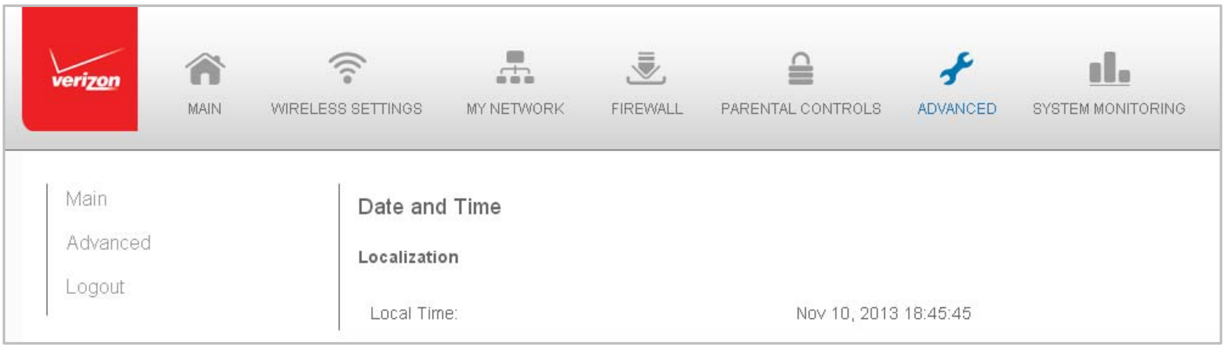
Automatic Time Update

☑ Enabled

| | |
|---|---|
| Protocol: | Network Time Protocol (NTP) |
| Time Server | Action |
| 0.north-america.pool.ntp.org | ✎ ✖ |
| 1.north-america.pool.ntp.org | ✎ ✖ |
| Add | |
| Status: | Got time update from server. Last update: Sun Nov 10 17:22:39 2013 |

Press the Refresh button to update the status.

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



Date and Time

Localization

Local Time: Nov 10, 2013 18:45:45

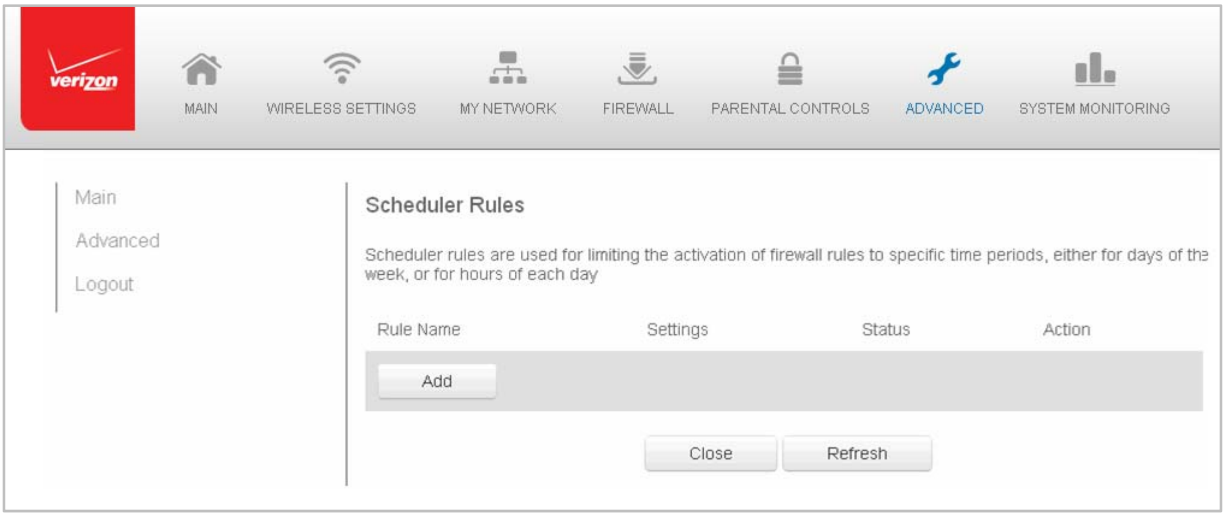
5. Enter the IP address or domain name of the time server, then click **Apply** to save changes.

## 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 Gateway is correct.
2. Select **Scheduler Rules** in the Advanced page.

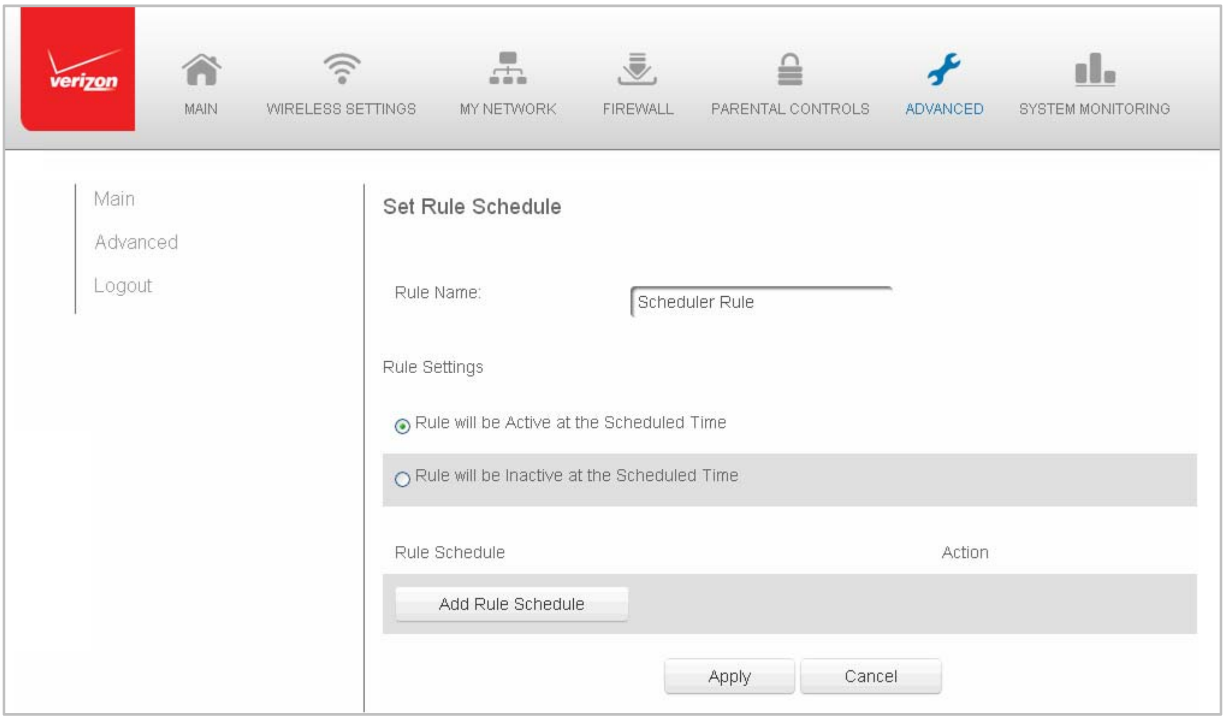


Scheduler Rules

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

| Rule Name | Settings | Status | Action |
|---|---|---|---|
| Add | | | |

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



Set Rule Schedule

Rule Name: Scheduler Rule

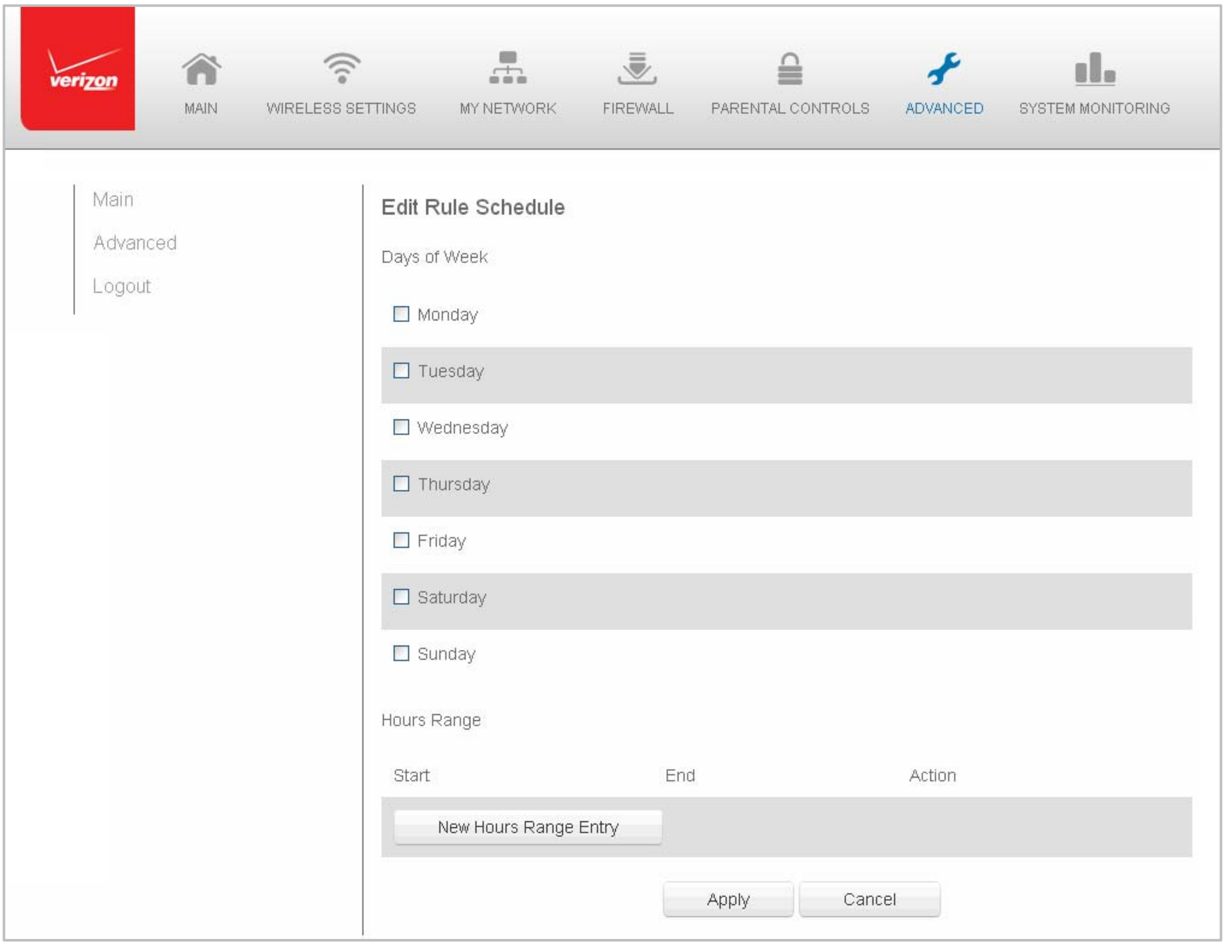
Rule Settings

● Rule will be Active at the Scheduled Time

○ Rule will be Inactive at the Scheduled Time

| Rule Schedule | Action |
|---|---|
| Add Rule Schedule | |

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.



Edit Rule Schedule

Days of Week

☐ Monday

☐ Tuesday

☐ Wednesday

☐ Thursday

☐ Friday

☐ Saturday

☐ Sunday

Hours Range

| Start | End | Action |
|---|---|---|
| New Hours Range Entry | | |

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.

## Configuration Settings

You can configure the following configuration settings:

- **Configuration File** – used for file backups and restoring configuration files
- **System Settings** – configures various system and management parameters
- **Port Configuration** – sets up Ethernet ports

### Configuration File

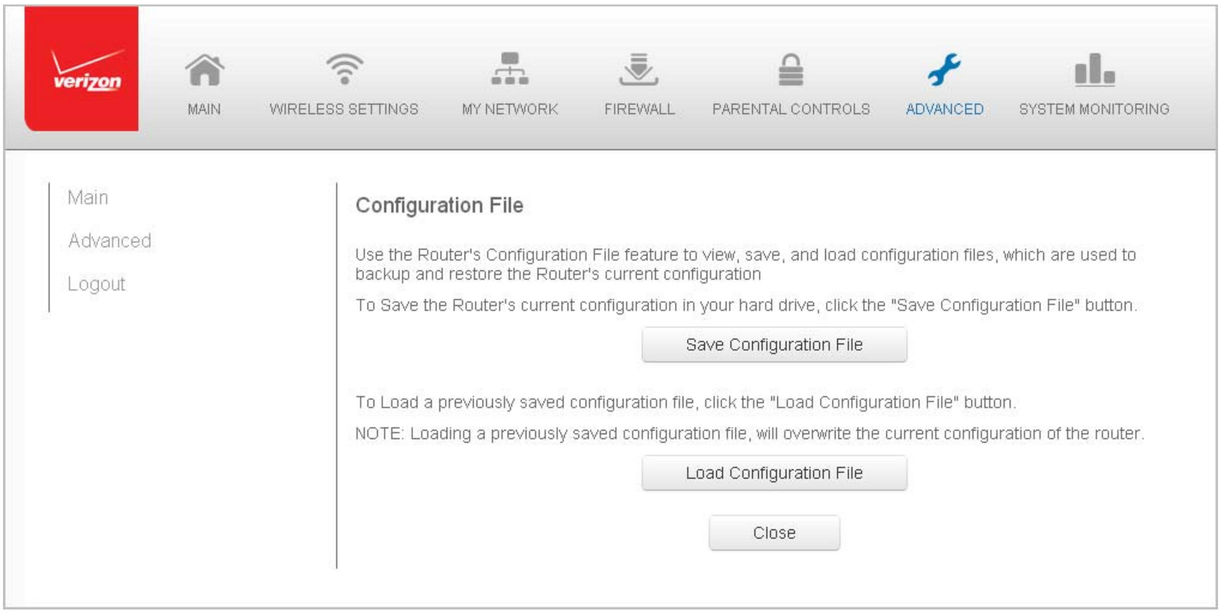
You can use the Configuration File functionality to view, save, and load configuration files. These files are used to backup and restore the current configuration of your Gateway.

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

**WARNING!** Manually editing a configuration file can cause your Gateway to malfunction or become completely inoperable.

➢ To save or load the configuration file:

1. Select **Configuration File**.



Configuration File

Use the Router's Configuration File feature to view, save, and load configuration files, which are used to backup and restore the Router's current configuration

To Save the Router's current configuration in your hard drive, click the "Save Configuration File" button.

To Load a previously saved configuration file, click the "Load Configuration File" button.

NOTE: Loading a previously saved configuration file, will overwrite the current configuration of the router.

2. To save the current configuration to a file, click **Save Configuration File**. The configuration file is saved to you web browser's download folder.
3. To load a previously saved configuration file, click **Load Configuration File**.

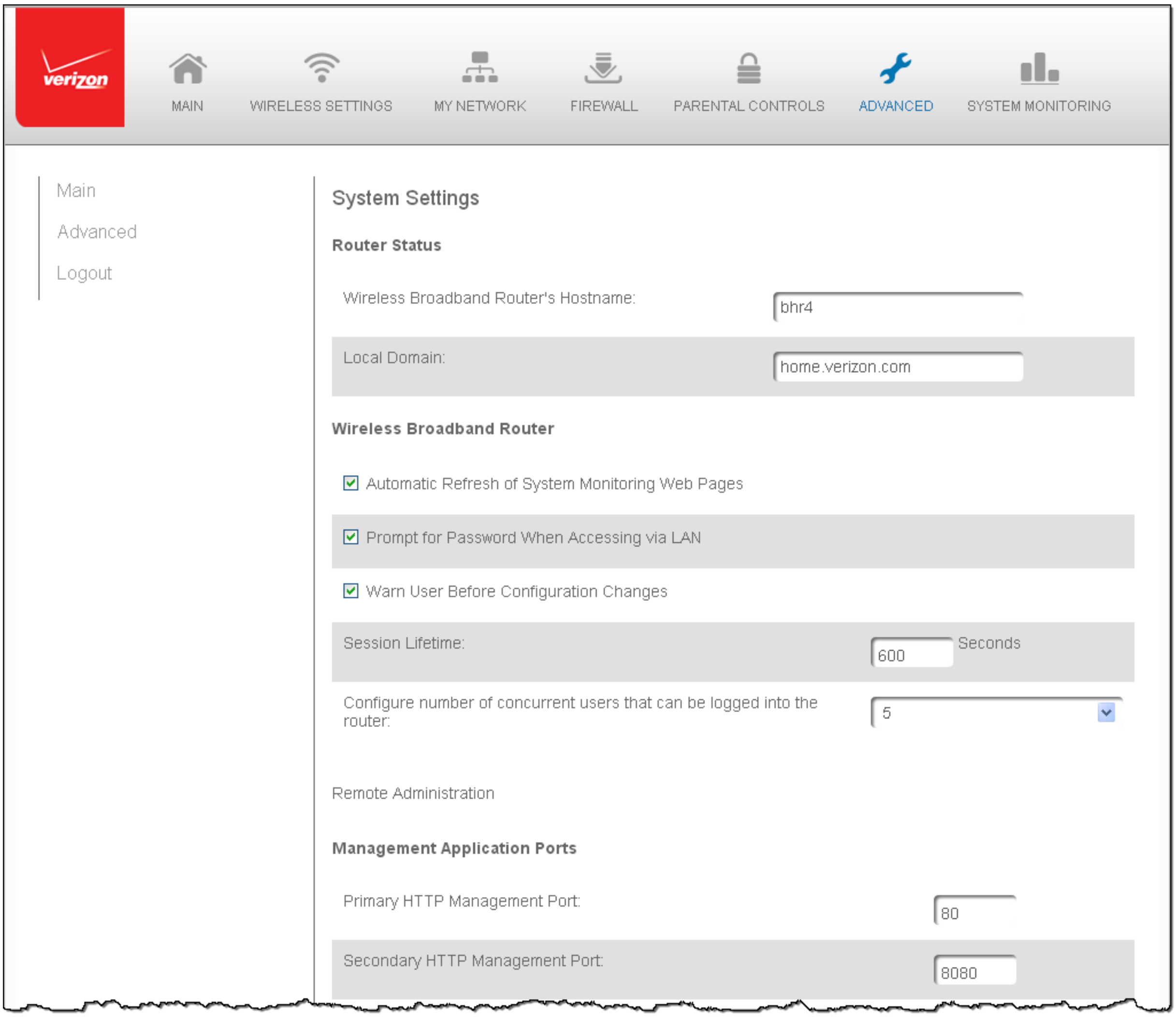
   Browse to the location of the file, then click **Apply** to begin the configuration uploading process. Your Gateway will automatically restart with that configuration.

## System Settings

You can configure various system and management parameters.

➢ To configure system settings:

1. Select **System Settings** in the Advanced page.



System Settings

**Router Status**

Wireless Broadband Router's Hostname: bhr4

Local Domain: home.verizon.com

**Wireless Broadband Router**

☑ Automatic Refresh of System Monitoring Web Pages

☑ Prompt for Password When Accessing via LAN

☑ Warn User Before Configuration Changes

Session Lifetime: 600 Seconds

Configure number of concurrent users that can be logged into the router: 5

Remote Administration

**Management Application Ports**

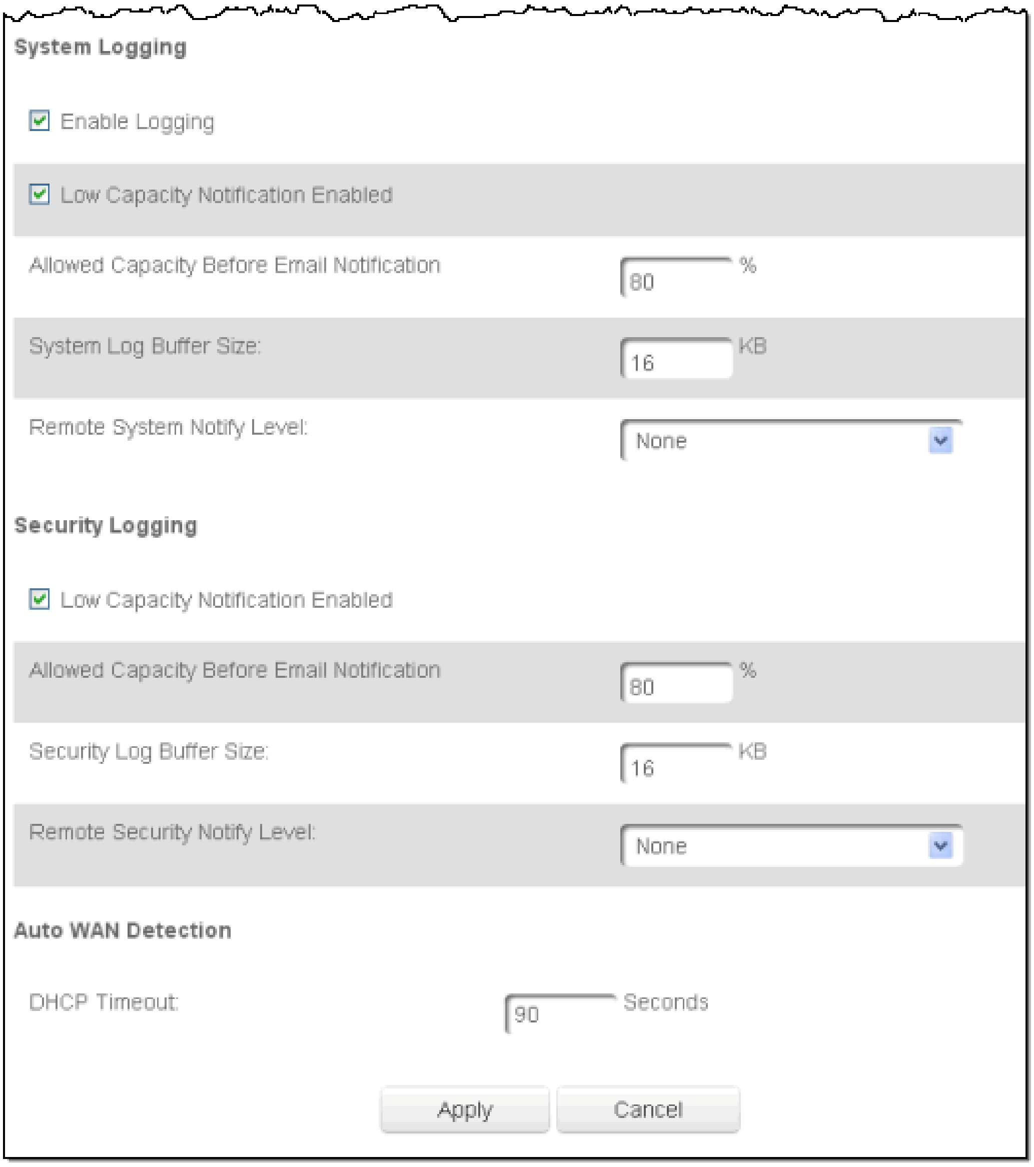
Primary HTTP Management Port: 80

Secondary HTTP Management Port: 8080

2. In the **Router Status** section, configure the following:
   - **Wireless Broadband Route's Hostname** – enter the host name or URL address of your Gateway. Both names are the same.
   - **Local Domain** – enter the local domain of the network.
3. In the **Wireless Broadband 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 Gateway to ask for a password when trying to connect to the network.
   - **Warn User Before Configuration Changes** – activates user warnings before network configuration changes take effect.

   In the **Session Lifetime** field, specify the length of time required before reentering a user name and password after your Gateway has been inactive.

   In the **Configure a Number of Concurrent Users** field, select the number of users that can access your Gateway at any time.
4. Select **Remote Administration** to configure the remote administration to your Gateway.
5. In the **Management Application Ports** section, change the primary and secondary HTTP management ports.
6. In the **System Logging** section, configure the following system log options:
   - **Enable Logging** – activates system logging.
   - **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.
   - **Remote System Notify Level** – specify the type of information, such as none, error, warning, and information, received for remote system logging.



System Logging

☑ Enable Logging

☑ Low Capacity Notification Enabled

|  |  |
|---|---|
| Allowed Capacity Before Email Notification | 80 % |
| System Log Buffer Size: | 16 KB |
| Remote System Notify Level: | None |

Security Logging

☑ Low Capacity Notification Enabled

|  |  |
|---|---|
| Allowed Capacity Before Email Notification | 80 % |
| Security Log Buffer Size: | 16 KB |
| Remote Security Notify Level: | None |

Auto WAN Detection

DHCP Timeout: 90 Seconds

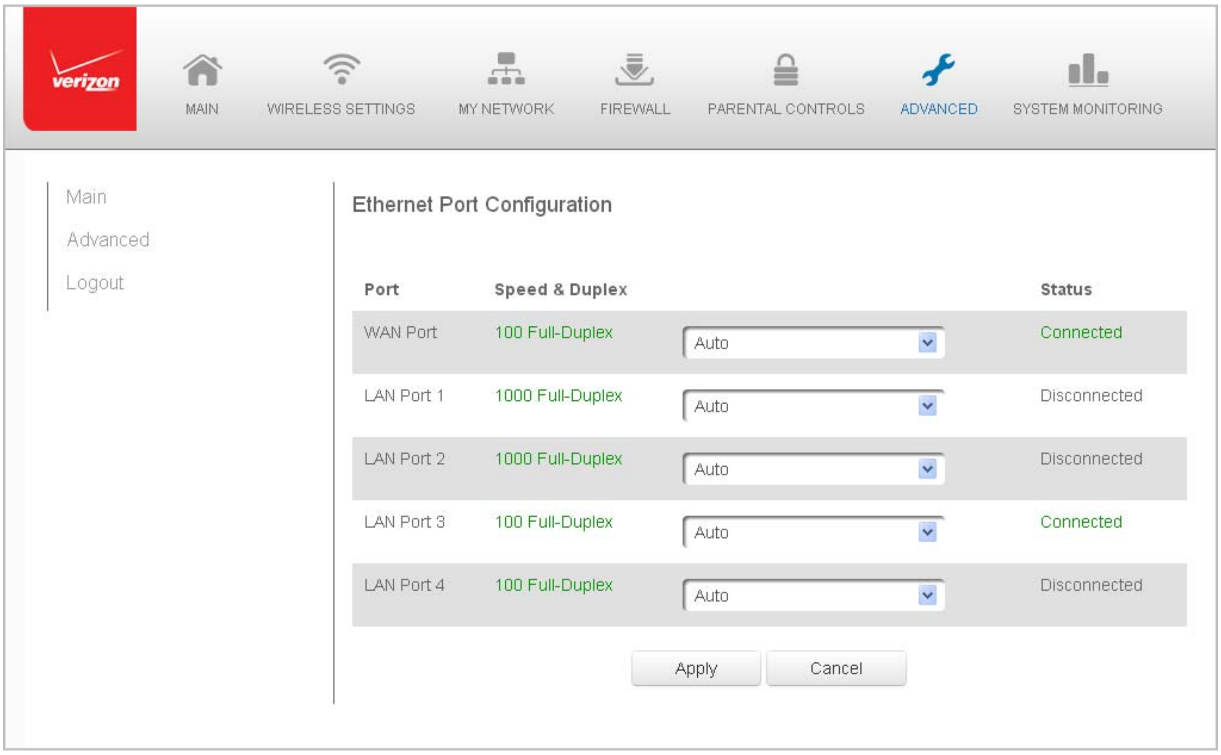
7. In the **Security Logging** section, configure the following security logging options:
   - **Low Capacity Notification Enabled** – activates low capacity notification. This works in conjunction with the Allowed Capacity before Email Notification and System Log Buffer Size.
   - **Allowed Capacity before Email Notification** – specify the capacity before an email notification is sent.
   - **System Log Buffer Size** – specify the size of the system log buffer.
   - **Remote System Notify Level** – specify the type of information, such as none, error, warning, and information, received for remote system logging.
8. In the **Auto WAN Detection** section, specify the DHCP timeout.
9. Click **Apply** to save changes.

## Ethernet 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 Advanced page.



Ethernet Port Configuration

| Port | Speed & Duplex | | Status |
|---|---|---|---|
| WAN Port | 100 Full-Duplex | Auto | Connected |
| LAN Port 1 | 1000 Full-Duplex | Auto | Disconnected |
| LAN Port 2 | 1000 Full-Duplex | Auto | Disconnected |
| LAN Port 3 | 100 Full-Duplex | Auto | Connected |
| LAN Port 4 | 100 Full-Duplex | Auto | Disconnected |

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.

# Chapter 9 Monitoring your Gateway

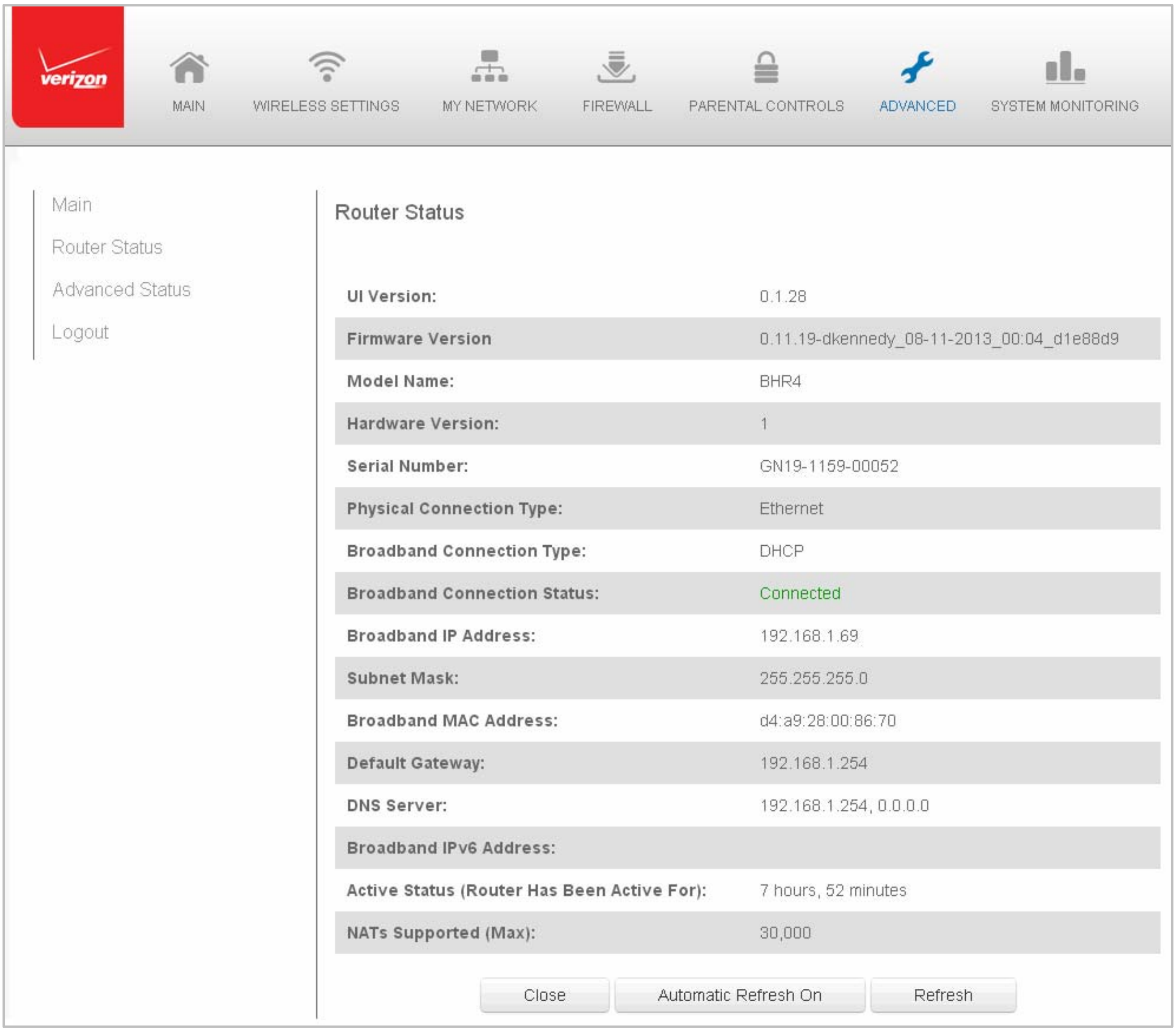
System Monitoring displays system information, including basic settings, system log, key network device parameters, and network traffic statistics.

## Gateway Status

You can view the basic settings of your Gateway.

➢ To view the basic settings:

1. Select **System Monitoring** in the Main menu. The Router Status page displays.



Router Status

| | |
|---|---|
| UI Version: | 0.1.28 |
| Firmware Version | 0.11.19-dkennedy_08-11-2013_00:04_d1e88d9 |
| Model Name: | BHR4 |
| Hardware Version: | 1 |
| Serial Number: | GN19-1159-00052 |
| Physical Connection Type: | Ethernet |
| Broadband Connection Type: | DHCP |
| Broadband Connection Status: | Connected |
| Broadband IP Address: | 192.168.1.69 |
| Subnet Mask: | 255.255.255.0 |
| Broadband MAC Address: | d4:a9:28:00:86:70 |
| Default Gateway: | 192.168.1.254 |
| DNS Server: | 192.168.1.254, 0.0.0.0 |
| Broadband IPv6 Address: | |
| Active Status (Router Has Been Active For): | 7 hours, 52 minutes |
| NATs Supported (Max): | 30,000 |

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

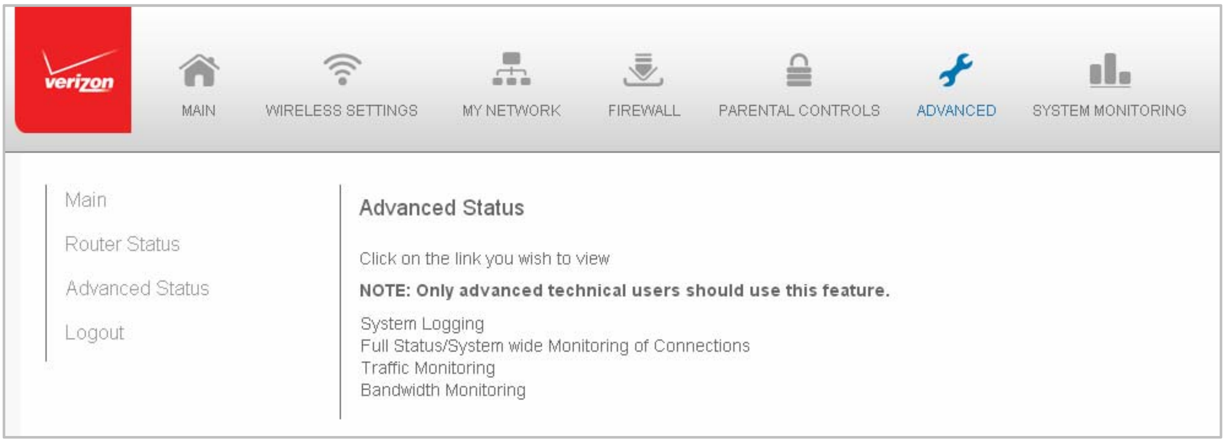
## Advanced Status

You can view the details and status of:

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

➢ To view the advanced status:

1. Select **Advanced Status**. A warning page displays.
2. Click **Yes**. The Advanced Status page displays.



Advanced Status

Click on the link you wish to view

**NOTE: Only advanced technical users should use this feature.**

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

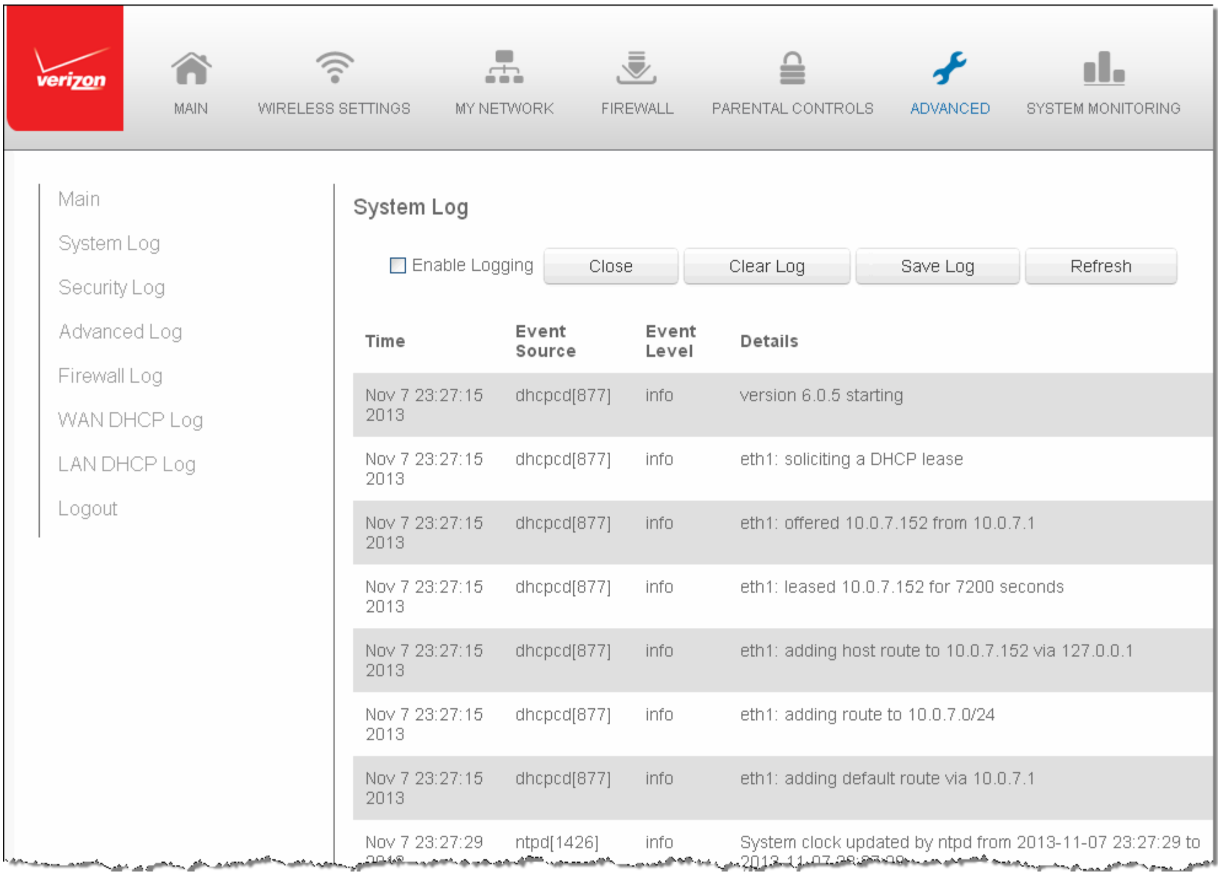
3. To view the details of the listed monitoring options, click the link.

## System Logging

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

➢ To view the system log:

1. In the Advanced Status page, click the **System Logging** link.



| Time | Event Source | Event Level | Details |
|---|---|---|---|
| Nov 7 23:27:15 2013 | dhcpcd[877] | info | version 6.0.5 starting |
| Nov 7 23:27:15 2013 | dhcpcd[877] | info | eth1: soliciting a DHCP lease |
| Nov 7 23:27:15 2013 | dhcpcd[877] | info | eth1: offered 10.0.7.152 from 10.0.7.1 |
| Nov 7 23:27:15 2013 | dhcpcd[877] | info | eth1: leased 10.0.7.152 for 7200 seconds |
| Nov 7 23:27:15 2013 | dhcpcd[877] | info | eth1: adding host route to 10.0.7.152 via 127.0.0.1 |
| Nov 7 23:27:15 2013 | dhcpcd[877] | info | eth1: adding route to 10.0.7.0/24 |
| Nov 7 23:27:15 2013 | dhcpcd[877] | info | eth1: adding default route via 10.0.7.1 |
| Nov 7 23:27:29 | ntpd[1426] | info | System clock updated by ntpd from 2013-11-07 23:27:29 to |

2. To monitor a specific feature, click the link in the System Log menu in the left column.

3. To enable logging, select the **Enable Logging** check box to monitor that functionality.

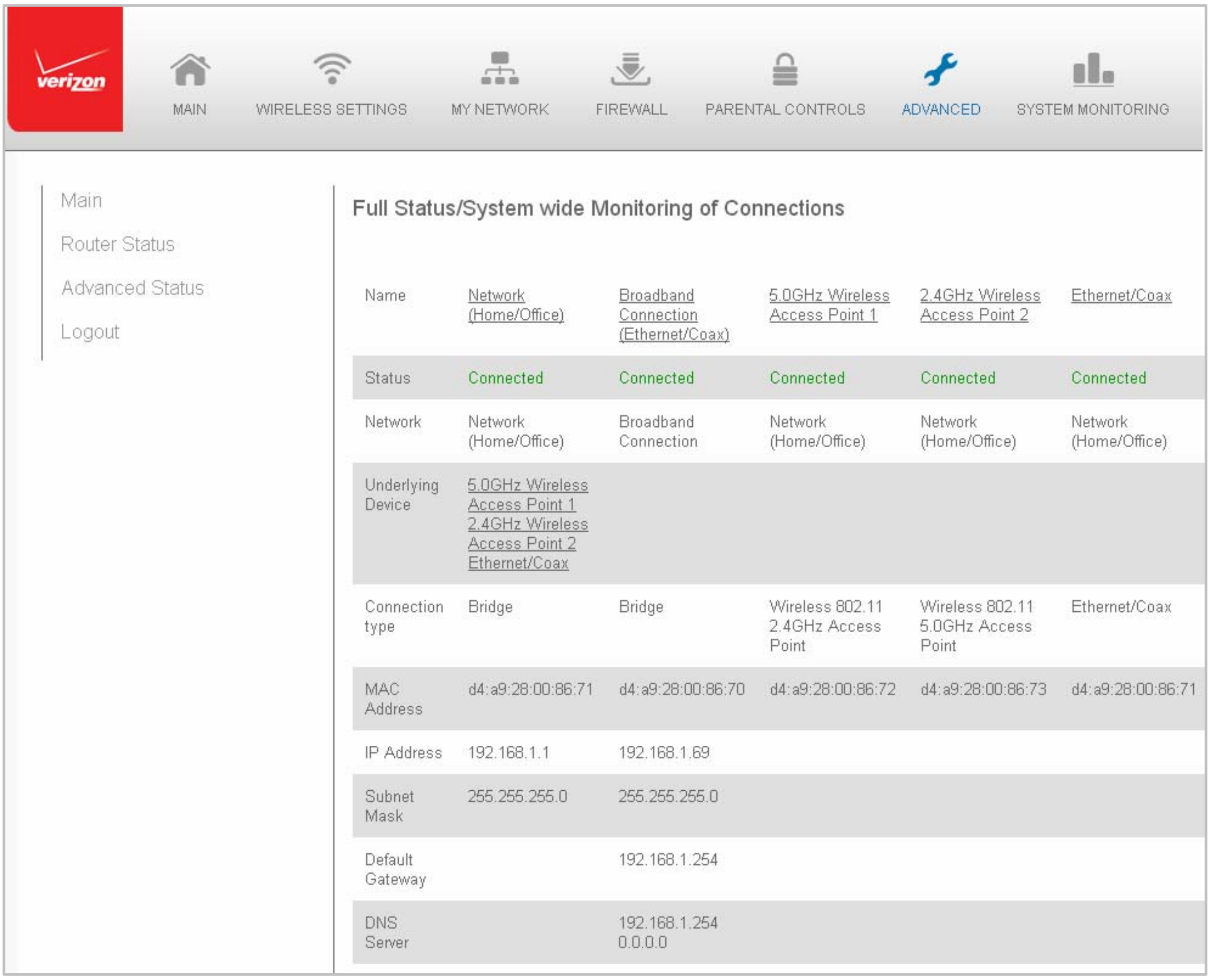
4. To update the data, click **Refresh**.

## Full Status/System wide Monitoring of Connections

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

➢ To view your Gateway’s full system status:

1. In the Advanced Status page, click **Full Status/System wide Monitoring of Connections**.



Full Status/System wide Monitoring of Connections

| Name | Network (Home/Office) | Broadband Connection (Ethernet/Coax) | 5.0GHz Wireless Access Point 1 | 2.4GHz Wireless Access Point 2 | Ethernet/Coax |
|---|---|---|---|---|---|
| Status | Connected | Connected | Connected | Connected | Connected |
| Network | Network (Home/Office) | Broadband Connection | Network (Home/Office) | Network (Home/Office) | Network (Home/Office) |
| Underlying Device | 5.0GHz Wireless Access Point 1<br>2.4GHz Wireless Access Point 2<br>Ethernet/Coax | | | | |
| Connection type | Bridge | Bridge | Wireless 802.11 2.4GHz Access Point | Wireless 802.11 5.0GHz Access Point | Ethernet/Coax |
| MAC Address | d4:a9:28:00:86:71 | d4:a9:28:00:86:70 | d4:a9:28:00:86:72 | d4:a9:28:00:86:73 | d4:a9:28:00:86:71 |
| IP Address | 192.168.1.1 | 192.168.1.69 | | | |
| Subnet Mask | 255.255.255.0 | 255.255.255.0 | | | |
| Default Gateway | | 192.168.1.254 | | | |
| DNS Server | | 192.168.1.254<br>0.0.0.0 | | | |

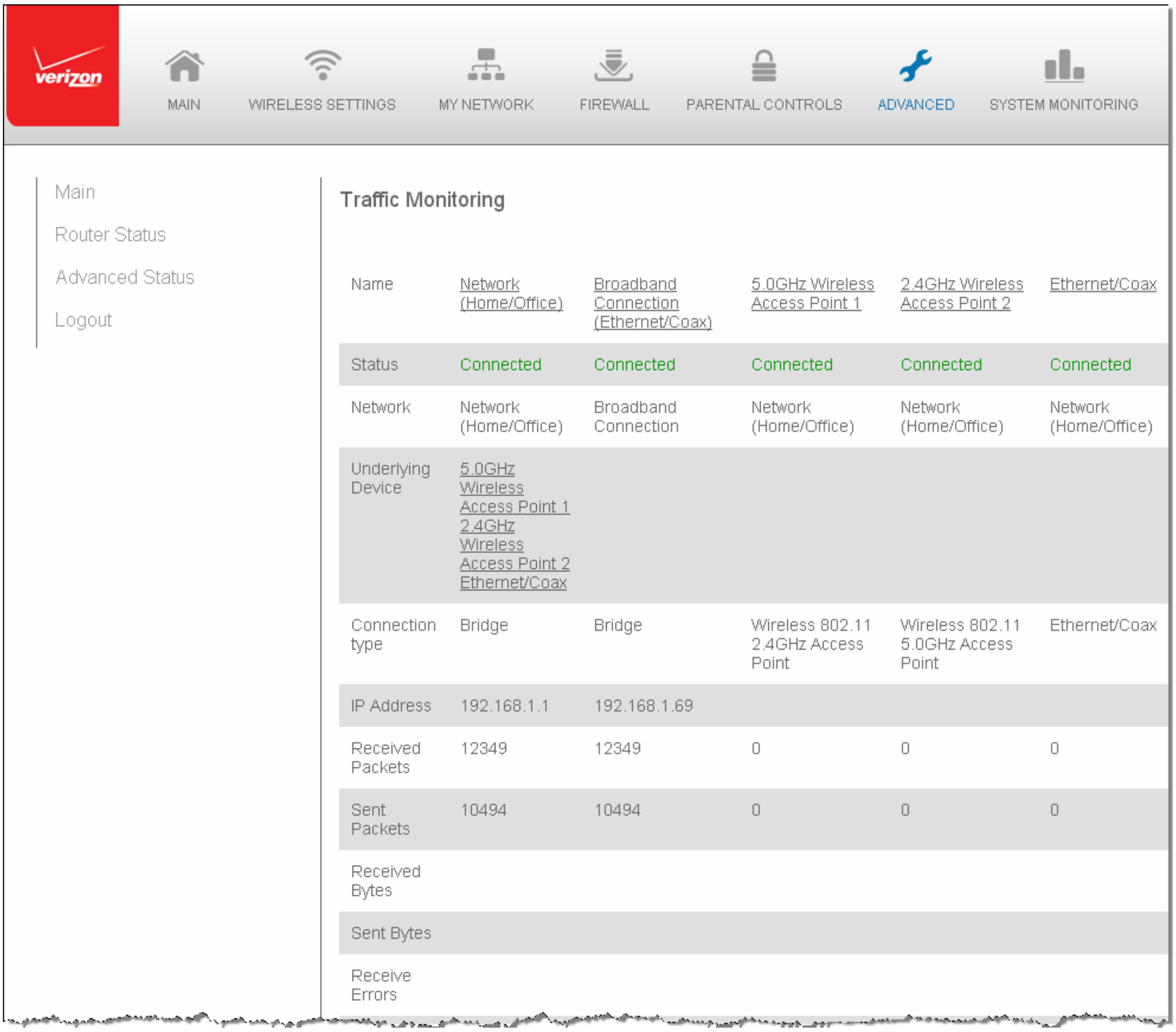
2. To modify the connection properties, click the individual connection links.
3. To refresh the page, click **Refresh**.
4. To continuously refresh the page, click **Automatic Refresh On**.

## Traffic Monitoring

Your Gateway continually monitors traffic in the local area network and between the local network and the Internet. You can view up to the second statistical information about data received from and transmitted to the Internet as well as data received from and transmitted to computers in the local network.

➢ To view the traffic monitoring data:

1. In the Advanced Status page, select **Traffic Monitoring**.



Traffic Monitoring

| Name | Network (Home/Office) | Broadband Connection (Ethernet/Coax) | 5.0GHz Wireless Access Point 1 | 2.4GHz Wireless Access Point 2 | Ethernet/Coax |
|---|---|---|---|---|---|
| Status | Connected | Connected | Connected | Connected | Connected |
| Network | Network (Home/Office) | Broadband Connection | Network (Home/Office) | Network (Home/Office) | Network (Home/Office) |
| Underlying Device | 5.0GHz Wireless Access Point 1<br>2.4GHz Wireless Access Point 2<br>Ethernet/Coax | | | | |
| Connection type | Bridge | Bridge | Wireless 802.11 2.4GHz Access Point | Wireless 802.11 5.0GHz Access Point | Ethernet/Coax |
| IP Address | 192.168.1.1 | 192.168.1.69 | | | |
| Received Packets | 12349 | 12349 | 0 | 0 | 0 |
| Sent Packets | 10494 | 10494 | 0 | 0 | 0 |
| Received Bytes | | | | | |
| Sent Bytes | | | | | |
| Receive Errors | | | | | |

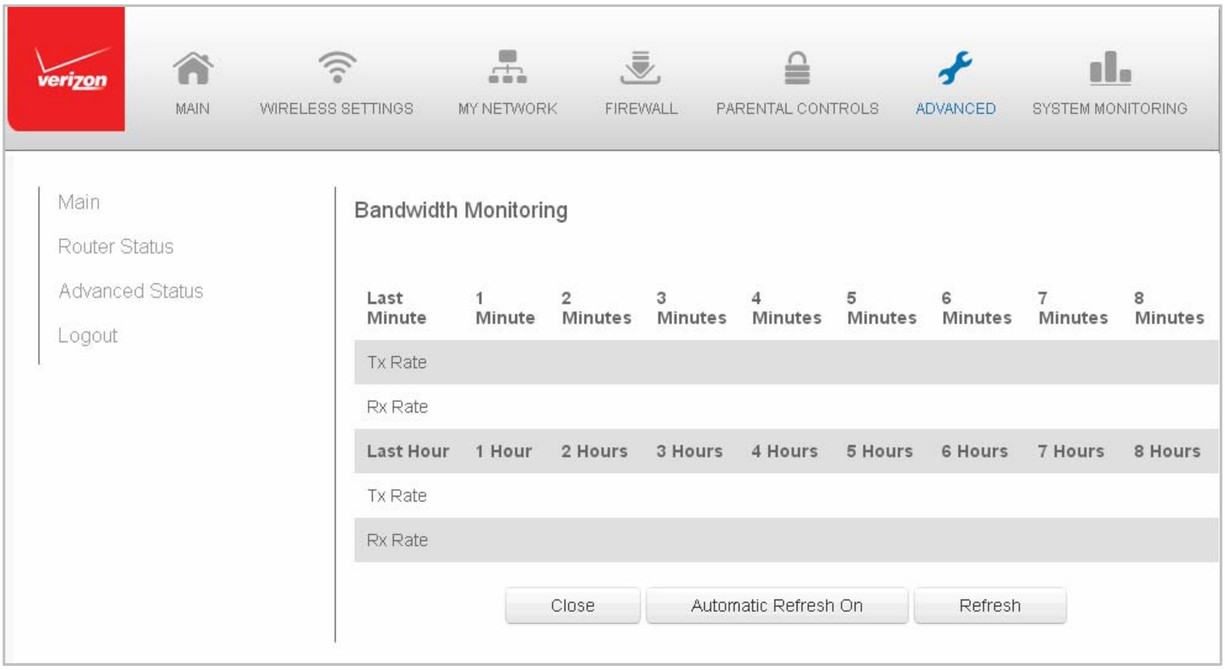
2. To refresh the page, click **Refresh**.
3. To continuously refresh the page, click **Automatic Refresh On**.

## Bandwidth Monitoring

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

➢ To view the bandwidth:

1. In the Advanced Status page, select **Bandwidth Monitoring**.



Bandwidth Monitoring

| Last Minute | 1 Minute | 2 Minutes | 3 Minutes | 4 Minutes | 5 Minutes | 6 Minutes | 7 Minutes | 8 Minutes |
|---|---|---|---|---|---|---|---|---|
| Tx Rate | | | | | | | | |
| Rx Rate | | | | | | | | |
| Last Hour | 1 Hour | 2 Hours | 3 Hours | 4 Hours | 5 Hours | 6 Hours | 7 Hours | 8 Hours |
| Tx Rate | | | | | | | | |
| Rx Rate | | | | | | | | |

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

# Chapter 10 Troubleshooting

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

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

## Troubleshooting Tips

### Accessing your Gateway if you are locked out

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

The common ways to lock access to your Gateway are:

- Scheduler

  If a schedule has been created that applies to the computer over the connection being used, your Gateway will not 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 Gateway is denied.

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

### Restoring your Gateway's default settings

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

- Using the tip of a ballpoint pen or pencil, press and hold the **Reset** button on the back of your Gateway for three seconds.
- Access the GUI and navigate to the Advanced Settings page. Select the **Restore Defaults** option. After saving your configuration, if desired, click the **Restore Defaults** button. For additional details, refer to the **Restore Defaults** section of this guide.

### LAN connection failure

To troubleshoot a LAN connection failure:

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

  If unsure, let the computer get the IP address automatically by initiating the DHCP function, then verify the computer is using an IP address within the default range of 192.168.1.2 through 192.168.1.254.

  If the computer is not using an IP address within the correct IP range, it will not connect to your Gateway.
- Verify the subnet mask address is set to 255.255.255.0.

### Timeout error occurs when entering the URL or IP address

Verify the following:

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

## Front Lighted Indicators

### Flash Speed

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

### Power/Internet Light

🌐

| | |
|---|---|
| Slow flash white | Gateway is starting |
| Solid white | Gateway is powered on and connected to the Internet |
| Slow flash red | Gateway has malfunctioned |
| Solid red | Unable to connect to the Internet |
| Fast flash red | Gateway is overheating. Please verify your Gateway is upright and has sufficient ventilation |

### Wireless Light

| | |
|---|---|
| • Solid white | Wi-Fi is on |

Additional Functions when pressing WPS button:

| | |
|---|---|
| • Slow flash white | When the WPS button is pressed, the Wireless Light slowly flashes white, while waiting for a WPS device to connect. This can require up to two minutes. |
| • Fast flash white | When a device begins connecting to the Gateway using WPS, the Wireless Light fast flashes white for two seconds as establishing connection. |
| • Solid white | When a device successfully completes its WPS association to the Gateway, the Wireless Light returns to solid white. |
| • Fast flash red | If an error occurs during Wi-Fi Protected Setup, the Wireless Light flashes red rapidly for two minutes. |

## 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 Mbps link |
| Solid green | Indicates  10/100 Mbps link |
| Fast flash green | Indicates LAN activity. The traffic can be in either direction. |

**LAN MoCA**

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

**WAN MoCA**

| | |
|---|---|
| Unlit | Indicates no link to the upstream MoCA device |
| Solid green | Indicates network link |

## Frequently Asked Questions

**I've run out of Ethernet ports on my Gateway. How do I add more computers or devices?**

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

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

  Use a crossover cable if there is no Uplink port/switch on your hub, use a crossover cable.

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

**How do I change the password on my Gateway GUI?**

To change the password:

1. On the Main screen, select **Advanced**, then select **Users**.
2. In the Users page, select **Admin**. The User Settings page displays.
3. In the **General** section, change the password.

**Is the wireless option on by default on my Gateway?**

Yes, your Gateway's wireless option is activated out of the box.

**Is the wireless security on by default when the wireless option is activated?**

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

**Which connection speeds does your Gateway support?**

The Ethernet WAN Internet connection supports 100 Mbps. The LAN Ethernet connections support 10/100/1000 Mbps. The 802.11ac wireless connection supports up to 1300 Mbps and the 802.11n supports up to 450 Mbps, depending on signal quality. The MoCA 2.0 connection supports 700 Mbps.

**Are your Gateway's Ethernet ports auto-sensing?**

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

### Can I use an older wireless device to connect to your Gateway?

Yes, your Gateway can interface with 802.11b, g, n, or ac devices. Your Gateway can be setup to handle only n wireless cards, g wireless cards, b wireless cards, or any combination of the three.

### Can my wireless signal pass through floors, walls, and glass?

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

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

In Windows 7, 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.

### My computer cannot connect to the Internet using MoCA. What should I do?

A computer cannot be connected directly using a MoCA cable. It must go through a NIM to connect. The NIM converts the MoCA signal to an Ethernet signal the computer can understand.

First, check the connection and verify all cables are connected correctly. Then verify the NIM is still connected and check the Ethernet connection to the NIM from the computer.

### I used DHCP to configure my network. Do I need to restart my computer to refresh my IP address?

No.  In Windows 7, unplug the Ethernet cable or wireless card, then plug it back in.

### I cannot access your Gateway GUI. What should I do?

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

### 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.

### How many computers can be connected through my Gateway?

Your Gateway 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.

# Chapter 11 Specifications

The specifications for your FiOS Quantum Gateway are as follows. This includes standards, cabling types, and environmental parameters.

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

## General

### Model Number

Model: FiOS-G1100

### Standards

IEEE 802.3x, 802.3u

IEEE 802.11b/g/n/ac

### IP

IP versions 4 and 6

### MoCA

MoCA WAN: 1350 – 1675 MHz and 975 - 1025 MHz

MoCA LAN: 1125 – 1225 MHz

### Speed

Wired WAN

Wired LAN Ethernet: 10/100/1000 Mbps auto-sensing

Wireless LAN:

- 802.11b – up to 11 Mbps
- 802.11g – up to 54 Mbps
- 802.11n – up to 450 Mbps
- 802.11ac – up to 1300 Mbps

**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

## LED Indicators

**Front Panel**

Power/Internet, Wi-Fi

**Rear Panel**

WAN Coax, LAN Coax, WAN Ethernet, and LAN Ethernet [4]

## Environmental Parameters

**Dimensions and Weight**

**FiOS Quantum Gateway (unit only)**

Size: 1.87” width x 10” height x 7.4” depth

Weight: 1.56 lbs / 0.71 kg

**Complete System (including packaging)**

Size: 9.88” / 251 mm width x 3.90” / 99 mm height x 9.57” / 243 mm depth

Weight: 2.63 lbs / 1.19 kg

**Power**

External, 12V DC, 3.0A

**Certifications**

FCC Part 15, UL 60950-1

**Operating Temperature**

10° C to 40° C (50° F to 104° F)

**Storage Temperature**

-20° C to 85° C (-4° F to 185° F)

**Operating Humidity**

8% to 95% (non-condensing)

**Storage Humidity**

5% to 100% (non-condensing)

# Chapter 12 Notices

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

## Regulatory Compliance Notices

### 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 implementing one or more of the following measures:

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

### Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by GreenWave Reality, Inc., may void the user's authority to operate the equipment.

Declaration of conformity for products marked with the FCC logo – United States only.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference
- This device must accept any interference received, including interference that may cause unwanted operation

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

For operation within the 5.15 ~ 5.25 GHz frequency range, this device is restricted to indoor environments. This device meets all the other requirements specified in Part 15E, Section 15.407 of the FCC Rules.

For questions regarding your product or the FCC declaration, contact:

**GreenWave Reality, Inc**

39 Parker, suite 100, Irvine, CA – 92618

USA

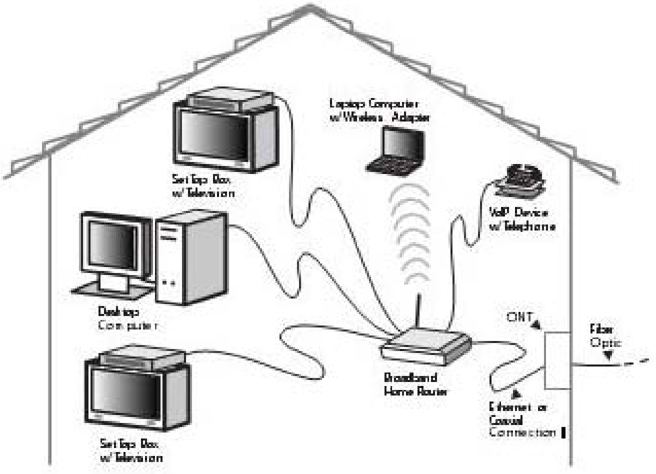
tel: +1 714 805 WAVE (9283)

email: na@greenwavereality.com

## NEBS Requirements

The coaxial cable screen shield must be connected to the Earth at the building entrance per ANSI/NFPA 70, the National Electrical Code (NEC), in particular Section 820.93, “Grounding of Outer Conductive Shield of a Coaxial Cable,” or in accordance with local regulation.

**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.



Typical Broadband Home Router Installation

**Caution:**The Broadband Home Router must be installed inside the home. The Router is not designed for exterior installation.

## General Public License

This product includes software code developed by third parties, including software code subject to the enclosed GNU General Public License (GPL) or GNU Lesser General Public License (LGPL).

The GPL Code and LGPL Code used in this product are distributed WITHOUT ANY WARRANTY and are subject to the copyrights of the authors, and to the terms of the applicable licenses included in the download. For details, see the GPL Code and LGPL Code for this product and the terms of the GPL and the LGPL.