

# Fios Router USER GUIDE



### **CONTENTS**

#### 01/INTRODUCTION

1.0	Package Contents	6
1.1	System Requirements	6
1.2	Features	6
1.3	Getting to Know Your Fios Router	9

## 02/

CONNECTING YOUR FIOS ROUTER

- 2.0 Setting up Your Fios Router 19
- **Expanding Wi-Fi** 2.1 26 coverage
- 2.2 Computer Network Configuration 28
- Main Screen 35 2.3

## 0.3 / WI-FI SETTINGS

- 3.0 Overview 41 3.1 **Basic Settings** 42
- **3.2** Advanced Settings 52

## 04/

CON	INECTED DEVICES	
4.0	Overview	59
1 1	Device Settings	50

evice Settings ວອ

## 05

SETTING PARENTAL CONTROLS 5.0 Activating Parental Controls 5.1 Active Rules 68

65

	<b>5</b> IFIGURING ADVANG TINGS	CED
6.0	Firewall	73
6.1	Utilities	86
6.2	Network Settings	98
6.3	Date & Time	149
6.4	DNS Settings	152
6.5	Monitoring	156
6.6	System Settings	162

## 07/

TROUBLESHOOTING

- 7.0Troubleshooting<br/>Tips168
- 7.1 Frequently Asked Questions 175

## 08/ SPECIFICATIONS

- 8.0General<br/>Specifications1820.1155100
- 8.1 LED Indicators 183
- 8.2 Environmental Parameters 183

#### 09/ NOTICES

9.0 Regulatory Compliance Notices 187

# O1/ INTRODUCTION

- 1.0 Package Contents
- **1.1** System Requirements
- 1.2 Features
- **1.3** Getting to Know Your Fios Router

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

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

## PACKAGE CONTENTS, SYSTEM REQUIREMENTS AND FEATURES

#### **1.0/ PACKAGE CONTENTS**

Your package contains:

- Fios Router
- Power adapter
- Ethernet cable, three meters (white)

#### **1.1/ SYSTEM REQUIREMENTS**

System and software requirements are:

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

#### **1.2/ FEATURES**

Your Fios Router features include:

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

- MoCA 2.5 LAN enabled to support speeds up to 2500 Mbps over coaxial cable
- MoCA 1.1 WAN enabled to support speeds up to 100 Mbps over coaxial cable
- One USB 3.0 port
- IoT Bluetooth and Wi-Fi
- Integrated Wi-Fi networking with 802.11a/b/g/n/ac/ax access point featuring:
  - backward compatible to 802.11a/b/g/n/ac
  - 2.4 GHz 11ax 4x4
  - two 5 GHz 11ax 4x4
- Enterprise-level security, including:
  - Fully customizable firewall with Stateful Packet Inspection (SPI)
  - Content filtering with URL-keyword based filtering, parental controls, and customizable filtering policies per computer
  - Intrusion detection with Denial of Service protection against IP spoofing attacks, scanning attacks, IP fragment overlap exploit, ping of death, and fragmentation attacks
  - Virtual server functionality; providing protected access to internet services such as web, FTP, email, and telnet
  - DMZ (demilitarized zone) host support of a network security neutral zone between a private network and the internet
  - Event logging
  - Home Network Protection

## FEATURES

- Static NAT
- Port forwarding
- Port triggering
- Access control
- Advanced Wi-Fi protection featuring WPA2 & WPA3 Modes and MAC address filtering
- Wi-Fi Multimedia (WMM) for Wi-Fi QoS (quality-of-service)
- Dual-stack network configuration of IPv4 and IPv6
- DHCP server
- WAN interface auto-detection
- Dynamic DNS
- DNS server
- LAN IP and WAN IP address selection
- MAC address cloning
- QoS support (end to end layer 2/3) featuring: Differentiated Services (Diffserv), 802.1p/q prioritization, and pass-through of WAN-side DSCPs, Per Hop Behaviors (PHBs), and queuing to LAN-side devices
- Secure remote management using HTTPS or My Fios app
- Static routing
- VPN (VPN pass through only)
- IGMP
- Daylight savings time support

#### **1.3/ GETTING TO KNOW YOUR FIOS ROUTER 1.3a/ FRONT PANEL**

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

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



Router S	tatus	LED
----------	-------	-----

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

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

## **GETTING TO KNOW YOUR FIOS ROUTER**

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

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

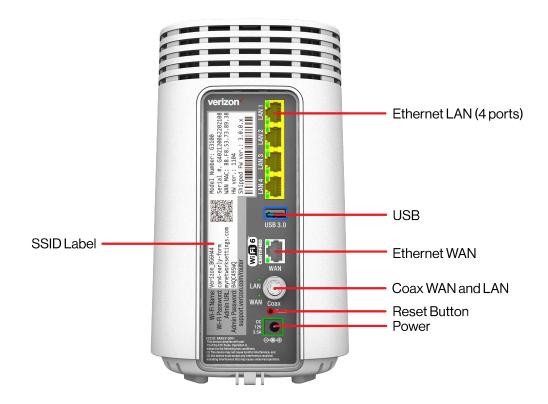
Refer to the "Connecting A Wi-Fi Device Using WPS" on page 31 for more details. In addition, the unified button also provides a quick view of the operational state of the Fios Router using various colors as indicated in the chart above. Please refer to section 7.0h for details on the rear LEDs.

#### 1.3b/ REAR PANEL

The rear panel of your router has a label that contains important information about your device, including the default settings for the Fios Router's Wi-Fi name (SSID), Wi-Fi password (WPA2 key), local URL for accessing the router's administrative pages, and administrator password. The label also contains a QR code that you can scan with your smartphone, tablet, or other cameraequipped Wi-Fi device to allow you to automatically connect your device to your Wi-Fi network without typing in a password (requires a QR code reading app with support for Wi-Fi QR codes).

Wi-Fi Name: Verizon\_BG6H44

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



## **GETTING TO KNOW YOUR FIOS ROUTER**

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

*Warning:* The WAN coax port is intended for connection to Verizon Fios only. It must not be connected to any exterior or interior coaxial wires not designated for Verizon Fios.

- Reset Button allows you to reset your router to the factory default settings. To perform a soft reboot, press and hold the button for at least three seconds. To reset your router to the factory default settings, press and hold the button for at least ten seconds.
- **Power** connects your Fios Router to an electrical wall outlet using the supplied power adapter.

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

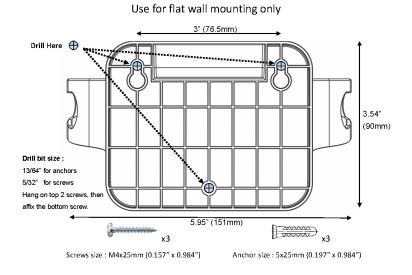
#### **1.3c/ MOUNTING THE FIOS ROUTER TO A WALL**

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

verizon.com/home/accessories/networking-wifi

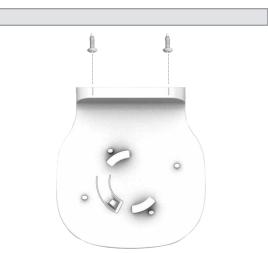
To mount your Fios Router to a wall:

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



## **GETTING TO KNOW YOUR FIOS ROUTER**

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



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



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



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



## **GETTING TO KNOW YOUR FIOS ROUTER**

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



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



## CONNECTING YOUR FIOS ROUTER

- 2.0 Setting up Your Fios Router
- **2.1** Expanding Wi-Fi coverage
- 2.2 Computer Network Configuration
- 2.3 Main Screen

18

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

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

## **SETTING UP YOUR FIOS ROUTER**

#### 2.0/ SETTING UP YOUR FIOS ROUTER

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

#### 2.0a/ INSTALLATION INSTRUCTIONS

- 1. CONNECT YOUR CABLES
  - A. Connect the coax cable from the coax port on your router to a coax outlet. (Required for Fios TV)
    - Separate subscription required for Fios TV; not available in all areas.
  - B. Connect the Ethernet cable from your router's WAN port to an Ethernet outlet. (Required for internet speeds greater than 100 Mbps)
  - C. Connect the power cord to your router then to an electrical outlet.



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

#### 2. CONNECT YOUR DEVICES

Wired or Wi-Fi? Your choice.

Wired

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

B. Connect the other end to your computer.

#### Wi-Fi

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



- B. On your device, choose your Wi-Fi name when it appears.
- C. Enter the Wi-Fi password exactly as it is on your router label.

## **SETTING UP YOUR FIOS ROUTER**

#### Wi-Fi Network

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

#### **3. COMPLETE ACTIVATION**

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

#### 2.0b/ CONFIGURE YOUR FIOS ROUTER

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

Alternately, you can enter: https://192.168.1.1

P	🛅 New tab	× +	
$\leftarrow$	ightarrow C	mynetworksettings.com	€≡

 If you see Your connection is not private on your screen when you visit <u>https://192.168.1.1</u> for GUI management. It's a security warning message of protecting you against suspicious websites. Your browser places a hold of website access with its security measures. To get to the login screen, click on **ADVANCED** button, then on **Proceed to 192.168.1.1** (unsafe) link.

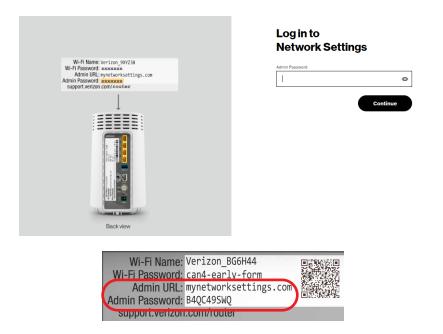
Privacy error	×	0
← → C ▲ Not secu	re   192.168.1.1	☆ 0
	Your connection is not private	
	Attackers might be trying to steal your information from <b>192.168.1.1</b> (for example, passwords, messages, or credit cards). <u>Learn more</u>	
	NET::ERR_CERT_AUTHORITY_INVALID	
	Q To get Chrome's highest level of security, turn on enhanced protection	
	Hide advanced Back to safety	
	This server could not prove that it is <b>192.168.1.1</b> ; its security certificate is not trusted by	
	your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.	
	Proceed to 192.168.1.1 (unsafe)	

4. The login screen will appear.

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

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

## **SETTING UP YOUR FIOS ROUTER**



 Click Continue. The Change Wi-Fi name screen displays. Move the selector to on for setting up your Guest Wi-Fi to personalize your Guest Wi-Fi Name and Password.



verizon <sup>,</sup>	
	Change Wi-Fi name
Wi-Fi Name: Verizon 9XY238 Wi-Fi Password: <del>xcocxocxic</del> Admin UR: mynetworksettings.com Admin Password: xcocxocxic supporturezon.com/cocuter	W-Fi Name Filos-72EK4 W-Fi Password
	Guest Wi-Fi Enabled C
Back view	Guest Wi-FI Password Enter new password
	Back Continue

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

7. Click Continue. The Apply Wi-Fi changes screen appears. You have an option of saving the Wi-Fi settings as an image on your device by clicking the Save as image button. After you click Save as image to save your Wi-Fi settings as an image, click Apply to save the Wi-Fi changes to your Fios Router.

## **SETTING UP YOUR FIOS ROUTER**

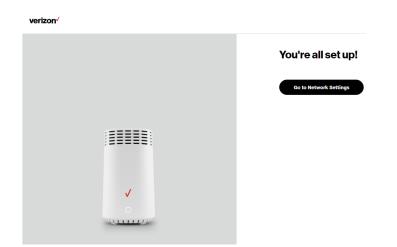
*Note:* If you select *Save as image*, the image file is saved to you web browser's download folder.

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

verizon <sup>/</sup>	
	Apply Wi-Fi changes
Wi-Fi Name: Verizor SVX233 Wi-Fi Possonod: sexecution Admin 21. synchronic settings.com Admin Passoword: sexecution support verizon com/recover	Wi-Flinfo (Save as image)
	W-FPassword fever92280ar8set
	Guest Wi-Fi ON
	Guest Wi-FI Name Fios-7zEK4-Guest Guest Wi-FI Password
Backview	123456789 Back Apply
	Copyright © 2021 Verizon

The **You're all set up!** screen displays once your Fios Router verifies the final settings and has successfully connected to the internet and is ready for use. You can click on **Go to Network Settings** to access the main screen of the Fios Router.





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

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

#### 2.1/ EXPANDING WI-FI COVERAGE

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

## **EXPANDING WI-FI COVERAGE**

#### 2.1a/ WI-FI INSTALLATION

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

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

#### 2.1b/ WIRED INSTALLATION

- 1. Place the Fios Extender and Fios Router near a coax outlet ideally in an area with spotty Wi-Fi coverage.
- Connect the coax cable from the extender to a coax outlet. (If the coax outlet is already in use, you can use the coax splitter included in the shipping box.)
- 3. Connect the power cord to your extender then to an electrical outlet.

4. The light on the extender should turn solid white within a few minutes, indicating the connection is complete.

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

#### 2.2/ COMPUTER NETWORK CONFIGURATION

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

#### 2.2a/ CONFIGURING DYNAMIC IP ADDRESSING

To configure a computer to use dynamic IP addressing:

#### WINDOWS 7/8

- 1. In the Control Panel, locate **Network and Internet**, then select **View Network Status and Tasks**.
- 2. In the View your active networks Connect or disconnect section, click Local Area Connection in the Connections field. The Local Area Connection Status window displays.
- 3. Click **Properties**. The Local Area Connection Properties window displays.

## **COMPUTER NETWORK CONFIGURATION**

- 4. Select Internet Protocol Version 4 (TCP/IPv4), then click Properties. The Internet Protocol Version 4 (TCP/IPv4) Properties window displays.
- 5. Click the **Obtain an IP address automatically** radio button.
- 6. Click the Obtain DNS server address automatically radio button, then click OK.
- 7. In the Local Area Connection Properties window, click **OK** to save the settings.
- 8. To configure Internet Protocol Version 6 (TCP/IPv6) to use dynamic IP addressing, repeat steps 1 to 7. However for step 4, select Internet Protocol Version 6 (TCP/IPv6) in the Properties option (refer to IPv6 section for Fios Router configuration).

#### WINDOWS 10

- 1. On the Windows desktop, click on the **Start** icon. Select **Settings** and click **Network & Internet**.
- 2. In the Network & Internet, click Ethernet.
- 3. Select Network and Sharing Center. The View your basic network information and set up connections window displays.
- 4. In the View your active networks, click Ethernet in the Connections field. The Ethernet Status window displays.
- 5. Click Properties. The Ethernet Properties window displays.

- 6. Select Internet Protocol Version 4 (TCP/IPv4), then click Properties. The Internet Protocol Version 4 (TCP/IPv4) Properties window displays.
- 7. Click the Obtain an IP address automatically radio button.
- 8. Click the Obtain DNS server address automatically radio button, then click OK.
- 9. In the Local Area Connection Properties window, click OK to save the settings.
- To configure Internet Protocol Version 6 (TCP/IPv6) to use dynamic IP addressing, repeat steps 1 to 9. However for step 6, select Internet Protocol Version 6 (TCP/IPv6) in the Properties option (refer to IPv6 section for Fios Router configuration).

#### **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.

## **COMPUTER NETWORK CONFIGURATION**

#### 2.2b/ CONNECTING OTHER COMPUTERS AND NETWORK DEVICES

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

#### ETHERNET

- 1. Plug one end of an Ethernet cable into one of the open yellow Ethernet ports on the back of your Fios Router.
- 2. Plug the other end of the Ethernet cable into an Ethernet port on the computer.
- 3. Repeat these steps for each computer to be connected to your Fios Router using Ethernet. You can connect up to four.

#### **CONNECTING A WI-FI DEVICE USING WPS**

Wi-Fi Protected Setup (WPS) is an easier way for many devices to set up a secure Wi-Fi network connection. Instead of manually entering passwords or multiple keys on each Wi-Fi client, such as a laptop, printer, or external hard drive, your Fios Router creates a secure Wi-Fi network connection.

In most cases, this only requires the pressing of two buttons – one on your Fios Router and one on the Wi-Fi client. This could be either a built-in button or one on a compatible Wi-Fi adapter/card, or a virtual button in software. Once completed, this allows Wi-Fi clients to join your Wi-Fi network. To initialize the WPS process, you can either press and hold the unified button located on the front of your Fios Router for more than two seconds or use the UI and press the on-screen button.

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

To access WPS using the user interface:

1. From the **Basic** menu, select **Wi-Fi** settings, then click **Wi-Fi Protected Setup**.

verizon <sup>,/</sup> Basic	Advanced		Hele Q ~
Network Device	~	Wi-Fi > Wi-Fi Protected Setup	
Home	^	Wi-Fi Protected Setup	
Wi-Fi	^	Enable Wi-Fi Protected Setup	WPS Enabled
Primary Network	_	Wi-Fi Protected Setup is an easy way to add Wi-Fi devices to your network. To use this feature, your Wi-Fi client device needs to support WPS.	
Guest Network	- 1	A Wi-Fi devices may briefly lose connectivity when turning WPS on or off.	
IoT Network			
Wi-Fi Protected Setup	- 1	Option 1 (Recomended)	Option 2
Devices	×	If your client device has a WPS button, press it and then click the button below to start WPS registration.	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":
Parental Controls	o	Start WPS	Enter PIN Register
Status	×		If your client supports it, enter the router's PIN into the client device;
	- 1		Enable router's PIN: 22466792

- 2. Enable the protected setup by moving the selector to on.
- 3. Use one of the following methods:
  - If your Wi-Fi client device has a WPS button, press the unified button on your Router for more than two seconds, then click the start WPS button in the Option 1 to start the WPS registration process.

## **COMPUTER NETWORK CONFIGURATION**

- If your client device has a WPS PIN, locate the PIN printed on the client's label or in the client documentation. Enter the PIN number in the Enter PIN field. The Client WPS PIN field is located in the Option 2 on the user interface.
- Click Register.
- Alternatively, you can enter the Router's PIN shown on this screen into the WPS user interface of your device, if this PIN mode is supported by your Wi-Fi device.
- 4. After pressing the unified button (WPS) on your Router, you have two minutes to press the WPS button on the client device before the WPS session times out.

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

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

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

#### CONNECTING A WI-FI DEVICE USING A PASSWORD

- 1. Verify each device that you are connecting with Wi-Fi has built-in Wi-Fi or an external Wi-Fi adapter.
- 2. Open the device's Wi-Fi settings application.
- 3. Select your Fios Router's Wi-Fi network name (SSID) from the device's list of discovered Wi-Fi networks.
- 4. When prompted, enter your Fios Router's Wi-Fi password (WPA2 or WPA3 key) into the device's Wi-Fi settings. Your Router's default Wi-Fi network name and password are located on the sticker on the rear panel of your Fios Router.



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

#### COAX

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

## MAIN SCREEN

#### 2.3/ MAIN SCREEN

When you log into your router, the dashboard main page displays the navigation menus of Basic and Advanced settings, Wi-Fi settings, Devices, Parental Controls, and connection status, and Basic quick links.

Fios Router	✓ S	atus Offline	>	Wi-Fi	>
Hoshoulei	·				· · · · · ·
lome				₩i-Fi Name     Fios-7zEK4	
Vi-Fi	~			- Wi-Fi Password	
Devices	U.S.			A	
		$\checkmark$			
Parental Controls	0			Parental Controls	>
itatus	~	CONTRACTOR OF THE OWNER OWNER OWNER OF THE OWNER			
		I			
	D	evices	>		
	E	A0005-NB2			
		E3200-b8f85384e668			

The main menu contains the following configuration options and chapters:

- Basic Settings
  - Status this chapter
  - Wi-Fi Chapter 3
  - Devices Chapter 4
  - Parental Controls Chapter 5
- Advanced Settings Chapter 6

#### 36

#### 2.3c/ STATUS

#### General

To view the status:

Access the dashboard Home page . You can quickly view your router's status by clicking **Status** > on the screen. This section displays the status of your router's local network (LAN) and internet connection (WAN), firmware and hardware version numbers, MAC Address, IP settings of Fios Router and Fios Extender(s) (if connected).

work Device		Status > General		
Fios Router	~	Status	Auto-refresh	Refresh
ome		Status		
/I-FI	~	Broadband IPv4	Broadband IPv6	
evices	*	Status Disconnected	Status Disconnected	
Parental Controls Status	0	IPv4 address is from: DHCP	IPv6 address is from: DHCPv6+PD	
General		IPv4 address 0.0.0.0	Delegated Prefix	
Open Source Software		Subnet Mask 0.0.0.0	IPv6 Address N/A	
		IPv4 Default Gateway 0.0.0.0	Link-Local Address	
		IPv4 DNS Address	IPv6 Default Gateway	
		NATs Supported (used / max) 0 / 30000	IPv6 DNS Address	
		Router		
		Firmware Version 3.1.0.12		

## **MAIN SCREEN**

verizon Basic Advance	ced		Hele 🔕 v
Network Device	Status > General		
Fios Router 🗸 🗸			
	Status	Auto-refresh	Refresh
Home			
WI-FI v	Router		
Devices ~	Firmware Version 3.1.0.12		
Parental Controls 0	Hardware Version ROB		
Status ^	Model Name G3100		
General	Serial Number G401119012200078		
Open Source Software	LAN IPv4 Address 192.168.1.1		
	Broadband MAC address 78:D0:12:C9:40:A3		
	Broadband Physical Connection Disconnected		
	Router has been active for 0 day(s) 0 hours 23 minutes 48 seconds		
		-	
	Extender		
	Device Name E3200-b8185384e668		_
			*
verizon <sup>/</sup> Basic Advan	bed		Hele 🛞 -
Network Device	Status > General		
Fios Router 🗸 🗸			
Home	Status	Auto-refresh	Refresh
WI-FI ~	Device Name E3200-b8f85384e668		<b>^</b>
Devices	Model Name E3200		
Parental Controls 0	Firmware Version 3.10.8-eng0		
Status ^	Hardware Version 1102		
General	Serial Number E301120071800005		
Open Source Software	MAC Address B8F8.53:84.E6.68		
	System Up Time 0 day(s) 3 hours 24 minutes 23 seconds		
	Backhaul Type Ethernet		



#### 2.3d/ Open Source Software

verizon <sup>4</sup> Bas	lc Advance	Hele Q ~
Network Device		Status > Open Source Software
Fios Router	~	
-		Open Source Software
Home		This product includes software made available under open source licenses. Additional information about that
WI-FI	~	software, applicable licenses, and downloadable copies of source code, is available at:
Devices	~	https://verizon.com/opensourse/ All open source software contained in this product is distributed WITHOUT ANY WARRANTY, All such software is
Parental Controls	0	subject to the copyrights of the authors and to the terms of the applicable licenses included in the download.
Status	^	This information is provided for those who wish to edit or otherwise change such programs. You do not need a copy of any of such open source software source code to install or operate the device.
General		
Open Source Softw	are	

This product includes software made available under open source licenses. Additional information about that software, applicable licenses, and downloadable copies of source code, is available at:

https://verizon.com/opensource/

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

All open source software contained in this product is distributed WITHOUT ANY WARRANTY. All such software is subject to the copyrights of the authors and to the terms of the applicable licenses included in the download.

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

# 03/ WI-FISETTINGS

- 3.0 Overview
- 3.1 Basic Settings
- 3.2 Advanced Settings

40

Wi-Fi networking enables you to free yourself from wires, making your devices more accessible and easier to use.

You can create a Wi-Fi network, including accessing and configuring Wi-Fi security options.

## **OVERVIEW**

## 3.0/ OVERVIEW

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

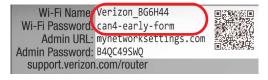
802.11b has a maximum data rate of 11 Mbps, 802.11a and 802.11g have a maximum data rate of 54 Mbps, 802.11n has a maximum data rate of 450 Mbps, 802.11ac has a maximum data rate of 3.12 Gbps, and 802.11ax has a maximum data rate of 4.8 Gbps.

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

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

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

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



#### **3.1/ BASIC SETTINGS 3.1a/ PRIMARY NETWORK**

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

verizon Basic	Advanced	d	Hele Q ~
Network Device	~	WLFI > Primary Network	
Home		Primary Network	
Wi-Fi	^	Wi-Fi Name Wi-Fi Nasword Filos-72EK4	Wi-Fi Enabled
Primary Network	- 1		Ø
Guest Network	- 1	Security Set encryption type used to secure the Wi-Fi traffic.	WPA2 V
IoT Network			
Wi-Fi Protected Setup	- 1	2.4 GHz	Wi-Fi Enabled 🌑 🔅 🗸
Devices	×	5 GHz 1	Wi-Fi Enabled 🌑 🖓 🗸
Parental Controls	0	5 GHz 2	Wi-Fi Enabled 🌑 🚷 🗸
Status	~		

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

- 1. From the **Basic** menu, select **Wi-Fi** from the left pane and then click **Primary Network**.
- 2. To activate the Wi-Fi radio, move the selector to **on**. If the radio is not enabled, no Wi-Fi devices will be able to connect to the home network.
- 3. If desired, enter a new name and password for the Wi-Fi network or leave the default name and password that displays automatically.

*Note:* The SSID is the network name. All devices must use the same SSID.

## **BASIC SETTINGS**

4. To configure the Wi-Fi security, click the setup 🕸 button and select WPA2 or WPA3.

etwork Device		Wi-Fi > Primary Network			
Fios Router	$\sim$				
	*	<b>Primary</b>	letwork		
lome	- 1	Wi-Fi Name	Wi-Fi Password		
/i-Fi	^	Fios-7zEK4	••••••	Wi-Fi Enabled	•
Primary Network	- 1				
Guest Network	- 1		Security	WPA2	
oT Network	- 1		Set encryption type used to secure the Wi-Fi traffic.		
Vi-Fi Protected Setup	- 1	2.4 GHz		Wi-Fi Enabled	•
evices	÷	5 GHz 1		Wi-Fi Enabled	
arental Controls	o	5 GHz 2		Wi-Fi Enabled	•
tatus	v		Broadcast		Enabled
	- 1		Broadcast Wi-Fi name from router to Wi-Fi clients.		Enabled
			Device Access List		<b>E</b> .414
verizon√ <sub>Basic</sub>	Advance	a	Device Access List MAG authentication limits the W-Fi clients that can connect.		Edit V
	Advance				,
twork Device		d Wi-Fi > Primary Network			,
twork Device Fios Router	Advance		MAC authentication limits the Wi-Fi clients that can connect.		,
twork Device Fios Router ome		Wi-Fi > Primary Network	MAC authentication limits the Wi-Fi clients that can connect.		Hele
twork Device Flos Router		Wi-Fi > Primary Network	MAC authentication limits the Wi-Fi clients that can connect.		Hele
twork Device Fios Router ome fi-Fi Primary Network		Wi-Fi > Primary Network	MAG authentication limits the Wi-Fr clients that can connect.		Hele Apply Changes Edit
Primary Network Suest Network		Wi-Fi > Primary Network	MAC authentication limits the Wi-Pi clients that can connect.	259200	<u>Hele</u> Apply Changes
Fios Router		Wi-Fi > Primary Network	MAG authentication limits the Wi-Pi clients that can connect.  Setwork  Previce Access Lit  MAG authentication limits the Wi-Pi clients that can connect.  Group Key  Lithung Comp Key  Lithung		Hele Apply Changes Edit
Those Router  The Router  The Router  The Router  The Router  Support Router		Wi-Fi > Primary Network	MAC authentication limits the Wi-Fr clients that can connect.		Hele Apply Changes Edit
Filos Router  TrFI  Primary Network  Guest Network  GT Network  W-Fi Protected Setup		Wi-Fi > Primary Network	MAG authenication limits the Wi-Fr clients that can connect.		Hale Apply Changes Enabled
twork Device	×	Wi-Fi > Primary Network	MAG authentication limits the Wi-Fr clients that can connect.		Hale Apply Changes Enabled
Filos Router Filos	× ^ *	Wi-Fi > Primary Network	MAG authentication limits the Wi-Fi clients that can connect.  Settwork  MAG authentication limits the Wi-Fi clients that can connect.  Group Key  MAG authentication limits the Wi-Fi clients that can connect.  Group Key  Wi-Fi Go Key based on time interval used to update the WPA chardo key.  Wi-Fi Go Key based on time interval used to update the WPA chardo key.  Wi-Fi Go Key based on time interval used to update the WPA chardo key.  Wi-Fi Go Key based on time interval used to update the WPA chardo key.  Wi-Fi Go Key based on time interval used to update the WPA chardo key.  Wi-Fi Go Key based on time interval used to update the wPA chardo key.  Wi-Fi Go Key based on time interval used to update the wPA wi-Fi down the Wi-Fi devices such as smart phones and		Hele Apply Changes Edit Enabled

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

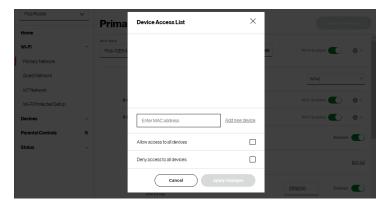
44

#### Broadcast

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

- To enable SSID broadcasting, move the selector to on.
   SSID broadcast is enabled by default. The SSID of the Wi-Fi network will be broadcast to all Wi-Fi devices.
- To disable SSID broadcasting, move the selector to off. The public SSID broadcast will be hidden from all Wi-Fi devices. You will need to manually configure additional Wi-Fi devices to join the Wi-Fi network.
- Device Access List

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



## **BASIC SETTINGS**

To set Wi-Fi MAC authentication:

- 1. To setup access control, click on the Edit List.
- 2. Enter the MAC address of a device.
- **3**. Select either:
  - Allow access to all devices allows the listed devices to access the Wi-Fi network.

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

- Deny access to all devices denies access to the listed devices. All other Wi-Fi devices will be able to access the Wi-Fi network if they use the correct Wi-Fi password.
- 4. Repeat step 2 and step 3 to add additional devices, as needed.
- 5. When all changes are complete, click **Apply Changes** to save the changes.
- Group key to update the WPA shared key, move the selector to on.
- Wi-Fi QoS (WMM) improves the quality of service (QoS) for voice, video, and audio streaming over Wi-Fi by prioritizing these data streams.

- WMM Power Save improves battery life on mobile Wi-Fi devices such as smart phones and tablets by fine-tuning power consumption.
- 802.11 Mode

You can limit the Wi-Fi access to your network by selecting the 2.4 GHz and 5 GHz Wi-Fi communication standard best suited for the devices you allow to access your Wi-Fi network.

Select the Wi-Fi mode as follows:

- Compatibility This is the default mode setting on 5 GHz, providing a good balance of performance and interoperability with existing Wi-Fi devices. 802.11a,n,ac and ax devices can connect.
- Legacy This is the default mode setting on 2.4 GHz, providing broad connection support for old and new Wi-Fi devices. Only 802.11b,g and n devices can connect.
- 802.11n is available on both 2.4 GHz and 5 GHz frequencies.
- Connecting 802.11a, b or g devices will cause your Wi-Fi network to slow on that radio and is not recommended.
- **Transmit Power** adjusts the power of the Wi-Fi signal.

## **BASIC SETTINGS**

#### **3.1b/ GUEST NETWORK**

The **Guest Network** is designed to provide internet connectivity to your guests but restricts access to your primary network and shared files. The primary network and the guest network are separated from each other through firewalls. You create one Guest Wi-Fi SSID and one password, and use it for all guests. The guest network SSID does not change when you make a change to your primary network SSID.

The Fios Router is shipped from the factory with Guest Wi-Fi turned off. The default SSID for Guest Wi-Fi is preconfigured at the factory to the default Wi-Fi network name (SSID) which is displayed on a sticker located at the rear of the router followed by hyphen guest (-Guest). For example – if the router is shipped with a default SSID of "Fios-ABCDE" then the default SSID for Guest Wi-Fi is "Fios-ABCDE-Guest".

verizon <sup>,</sup> Ba	isic Adv	anced			Hele Q ~
Network Device		WI-FI > G	uest Network		
Fios Router	~				
Home		Gue	est Network		
Wi-Fi	~	Band	Wi-Fi Name	Wi-Fi Password	_
		2.4 GHz	Fios-7zEK4-Guest	••••••	Wi-Fi Enabled 🚺 🐐
Primary Network					
Guest Network			Security	e used to secure the Wi-Fi traffic.	WPA2 ~
IoT Network			and in cryption cyp		
Wi-Fi Protected Set	tup				
Devices	v				
Parental Controls	0				
Status	v			Copyright © 2021 Verizon	

To configure the security settings for your guest network:

- 1. From the **Basic** menu, select **Wi-Fi** and then click **Guest Network**.
- 2. Move the selector to on.
- 3. If desired, enter a new name and password for the Wi-Fi network or leave the default name and password that displays automatically.
- 4. Press Apply Changes to save the changes.

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

#### **3.1c/IOT NETWORK**

The router supports connection of multiple IoT devices on a separate WiFi SSID. The IoT Network is designed to provide an easier setup experience for your Internet of Things (IoT) devices which benefit from connecting to the 2.4 GHz band while keeping your Primary Network settings unchanged. IoT devices and Primary devices can communicate with no firewall restrictions separating them.

The Fios Router is shipped from the factory with IoT Wi-Fi turned off. The default SSID for IoT Wi-Fi is preconfigured at the factory to the default Wi-Fi network name (SSID) which is displayed on a sticker located at the rear of the router followed by hyphen IoT (-IoT). For example – if the router is shipped with a default SSID of "Fios-ABCDE" then the default SSID for IoT Wi-Fi is "Fios-ABCDE-IoT".

## **BASIC SETTINGS**

verizon Basic	Advance	d				Hele @
Network Device		WI-FI > 10	F Network			
Fios Router	~					
Home		loT	Network			Apply Changes
Wi-Fi	^	Band	Wi-Fi Name Fios-7zEK4-IoT	Wi-Fi Password	٩	Wi-Fi Enabled 🌑 👸
Primary Network						Ċ,
Guest Network			Security Set encryption	type used to secure the Wi-Fi trafi	fic.	WPA2 ~
IoT Network						
Wi-Fi Protected Setup						
Devices	v					
Parental Controls	0					
Status	~			Copyright F	© 2021 Verizon	

To enable IoT Wi-Fi link:

- 1. From the **Basic** menu, select **Wi-Fi** and then click **IoT Network**.
- 2. Move the selector to on.
- 3. If desired, enter a new name and password for the Wi-Fi network or leave the default name and password that displays automatically.
- 4. Press Apply Changes to save the changes.

#### 3.1d/ WI-FI PROTECTED SETUP (WPS)

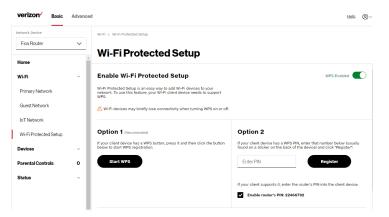
Wi-Fi Protected Setup (WPS) is an easier way for many devices to set up a secure Wi-Fi network connection. Instead of manually entering passwords or multiple keys on each Wi-Fi client, such as a laptop, printer, or external hard drive, your Fios Router creates a secure Wi-Fi network connection. In most cases, this only requires the pressing of two buttons – one on your Fios Router and one on the Wi-Fi client. This could be either a built-in button or one on a compatible Wi-Fi adapter/card, or a virtual button in software. Once completed, this allows Wi-Fi clients to join your Wi-Fi network.

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

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

To access WPS using the user interface:

1. From the **Basic** menu, select **Wi-Fi** and then click **Wi-Fi Protected Setup (WPS)**.



2. Enable the protected setup by moving the selector to on.

## **BASIC SETTINGS**

- **3**. Use one of the following methods:
  - If your Wi-Fi client device has a WPS button, press the unified button on your router for more than two seconds, then click the start WPS button in the Option 1 to start the WPS registration process.
  - If your client device has a WPS PIN, locate the PIN printed on the client's label or in the client documentation. Enter the PIN number in the Enter PIN field. The Client WPS PIN field is located within Option 2 on the user interface.
  - Click Register.
  - Alternatively, you can enter the router's PIN shown on this screen into the WPS user interface of your device, if this PIN mode is supported by your Wi-Fi device.
- 4. After pressing the unified button (WPS) on your router, you have two minutes to press the WPS button on the client device before the WPS session times out.

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

If WPS fails to establish a connection to a Wi-Fi client device within two minutes, the Router Status LED on your router flashes red for two minutes to indicate the WPS pairing process was unsuccessful. After flashing red, the light returns to solid white to indicate that Wi-Fi is on. *Note:* Wi-Fi Protected Setup (WPS) cannot be used if WPA3 security is enabled or SSID broadcast is disabled or if MAC address authentication is enabled with an empty white list.

#### **3.2/ ADVANCED SETTINGS 3.2a/ PRIMARY NETWORK**

#### Self-Organizing Network (SON)

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

verizon Basic	Advan	ed	Help & ~
Network Device		WI-FI > Primary Network	
Fios Router	$\sim$		
Home		Primary Network	
WI-FI	^	Self-Organizing Network (SON) Allow devices to move seamlessly botween Wi-Fi bands and extenders, when connected.	SON Enabled
Primary Network		and extenders, when connected.	
Guest Network		Wi-FI Name Wi-FI Password Fios-7zEK4	Wi-Fi Enabled 💽 🔞 ^
IoT Network			
Wi-Fi Protected Setup		Security Set encryption type used to secure the Wi-Fi traffic.	WPA2 V
Channel Settings			
Devices	~	2.4 GHz	Wi-Fi Enabled 🌑 🖓 🗸 I
Parental Controls	0	5 GHz 1	Wi-Fi Enabled 🔵 😵 ~
tatus	~	5 GHz 2	Wi-Fi Enabled 🌑 😫 ^
irewall	~	Broadcast	
Itilities	~	Broadcast Wi-Fi name from router to Wi-Fi clients.	Enabled
letwork Settings	v	Device Access List MAC authentication limits the Wi-Fi clients that can connect.	Edit list
Date & Time	~	Austremolation multis the WH-P Cherts that can connect.	

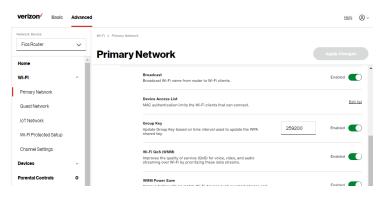
## **ADVANCED SETTINGS**

To configure SON, Wi-Fi radio, SSID and security settings:

- 1. From the Advanced menu, select Wi-Fi from the left pane and then click Primary Network.
- 2. To enable SON, move the selector to on.
- 3. To activate the Wi-Fi radio, move the selector to **on**. If the radio is not enabled, no Wi-Fi devices will be able to connect to the primary network.
- If desired, enter a new name and password for the Wi-Fi network or leave the default name and password that displays automatically.

*Note:* The SSID is the network name. All devices must use the same SSID.

 To configure the Wi-Fi security, click the setup <sup>®</sup> button and select WPA2 or WPA3.



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

## **3.2b/ CHANNEL SETTINGS**

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

verizon Basic	Advanced		Help 🛞 -
Network Device		WI-FI > Channel Settings	
Fios Router	~		
Home	^	Channel Settings Settings Settings History	rm Scan
WI-FI	^	Channel Score 2.4 GHz 5 GHz1 5 GHz2 Channel Analysis 2.4 GHz 5 GHz1 5 GHz2	
Primary Network			- 1
Guest Network	- 1	6 4	
IoT Network	- 1	-70	
Wi-Fi Protected Setup	- 1	1 2 3 4 5 6 7 8 9 10 11 1 2 3 4 5 6 7 8 9 10 11 Score Channel Signal Channel	12 13 14
Channel Settings			
Devices	~	Band         Channel         Width         Health           2.4 GHz         Ch. 1 (Auto)         20/40MHz         9.01	Save
Parental Controls	0		
Status	~	Band Channel Width Health	
Firewall	~	5 GHz 1 Ch. 132 (Auto) V 80MHz V 9.84	Save

To view and configure the channel settings:

- 1. From the Advanced menu, select Wi-Fi and then click Channel Settings.
- 2. Click on **Settings** on the top right-hand side of the **Channel Settings** page to configure the channel scan settings:

	Channel Score 2.4 GHz 5 GHz 1	GHz 2 Cha	annel Analysis 2.4 GHz	
Primary Network	Scan Settings	1	×	
Guest Network	8			
IoT Network	2 Keep my channel s	election during power cycle		
Wi-Fi Protected Setup	1 2 Score Enable DFS chann	els during channel scan	2 3 4 3	
Channel Settings			_	
Devices ~	Band Ch 2.4 GHz C	Apply Changes	D1	
Parental Controls 0				

## ADVANCED SETTINGS

- Select the Keep my channel selection during power cycle check box to save your channel selection when your Fios Router is rebooted.
- Enable DFS channels during channel scan: DFS channels are enabled by default during channel scans.

*Note:* DFS channels are a subset of the 5 GHz network that is shared with radar systems. Some consumer devices do not support these channels and cannot connect to routers using them. Examples include some media streaming devices. Disabling this feature will allow the router to select the best available channel to broadcast on and allow these devices to connect.

- Press Apply Changes to save the changes.
- 3. Click **Perform Scan** to perform channel availability scan for the Fios Router accommodating the best radio channel and providing the best Wi-Fi performance.
- 4. On the **Channel Settings** page for either 2.4 GHz or 5 GHz, the following information displays and can be configured:
  - Channel Score displays a network congestion score of one to ten in each Wi-Fi channel. It can be used to determine which channels to use or to avoid. Higher score indicates less congestion in a channel.
  - **Channel Analysis** scans and displays channel bandwidth and signal strength of available APs.
  - **Channel** this is the radio channel used by the Wi-Fi router and its clients to communicate with each other.

The channel must be the same on the router and all of its Wi-Fi clients. Select the channel you want the Wi-Fi radio to use to communicate, or accept the default (**Auto**) channel selection. Then the router will automatically assign itself a radio channel.

• Width - displays the Wi-Fi channel currently in use on each band. Users can select from available channels.

To view the channel settings history:

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

verizon Basic	Advanced						Help 🛞 🗸
Network Device	~	Wi-Fi > Channel Setting				Settings	erform Scan
Home	-	Settings History	Settings				
WI-FI	^	Band	Channel	Time	Date		^
Primary Network Guest Network		2.4 GHz	Ch. 11	N/A	N/A		
IoT Network		2.4 GHz	Ch. 1	N/A	N/A		
Wi-Fi Protected Setup		2.4 GHz	Ch. 11	N/A	N/A		
Channel Settings		2.4 GHz	Ch. 6	N/A	N/A		
Devices Parental Controls	ŏ	2.4 GHz	Ch. 11	N/A	N/A		
Status	Ĵ	5 GHz 1	Ch. 132	N/A	N/A		_
Firewall	v	5 GHz 1	Ch. 100	N/A	N/A		

## 04/ CONNECTED DEVICES

**4.0** Overview**4.1** Device Settings

04 / CONNECTED DEVICES

58

You can view the settings of the network devices connected to your Fios Router's network.

## **OVERVIEW**

## 4.0/ OVERVIEW

The **Devices** section allows you to view and manage your Primary/ Guest/IoT network connections and devices. You can view device details, block internet service, and rename devices.

## 4.1/ DEVICE SETTINGS

To view and manage the connected devices on your network:

- 1. From the **Basic** menu, select **Devices** from the left pane.
- 2. The screen displays information about connected devices including **Device Name** and identifiers, **Parental Controls**, the type of network connection, and settings that you can view and configure.
- The Fios Router provides sort function for listing connected devices in a meaningful order. For example, select Sort A to Z from the dropdown list to view the connected device in alphabetical order.

Devices > /	AJI		
Devi	ces		
All (2)	Primary (2)	Guest (0)	Io
Sort A to 2	2	,	, hr
Sort A to	z	````	1
Sort Z to	A		T
Sort Stro	ng to Weak		-
Sort Wea	k to Strong		1
Sort IPv4	0 to 9		1
Sort IPv4	9 to 0		L

- 4. Select **Show All** from the dropdown list to display all devices on your network.
- 5. Select **Expanded List** from the dropdown list to view additional device information for all connected devices.

verizon <sup>,</sup> B	asic Advar	nced			Help @~
Fios Router	~				
Home		All (2) Primary (2) Guest (0) 101	(0)		
Wi-Fi	`	Sort A to Z	Show All	~	Expanded List
Devices	,	Device Name	Parental Controls	Connection	Compact List
Devices	2	2 Online			Expanded List
Parental Controls	c				
Status	,	□         ✓ A0005-H82           □         Device: PO           Connected to: G3100         Max: Address: 48.5b.39.4556.08           IPv4 Address: 192.188.1163	None	C Ethernet	• • •
		✓ E3200-b8f85384e668 Device: Extender Connected to: G300 Ma: Address: b8f65384e668 IPv4 Address: 192/68.100	None	C Ethernet	
		048			(Class Eat)

• **Block/Allow** - Click this option to quickly enable/disable a device from having internet access.

For additional information about blocking websites, refer to Chapter 5 Setting Parental Controls.

6. Click the Settings icon to access the Device Details page for that device:

## **DEVICE SETTINGS**

verizon Basic			
letwork Device	Devices > Device Setting	5	
Fios Router		ettings Reset to Default Settings	
Home	Device 3	Reset to Default Settings	
WI-FI	Device Informati	on	
Devices	Name:	E3200-b8f85384e668 Online	
Devices	2 Location:	Other V	
arental Controls	O Mobility:	Portable V	
tatus	V Device Information:	Edit	_
	Type:	Extender	
	Mac Address:	b8/8.53.84 e6.68	
	Connected to:	G3100	
	IPv4 Address:	192.168.1.100	
	Device Add-Ons		_
	Port Forwarding Rule	Go to Port Forwards	( <u>q.</u> ):
rerizon√ Basic	Port Forwarding Rule		
_	Advanced	Hale	
twork Device	Advanced Devices > Device Setting	s	
Fios Router	Advanced Devices > Device Setting	Hale	
twork Device Fios Router	Advanced Devices > Device Setting	ettings Reset to Defeet Settions Serve	
work Device Flos Router ome	Advanced	ettings Reset to Defeet Settions Serve	
twork Device Flos Router ome /I-FI evices	Advanced Cevetes > Device Setting Device Connection Connection Info	n ettings Reset to Outward Settions Setting on Network Info	
twork Device Flos Router ome fliFl evices Devices	Advanced Cervices > Device Setting Device Connection Connection Info C Connection Info C Connection Cervice Connection Cervice Connection Cervice Connection Cervice C	s ettings Reset to Defend Settings on Network Info Store Math Store Math	
There is the set of th	Advanced	sections Reset to Default Sections Section Sec	
There is the set of th	Advanced	A A A A A A A A A A A A A A	
There is the set of th	Advanced	s ettings Reset to Default Settions e	
There is a constraint of the c	Advanced	s ettings <sub>Bast to Defaul Settions</sub> on Alter Visions ate Default Autores Montion June Vision Default Autores Montion June Vision Default Parties Default Pa	
There is a constraint of the c	Advanced	s ettings estings estings estings esting est	
There is a constraint of the c	Advanced	s extenses e	
etwork Device	Advanced	the state of the second	

#### - Device Information:

- Name, Location, Mobility, and Type Displays the current known information of the device. These can be updated or corrected as needed. Click Edit and Save to apply any changes.
- This section also provides the device MAC Address, Access Point information the device is connected to as well as the IPv4 Address of the device.
- Device Add-Ons

**Port Forwarding** - Port Forwarding allows your network to be exposed to the internet in specific limited and controlled ways. For example, you could allow specific applications, such as gaming, voice, and chat, to access servers in the local network. To access the Port Forwarding page, click **Go to Port Forwarding**.

For additional information, refer to the Port Forwarding section in Chapter 6 Configuring Advanced Settings.

If any Port Forwarding Rules are applied to this device, then the first row of that rule will be displayed here.

Device Connection

This section displays Connection information of how and how well the device is connected to the Access Point. It also displays the Network related information, including IPv6 addresses and a **Ping Test** option.

## 05/ SETTING PARENTAL CONTROLS

- 5.0 Activating Parental Controls
- 5.1 Active Rules

64

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 Fios Router's Parental Controls were designed to allow control of internet access on all locally networked devices.

## **ACTIVATING PARENTAL CONTROLS**

## **5.0/ ACTIVATING PARENTAL CONTROLS**

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

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

verizon Basic	Advanced								<u>Help</u>	8
Network Device	~	Parental Controls > /	и							
	-	Parenta	l Conti	ols					New Rule	
Home WI-FI	~	Home Networ		l protect your devices in ;					Get app	o nov
Devices	~	Start using it today o	n the My Fios ap	p.	our nome or bi	isiness.				
Parental Controlo	1	Rule Template	8							_
Status	Ŷ	Bedtime No Wi-Fi 9pm - 8am		School Day School Sites Only 8am - 3pm		Off Limits Blocked Sites Always on				
			>		>		>			
		Active Rules								_
		Bedtime	All Internet Sun,Mon,Tu 9:00pm - 8	e,Wed,Thu,Fri,Sat	unknown_t	08:18:53:84:e6:69		Enabled	Remove !	Edit

To limit device access:

- 1. From the **Basic** menu, select **Parental Controls** from the left pane.
- 2. To use the default **Rule Templates**, select one of the predefined rules as shown on screen to quickly setup access policy for devices on your network.

3. To create a new access policy, click on the **New Rule** and the configuration page displays.

verizon Basic	Advanced	I.							Help & ~
Network Device		Parental Controls > All							
Fios Router	~	Create Ne	wR	ule					
Home							Required		Change rule name >
WI-FI	×	Name:					nequired		Unande rule name >
Devices	*	Bule Name			(	Done	)		
Parental Controls	0								
Status	ř	Days:					Required		Change days when rule is active >
		Days Sun Mon Tue	Wed	Thu Fri	Sat	G	Done		
		Time:			-		Required		Change time when rule is active >
		Start Time		End Time			$\frown$		
		12:00 am	~	12:00 am		~	Done		
		Condition:					Required		Change rule condition >
		All Internet OFF							
		-							
Network Device	Advanced	Parental Controls > All							Hele 🛞 ~
Fios Router	~	Create Ne	wR	ule					
Home		12:00 am	~	12:00 am		~			
WI-FI	*	Condition:					Required		Change rule condition >
Devices	ř	Condition:							
Parental Controls	0	All Internet OFF							
Status	ř	All Internet ON							
		Devices:					Required		Assign devices to this rule >
		Exceptions (Websites Enter a specific URL such www.example.com	): 1 05						Make exceptions to this rule +
		www.example.com					Optional		
		www.example.com			Enterw	ebsite	Optional	Add	
		www.example.com Exceptions (URL Keys Enter a word that appear	vords):	URL	Enter w	ebsite	Optional	Add	Make exceptions to this rule >
		Exceptions (URL Keys	vords):	URL	Enter w			Add	Make exceptions to this rule 2

## **ACTIVATING PARENTAL CONTROLS**

- 4. Create a rule name.
- 5. Create a schedule by selecting the days of the week when the rule will be active or inactive.
- 6. Set the time when the rule will be active or inactive, then specify the start time and end time.
- 7. Select the **Condition** rule of **All Internet OFF/All Internet ON** to block/allow the access to all internet websites.
- 8. Click **Assign devices to this rule** to select the computers or device where you are limiting access. Click **Apply** to save changes.

Home		Create	Assign devices to this rule	×	Apply changes
WI-FI			A040025-NB2 PC		
Devices		Condition:	unknown_b8:f8:53:84:e6:69 unknown		
Parental Controls	0	O All Interne			
Statuo		All Internet			
		Devices:			
		Exceptions (V Enter a specific www.example.or			
		Exceptions (U Enter a word the	Apply		

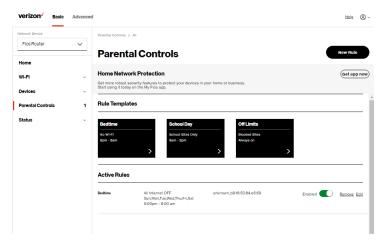
- 9. To remove a device from the list, click **Remove** to the assigned device.
- 10. Click Make exceptions to this rule for the following Exceptions options:
  - Enter the name of the website or keywords within a URL to block/allow the specified websites and websites with names containing the specified keyword.

- 11. To remove a website or keyword, click **Remove** to the word.
- 12. Click Apply changes to save changes.

*NEW!* The *Verizon My Fios* app provides robust security to protect your home and business networks. Click the **Get app now** link to download the My Fios app for using the My Fios app on the iOS or Android OS.

## **5.1/ ACTIVE RULES**

You can view the rules created for your Fios Router shown on the **Parental Controls** page.



# CONFIGURING ADVANCED SETTINGS

- 6.0 Firewall
- 6.1 Utilities
- 6.2 Network Settings
- 6.3 Date & Time
- 6.4 DNS Settings
- 6.5 Monitoring
- 6.6 System Settings

70

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

Fios Router's security suite includes comprehensive and robust security services, such as stateful packet inspection, firewall security, user authentication protocols, and password protection mechanisms.

These and other features help protect your computers from security threats on the internet.

#### This chapter covers the following advanced features:

Firewall - select the security level for the firewall.

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

#### Utilities

- Diagnostics performs diagnostic tests.
- Save and Restore resets your Fios Router to its default settings.
- Reboot Router restarts your Fios Router.
- MAC Cloning clones the MAC address.
- ARP Table displays active devices with their IP and MAC addresses.

- NDP (Neighbor Discovery Protocol) Table displays active devices with their IPv6 and MAC addresses of DHCP connection.
- Users creates and manages remote users.
- Remote Administration enable remote configuration of your Fios Router from any internet-accessible computer.
- LED Brightness controls the Router Status LED light to either dim or brighten.

#### **Network Settings**

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

### FIREWALL

#### Date & Time

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

**DNS Settings** - manages the DNS server host name and IP address.

Monitoring - displays the details and status of:

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

**System Settings** - sets up various system and management parameters.

### 6.0/ FIREWALL

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

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

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

The firewall regulates the flow of data between the local network and the internet. Both incoming and outgoing data are inspected, then either accepted and allowed to pass through your Fios Router or rejected and barred from passing through your Fios Router, according to a flexible and configurable set of rules. These rules are designed to prevent unwanted intrusions from the outside, while allowing local network users access to internet services.

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

Each request for a service that the firewall receives is checked against the firewall rules to determine whether the request should be allowed to pass through the firewall. If the request is permitted to pass, all subsequent data associated with this request or session is also allowed to pass, regardless of its direction.

For example, when accessing a website on the internet, a request is sent to the internet for this site. When the request reaches your Fios Router, the firewall identifies the request type and origin, such as HTTP and a specific computer in the local network. Unless your Fios Router is configured to block requests of this type from this computer, the firewall allows this type of request to pass to the internet.

# FIREWALL

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

### 6.0a/ SETTING FIREWALL CONFIGURATION

You can select a normal, high, or low security level to limit, block, or permit all traffic. The following table shows request access for each security level.

Security Level	Internet Requests Incoming Traffic	Local Network Requests Outgoing Traffic
High	Blocked	Limited
Normal	Blocked	Unrestricted
Low	Unrestricted	Unrestricted

The request access is defined as:

- Blocked traffic no access allowed, except as configured in Port Forwarding and Remote Access
- Limited permits only commonly used services, such as email and web browsing
- Unrestricted permits full access of incoming traffic from the internet and allows all outgoing traffic, except as configured in Access Control

#### 6.0b/ SPECIFYING GENERAL SETTINGS FOR IPV4 OR IPV6

To set your firewall configuration:

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

verizon Basic	Advanced	1	Help & ~
Network Device		Firewall > General	
Fios Router	$\sim$	0	
Home	*	General	Apply Changes
WI-FI	~	IPv4 Settings	
Devices	×	Normal Security     Remote administration will overide the security	
Parental Controls	o	inbound policy	
Status	~	High Security Remote administration will overide the security	Set Top Box traffic disabled
Firewall	^	inbound policy	
General	- 1	Low Security     Remote administration will overide the security     inbound policy	
Access Control	- 1	magana pana)	
Port Forwarding	- 1	IPv6 Settings	
Port Triggering	- 1	Normal Security     Remote administration will overide the security	
DMZ Host		inbound policy	
Static NAT		High Security     Remote administration will overide the security     inbound policy	
IPv6 Pinholes		incound policy	
Utilities	×	Low Security     Remote administration will overide the security     inbound policy	
Network Settings	× .	полито рольу	

- Select a security level by clicking one of the radio buttons. Using the Low Security setting may expose the local network to significant security risks, and should only be used for short periods of time to allow temporary network access.
- 3. Click Apply Changes to save changes.

### **FIREWALL**

### 6.0c/ Access Control

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

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

### **ALLOW OR RESTRICT SERVICES**

To allow or restrict services:

1. From the Advanced menu, select Firewall from the left pane and then click 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.

verizon Basic	Advanced	I				Help 🔕 -
Network Device		Firewall > Access Control				
Fios Router	~	Access Cor	ntrol		(	
Home						
WI-FI	~	Block access to the Internet	services from within the Home Network (	(LAN).		
Devices	~	Create Rule				
Parental Controls	0	Networked Device	Network Address	Protocols	Status	Action
Status	~		Y	fou have no rules.		
Firewall	^					
General	- 1	(bba)				
Access Control	- 1					

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

verizon Basic	Advanced			<u>Help</u>	® -
Network Device		Firewall > Access Control > Create rule			
Fios Router	~				
Home	<b>^</b>	Access Control			
WI-FI	v	Block access to the Internet services fro	om within the Home Network (LAN).		
Devices	×	Add Access Control			
Parental Controls	0	Networked Device	Any V		
Statue	~		Anne V		
Firewall	~	Protocol	Any v		
General	- 1	When should rule occur?	Ahvays		
Access Control	- 1		Always		
Port Forwarding	- 1	Cancel Ap	User Defined		

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

# FIREWALL

verizon Basic	Advanced											Help	8
Network Device		Firewall > Access Control	> Create rule										
Fios Router	~												
Home	<b>^</b>	Access Co	ontrol										
WI-FI	~	Block access to the Intern	et services from within	the Hor	e Netwo	rk (LAN).							
Devices	~	Set Rule Schedule	,										-
Parental Controls	o	Rule name:									 		_
Status	~												
Firewall	~	Rule days:	Sun	Mon	Tue	Wed	Thu	Fri	Sat				
General	- 1	Rule time:	Start Tim 9:00 pr			v	End Tim 12:00			~			
Access Control	- 1		Bule	will be a	active du	ring sohe	duled tim	•					
Port Forwarding			-										
Port Triggering			() Rule	will be i	nactive	luring so	heduled ti	me					
DMZ Host		Cancel	Apply										
Static NAT		Cunter	Abbiy										

- 6. Enter the rule name, specify days of the week, and set the start time and end time when the rule will be active or inactive.
- 7. Click **Apply** to save changes.
- 8. 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.

#### 6.0d/ 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 **Advanced** menu, select **Firewall** from the left pane and then click **Port Forwarding**. The **Port Forwarding** page opens with the current rules displayed.

etwork Device		Firewall > Port Fo	ovarding					
Fios Router	~	Theman y Fortre	a mananing					
ome	A	Port Fo	orwardin	g				Apply Changes
/I-FI	~	Open a tunnel be	tween remote compute	ers and a device port of	on your Home Network (	LAN). Supports gami	ng, IoT, home security	devices and more.
Devices	~	Create Rule						
Parental Controls	0	Application	Original Port	Protocol	Fwrd to Address	Fwrd to Port	Schedule	
tatus	~	test	1234	TCP 🗸	127.0.0.2	5678	Alwa 🗸	Add to list
irewall	^	Rules List						- \
General	- 1	Rules List						
Access Control	- 1	Application	Original Port	Protocol	Fwrd to Address	Fwrd to Port	Schedule	Enable
			4567	TCP	127.0.0.1	4567	Always	
			4577	TCP	127.0.0.1	4577	Always	
Port Forwarding								

# FIREWALL

- 2. To create a new rule, enter the application name, configure its inbound and outbound port numbers, then select the protocol.
- 3. To schedule the rule, select either **Always** or **User Defined** in the **Schedule** list box.
- 4. Click Add to list. The rule displays in the Rules List section.
- 5. Click Apply Changes to save changes.

#### 6.0e/ Port Triggering

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

For example, a gaming server is accessed using UDP protocol on port 2222. The gaming server then responds by connecting the user using UDP on port 3333, when a gaming session is initiated.

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

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

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

To configure port triggering:

1. From the Advanced menu, select Firewall and then click Port Triggering.

verizon Basic	Advanced						Hele 🛞 -
Network Device	×	Firewall > Port Trigge	ering				
	^	Port Trig	ggering				Apply Changes
Home		Onen a lunnel heliur	en remote computers and a	fouries part on your Home I	Network (LAN) Supports an	ning laT home convilu	devices and more
WI-FI	~	open a turner betwe	en remote compaters and a	serve port on your nome	retwork (carb, supports ga	ning, ior, nome secondy	serves and more.
Devices	~	Create Rule					
Parental Controls	0	Application	Triggered Port Range	Protocol	Forwarded Port Range	Schedule	
Status	•	test	Start End 1234 5678	TOP 🗸	Start End 2345 6789	Always 🗸	Add to list
Firewall	^						
General	- 1	Rules List					
Access Control	- 1	Application	Triggered Port Range	Protocol	Forwarded Port Range	Schedule	Enable
Port Forwarding	- 1	test	Start End 1234 5678	TCP	Start End 2345 6789	Always	🗸 / 🖻
Port Triggering							
DMZ Host							

- 2. To add a service as an active protocol, enter the application name, configure its inbound and outbound (triggered/ forwarded) port range, then select the protocol.
- 3. To schedule the rule, select either **Always** or **User Defined** in the **Schedule** list box.
- 4. Click Add to list. The rule displays in the Rules List section.
- 5. Click Apply Changes to save changes.

### **FIREWALL**

### 6.0f/ DMZ Host

DMZ Host allows a single device on your primary network to be fully exposed to the internet for special purposes like internet gaming.

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

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

- 1. From the Advanced menu, select Firewall and then click DMZ Host.
- 2. Select Enable for the DMZ Host.
- 3. Enter the IP address or select the MAC address of the device you want to designate as the DMZ Host.
- 4. Click **Apply Changes** to save changes.

verizon Basic	Advanced			Hela 🕲 -
Network Device		Firewall > DMZ Host		
Flos Router	~	DMZ Host		
Home		DINETIOS		
WI-FI	~	How It works Allow a single computer or device to be fully expos	ed to the	
Devices	~	Internet.		
Parental Controls	0	DMZ IPv4 Host	Disabled	
Status	~	IPv4 Address	192 168 1 0	
Firewall	^			
General		DMZ IPv6 Host	Disabled	
Access Control		Select Host	Menu ~	
Port Forwarding				
Port Triggering		MAC Address		
DMZ Host				

### 6.0g/ Static NAT

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

To configure static NAT:

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

	verizon	Basic	Advanced			Help (8)	v
	Network Device		~	Firewall > Static NAT			
	Home		-	Trigger opening of ports for incoming data.			
	WI-FI Devices		v v	Create Rule			-
	Parental Contr	ols	0	Local Host	Public IP Address	Port Fwd	1
	Status		×	Select	0 0 0 0	Add to lis	4
	Firewall General		^	192.168.1.151 - NB1			_
	Access Contro	ы		192.168.1.100 - E3200-b8/85384e668	Public IP Address	Port Fwd	
	Port Forwardin	ig .	- 1				
	Port Triggering						
	DMZ Host						
I	Static NAT				Copyright © 2021 Verizon		
	IPv6 Pinholes						

- 2. To create a static NAT, select a source address in the Local Host field.
- 3. Enter the Public IP Address.
- 4. If using port forwarding, select the **Port Fwd** check box.
- 5. Click Add to list. The rule displays in the Rules List section.

# **FIREWALL**

- 6. Click Apply Changes to save changes.
- 7. Repeat these steps to add additional static IP addresses.

#### 6.0h/ IPv6 Pinholes

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

To configure the rules:

1. From the Advanced menu, select Firewall and then click IPv6 Pinhole.

× +			FTP (File Transfer)
secure   192.168.1.1/#	/adv/firew	all/pinholes	HTTP (Web Server)
verizon Basic	Advanced		HTTPS (Secured Web Server)
Network Device	~	Firewall > IPv6 Pinholes	IMAP (Messaging Server) L2TP (Layer Two Tunneling Protocol)
		IPv6 Pinholes	POP3 (Incoming Mail)
Home WI-FI	•	How It worke	SMTP (Outgoing Mail)
Devices	÷	Open a tunnel between remote computers and a device port on your gaming, IoT, home security devices and more.	Home Netw SNMP (Simple Network Management Protocol) Telnet (Remote Connection)
Parental Controls	0	Create Rule	TFTP (Trivial File Transfer Protocol)
Status	~	External Host Internal Host Protocol	Traceroute (Route Tracking Utility)
Firewall	^	Select external host V Select Internal host V TCP	Select applicatio     Always     Add to list
General	- 1	Rules List	νβ 
Access Control	- 1	External Host Internal Host Protocol	Application/Port Schedule
Port Forwarding	- 1		
Port Triggering			
DMZ Host			
Static NAT			
IPv6 Pinholes		Cop	yright © 2021 Verizon
Utilities	~		

2. Select external and internal host, protocol and the application port type.

- 3. To schedule the rule, select either **Always** or **User Defined** in the **Schedule** list box.
- 4. Click Add to list. The screen displays opened pinhole port and its status. It shows the IP addresses of remote device and connected device on your network.
- 5. Click **Apply Changes** to save changes.

### 6.1/ UTILITIES

You can access the following advanced settings:

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

# UTILITIES

### 6.1i/ DIAGNOSTICS

You can use diagnostics to test network connectivity.

To diagnose network connectivity:

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

verizon Basic	Advanc	Hele	8~
Network Device		Utilities > Diagnostics	
Fios Router	~	<b>_</b>	
Devices	~	Diagnostics	
Parental Controls	0	How It works	Î
Status	v	Diagnolics can assist In testing network connectivity. This keature 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.	
Firewall	×	IPv4 Ping (ICMP Echo)	
Utilities	^	Destination Qo	5
Diagnostics			-1
Save & Restore		Number of pings 4	
Reboot Router		Status	
MAC Cloning			
ARP Table		IPv6 Ping (ICMP Echo)	-1
NDP Table		Destination	
Users		Number of pings 4	
Remote Administratio	n		
LED Brightness		Status	-

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

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

### 6.1j/ SAVE AND RESTORE

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

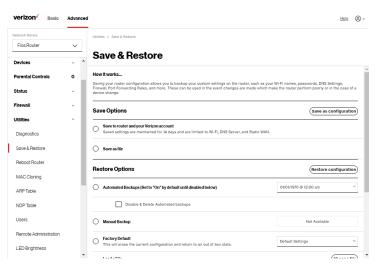
Only configuration files saved on a specific Fios Router can be applied to that Fios Router. You cannot transfer configuration files between Fios Routers.

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

### **Save Options**

To save the configuration file:

1. Select Save & Restore in the Utilities section.



# UTILITIES

- 2. Select Save to router and your Verizon account or Save as file to save the current configuration, then click Save as configuration.
- 3. If you select **Save as file**, the configuration file is saved to you web browser's download folder.

#### **Restore Options**

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

Prior to restoring the factory defaults, you may want to save your current configuration to a file. This allows you to reapply your current settings and parameters to the default settings, as needed.

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

To backup your Fios Router's settings:

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

To restore your Fios Router's factory default settings:

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

verizon	Basic Advan	ed	Help 🛞 -
Network Device		Utilities > Save & Restore	
Fios Router	~	Save & Bestore	
Devices	×		
Parental Controls	• •	Restore Options	Restore configuration
Status	×	Automated Backups (Set to "On" by default until disabled below)	01/01/1970 @ 12:00 am
Firewall	×	Disable & Delete Automated backups	
Utilities	^	Manual Backup	Not Available
Diagnostics			
Save & Restore		Factory Default     This will erase the current configuration and return to an out of box state.	Default Settings V
Reboot Router		LoadaFile Browse to locate file, then press Apply to begin the configuration file uploading process.	Choose file)
MAC Cloning		Restore From Account	
ARP Table		<ul> <li>To complete this action, use the My Fios App or My Verizon account to view your recently saved se and restore them to the router.</li> </ul>	ettings Go to Apple App Store Go to Google Play Store
NDR Table			

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

#### To load the configuration file:

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

# UTILITIES

- 3. Browse to the location of the file, and click **Restore configuration** button to begin the configuration uploading process.
- Accessing the My Fios app or the My Verizon account also allows you to restore the previously saved settings. Click Restore From Account and select Go to Apple App Store/ Go to Google Play Store to restore the saved settings to the router.
- 5. Click **Restore configuration** button. Your Fios Router will automatically restart with that configuration.

### 6.1k/ REBOOT FIOS ROUTER

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

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

To reboot your Fios Router using the user interface:

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

verizon	Basic	Advan	ced	Helt @ ~
Network Device				Utilities > Reboot Router
Fios Router		~		Reboot Device
Devices		~	^	Reboot Device
Parental Contro	ole	0		
Status		~	l	
Firewall		~	l	
Utilities		^	l	Copyright © 2021 Verizon
Diagnostics			l	
Save & Restore	9		l	
Reboot Router				

- 2. To reboot, click **Reboot Device**. Your router will reboot. This may take up to a minute.
- 3. To access your Fios Router user interface, refresh your web browser.
- 4. After the Router Status LED on the front panel turns solid white, you will automatically be sent to the web browser login page.

### 6.11/ MAC CLONING

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

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

To copy the MAC address of the existing device:

1. Select MAC Cloning in the Utilities section.

verizon	Basic	Advanced			Help	<u>®</u> ~
Network Device			Utilities > MAC Cloning			
Fios Router		~	MAC Clamina			
Devices		~ <b>^</b>	MAC Cloning			
Parental Contr	olo	0	How It works			
Status		~	MAC Address Cloning provides the ability to emul	ate the routers MAC address to appear identical to the original hardware address.		
Firewall			Set MAC of Device	Broadband Connection (Ethernet)	Apj	
Utilities			To physical address	78 : DD : 12 : C9 : 9D : A3		
Diagnostics		- 1		Restore factory MAC address		
Save & Restore		- 1				
Reboot Router		- 1				
		- 1				
MAC Cloning		- 5		Convrint © 2021 Verizon		

# UTILITIES

- 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.

#### 6.1m/ ARP TABLE

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

*To view the IPv4 and MAC addresses for each device: s*elect **ARP Table** in the **Utilities** section.

verizon Basic	Advance	d			Helo (8)
Network Device		Utilities > ARP Table			
Fios Router	~				
Devices	v *	ARP Tab	ble		Refresh
Parental Controls	0	The ARP Table below	v displays the IPv4 and MAC add	iress of each DHCP connection	
Status		IPv4 Address	MAC Address	State	Device
		192.168.1.254		FAILED	Network (Home/Office)
Firewall	ř	169.254.145.215	-	FAILED	Network (Home/Office)
Utilities	^	192.168.1.151	48.5b:39:4f:56:08	REACHABLE	Network (Home/Office)
Diagnostics	- 1	192.168.1.100	b8:f8:53:84:e6:68	REACHABLE	Network (Home/Office)
Save & Restore	- 1				
Reboot Router	- 1				
MAC Cloning	- 1				
ARP Table	- 1			Copyright © 2021 Verizor	n
NDP Table					

### 6.1n/ NDP TABLE

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

*To view the IPv6 and MAC addresses for each device:* select **NDP** (Neighbor Discovery Protocol ) **Table** in the **Utilities** section.

letwork Device		Utilities > NDP Table					
Fios Router	$\sim$					-	Refresh
Devices	v *	NDP Table					terresn
Parental Controls	0	The NDP Table below displays the IP	v6 and MAC address of each DHCP o	onnection			
Status		IPv6 Address	MAC Address	State	Rtr	Device	
Firewall	,	fe80::1116.b296.bd9-91d7	48.5b:39.41.56.08	REACHABLE	No	Network (Home/Office)	
Jtilities	^						
Diagnostics	- 1						
Save & Restore	- 1						
Reboot Router	- 1		Copyright	© 2021 Verizon			
MAC Cloning	- 1						
ARP Table	- 1						
NDP Table							
Users							

### 6.10/USERS

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

## UTILITIES

#### To view users:

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

verizon <sup>4</sup> Basic	Advanced				Help @
Network Device		Utilities > Users			
Fios Router	~				
Devices	v *	Users			
Parental Controls	0	The User page provides th	e ability to edit device administrator s	ettings.	
Status	×	Login Configuration		Maximum Unsuccessful Login Attempts:	10 ~
Firewall	×	Full Name	Username	Permissions	Action
Jtilities	^	Administrator	Admin	Administrator	Ed is
Diagnostics					du
Save & Restore					
Reboot Router					
MAC Cloning					
ARP Table	- 1		c	opyright © 2021 Verizon	
NDP Table					
Users					
Remote Administration					

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

verizon Basi	c Advanced				Help & ~
Network Device		Utilities > Users > Edit User Settings			
Fios Router	~	Edit User Setti	ngs		Apply Changes
Devices	× *				
Parental Controls	۰ _	Full name	Administrator		
Status	v	User name	Admin		
Firewall	v	Permissions	Administrator		
Utilities	^	Set new password		minimum 8 characters	
Diagnostics					
Save & Restore	- 1	Retype new password			
Report Poutor					

- 4. Edit the Full name, Username and set a new password.
- 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. Verify the level of access for the user in the **Permissions** field.
- 7. Click **Apply changes** to save changes. The **Users** page opens with the user information displayed.

### 6.1p/ REMOTE ADMINISTRATION

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

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

You can allow incoming access to the following:

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

# UTILITIES

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

To enable remote administration:

1. Select Remote Administration.

verizon Basic	Adva	inced		Help (8)
Network Device			Utilities > Remote Administration	
Fios Router	~	-	Remote Administration	
Devices	~	^		
Parental Controls	0	J.	Configure Remote Administration to the router	
Status	~	L	Attention With Remote Administration enabled, your local network will be at risk from outside attacks	
Firewall	~	I	Allow Incoming WAN Access to Web-Management	(System Settings)
Utilities	^	I	Using Primary HTTPS Port (443)	
Diagnostics				
Save & Restore		L	Diagnostic Tools	
Reboot Router		I	Allow Incoming WAN ICMP Echo Requests (e.g. pings and ICMP traceroute queries)	
MAC Cloning		l	Allow Incoming WAN UDP Traceroute Queries	
ARP Table				
NDP Table				
Users				
Remote Administration				
LED Brightness		•	Copyright © 2021 Verizon	

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

#### 6.1q/ LED BRIGHTNESS

The Fios Router allows yout to set the LED brightness to turn Off(0%) or stay bright (50% or 100%) using the user interface.

### To control the LED brightness:

1. Select LED Brightness in the Utilities section.

verizon Basic Advanced	Helle 🕲 v
Network Device	URilities > LEO Brightness
Fios Router 🗸	
Save & Hestore	LED Brightness Apply Changes
Reboot Router	Set the LED brightness to turn Off or stay bright when everything is normal. The light will activate again on status changes like VMS pairing or loss of connection.
MAC Cloning	LED Brightness
ARP Table	0% 50% 100%
NDP Table	
Users	
Remote Administration	
LED Brightness	Copyright © 2021 Verizon
Network Settings 🗸 🗸	

- 2. Slide the bar to adjust the brightness of the LED.
- 3. Click Apply changes to save changes.

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

### 6.2/ NETWORK SETTINGS

You can configure the following network settings:

- Network Objects defines a group, such as a group of computers.
- Network Connections displays and manages manages the details of a specific network connection.
- Universal Plug and Play (UPnP) checks the validity of all UPnP services and rules.

# **NETWORK SETTINGS**

- Port Forwarding Rules displays port forwarding rules.
- IPv6 enables IPv6 support.
- Routing manages the routing and IP address distribution rules.
- IPv4/IPv6 Address Distribution adds computers configured as DHCP clients to the network.
- **Port Configuration** sets up the Ethernet ports as either full- or half-duplex ports, at either 10 Mbps, 100 Mbps, or 1000 Mbps.

### 6.2a/ NETWORK OBJECTS

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

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

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

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

verizon Basic	Advanced	Hele 🛞 ~
Fios Router	~	Network Objects Apply Changes
Home WI-FI	Â	Network Objects         Apply Changes           Alletorio Object is a set of host names, P addresses, or MAC addresses. Security rules can be applied to a distinct LAH subnet using Network Objects.         Security rules can be applied to a distinct LAH subnet using Network Objects.
Devices	÷	Netwick Object Items Add Inew
Parental Controls Status	o U	
Firewall	÷	
Utilities Network Settings	~	Copyright © 2021 Verizon
Network Objects		

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

verizon Basic	Advanced		Help	8~
Network Device		Network Settings > Network Objects > Edit Network Objects		
Fios Router	~	Edit Network Objects		
Home	<b>^</b>			
WI-FI	~	Edit Network Objects		
Devices	×	Description Global Object		
Parental Controls	o	Item Action		
Status	v	bba .		
Firewall	×	Cancel Apply Changes		
Utilities	×			
Network Settings	^			
Network Objects				
Network Connections				
		C		

# **NETWORK SETTINGS**

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

verizon Basic	Advanced			Help	<u>®</u> ~
Network Device		Network Settings > Network Objects > E	Edit Network Objects		
Fios Router	~	Edit Network O	bjects		
Home	Î.		-		
WI-FI	~	Edit Items			
Devices	~	Network Object Type	IP Address		
Parental Controls	0	IP Address	IP Address		
Status	~		IP Subnet		
Firewall	v	Cancel	MAC Address		
Utilities	~		Host Name		
Network Settings	~		DHCP Option		
Network Objects	- 1				
Network Connections			Copyright © 2021 Verizon		

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

### 6.2b/ NETWORK CONNECTIONS

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

To view the network connections:

1. From the Advanced menu, select Network Settings from the left pane and then click Network Connections.

verizon√ Basic	Advan	loed			Help & ~
Network Device		Network Settings > Network Connections			
Fios Router	$\sim$				
Home		Network Connectio	ons		
WI-FI	~	Network name	Status		
Devices	~	Network (Home/Office)	Connected	Edit	
Parental Controls	0	5 GHz 1 Wi-Fi Access Point	Disconnected	Edit	
		5 GHz 2 Wi-Fi Access Point	Disconnected	Edit	
Status	×	2.4 GHz Wi-Fi Access Point	Disconnected	Edit	
Firewall	×	Ethernet	Connected	Edit	
Utilities	v	Coax	Cable Disconnected	Edit	
Network Settings	^	Broadband Connection (Ethernet/Coax)	Disconnected	Edit	
Network Objects		Full Status			
Network Connections					
Universal Plug & Play					

2. To view and edit the details of a specific network connection, click the hyperlinked name or the action icon. The following sections detail the types of network connections that you can view.

### **NETWORK (HOME/OFFICE) CONNECTION**

You can view the properties of your local network. This connection is used to combine several network interfaces under one virtual network. For example, you can create a home/office network connection for Ethernet and other network devices.

# **NETWORK SETTINGS**

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

To view the connection:

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

verizon <sup>4</sup> Basic	Advance	d		Helo 🛞
letwork Device		Network Settings > Network Co	nections > Network (Home/Office)	
Fios Router	~	Notwork (H	ome/Office)	tings Save
Home	-	Network (H		
WI-FI	~	Important: Only advanced tech	nical users should use this feature.	
Devices	~	Name:	Network (Home/Office)	
Parental Controls	0	Status:	Connected	
Status	×	Network:	Network (Home/Office)	
Firewall Jtilities	č	Underlying Device:	5.0Hz 1 Wi-Fi Access Point 5.6Hz 2 Wi-Fi Access Point 2.4 6Hz Wi-Fi Access Point	
Network Settings	^		Ethernet Coax	
Network Objects	. 1	Connection Type:	Bridge	
Network Connections		MAC Address:	78:DD:12:C9:9D:A4	
Universal Plug & Play Port Forwarding Rules		IPv4 Address:	192.168.11	
IPv6		Subnet Mask:	255.255.255.0	
Routing		IP Address Distribution:	DHCP Server	
IPv4 Address Distribution k/networkconnections/net		ngs wo LAN Prefix:	0	

#### 06 / CONFIGURING ADVANCED SETTINGS



verizon Basic	Advanced				<u>Help</u>	® -
Network Device Fios Router	~	Network Settings > Network Connection		Settings		
Home	-					
WI-FI	•	Subnet Mask:	255,255,255.0			
Devices	×	IP Address Distribution:	DHCP Server			
Parental Controls Status	o v	Ipv6 LAN Prefix:	0			
Firewall	~	lpv6 Address:				
Utilities	~	Link Local Address:	0			1
Network Settings	^	IPv6 Address Distribution:	Stateless			1
Network Objects	- 1	Received Packets:	73095			
Network Connections		Sent Packets:	21417			
Port Forwarding Rules		Time Span:	1:35:14			

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

#### **CONFIGURING THE HOME/OFFICE NETWORK**

To configure the network connection:

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

# **NETWORK SETTINGS**

verizon Basic	Advanced							Help & ~
Network Device		Network Settings > Network Connections	s > Network (Ho	ne/Office)				
Fios Router	~	Network (Home	o/Offi	<b>(</b>				Changes
Home		Network (Holling	e/Onic	,e)			Save	Changes
WI-FI	~	Important: Only advanced technical use	ers should use t	is feature.				
Devices	~	General						
Parental Controls	0	Status:		Co	nnected			
Status	~	Connection Type:		Ne	work (H	lome/Office)		_
Firewall	~	Physical Address:		78:	DD:12-C	9.9D.A4		- 1
Utilities	~							- 1
Network Settings	^	MTU:	Automatio	~		1500		
Network Objects	- 1	Internet Protocol:	Use the Follow	in ~				
Network Connections		IP Address:	192 168	1	1			
Universal Plug & Play		Subnet Mask:	255 255	255	0			
Port Forwarding Rules		Bridge						- 1
IPv6								_
Routing		Name		٧L	AN	Status		
IPv4 Address Distribution		Broadband Connection (Etherne	at/Coax)	Dis	able	Disconnected	Edit	
	*	5 GHz 1 WILEI Accose Point		Die	oblo	Disconnected	Edit	*

verizon <sup>,/</sup> Bas	alo Advanceo	1				н	lele 🛞 -
Network Device		Network Settings > Network Connection	ins > Network (Home/Office	2)			
Fios Router	~	Network (Hom				Save C	
Home	*	-	le/Onice)			Save C	hanges
WI-FI	~	Bridge					
Devices		Name		VLAN	Status		
Parental Controls	0	Broadband Connection (Ether	net/Coax)	Disable	Disconnected	Edit	
Status	÷	5 GHz 1 Wi-Fi Access Point		Disable	Disconnected	Edit	
		5 GHz 2 WI-FI Access Point		Disable	Disconnected	Edit	
Firewall	×	2.4 GHz WI-FI Access Point		Disable	Disconnected	Edit	- 1
Utilities	~	Ethernet		Disable	Connected	Edit	- 1
Network Settings	^	Coax		Disable	Disabled	Edit	- 1
Network Objects		IP Address Distribution:	DHCP Server				
Network Connection	ns	Start IP Address:	192 168 1	2			
Universal Plug & Play	y	End IP Address:	192 168 1	25	1		
Port Forwarding Rul	es	WINS Server:	0 0 0	0			
IPv6							
Routing		Lease time in minutes:	1440				
IPv4 Address Distrib	oution	IP Address Distribution According to	DHCP Option 60 (Vendor 0	Class Identifi	er)		

#### 06 / CONFIGURING ADVANCED SETTINGS



etwork Device		Network Settings > Network Connecti	ons > Network (Home/Office)				
Fios Router	$\sim$						
lome	^	Network (Hon	ne/Oπice)				Save Changes
WI-FI	~	End IP Address:	192 168 1 2	34			
Devices	~	WINS Server:	0 0 0 0				
Parental Controls	0	Lease time in minutes:	1440				
Status	~	IP Address Distribution According to	DHCP Option 60 (Vendor Class Identi	Gar)			
Firewall	~						
Jtilities		Vendor Class ID	IP Address	MAC Address		QoS	
Network Settings	~	MSFT 5.0	192.168.1.153	48:58:39:4F:56:08			
-	- 1	Verizon BHRx1 DHCP Detect	192.168.1.100	B8.F8:53.84.E6.68			
Network Objects	- 1	Routing Table					
Network Connections		Name Destination	on Gateway	Netmask	Metric	Status	Action
Universal Plug & Play							

2. Configure the following sections, as needed.

### General

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

- Status displays the connection status of the network.
- **Connection Type** displays the type of connection interface.
- **Physical Address** displays the physical address of the network card used for the network.
- **MTU** displays the Maximum Transmission Unit (MTU) indicating the largest packet size permitted for internet transmissions:
  - **Automatic**: sets the MTU (Maximum Transmission Unit) at 1500.

# **NETWORK SETTINGS**

- Automatic by DHCP: sets the MTU according to the DHCP connection.
- Manual: allows you to manually set the MTU.
- Internet Protocol

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

- No IPv4 Address: the connection has no IP address. This is useful if the connection operates under a bridge.
- Obtain an IPv4 Address Automatically: the network connection is required by Verizon to obtain an IP address automatically. The server assigning the IP address also assigns a subnet mask address, which can be overridden by entering another subnet mask address.
- Use the Following IP Address: the network connection uses a permanent or static IP address and Subnet Mask address, provided by Verizon or experienced network technician.

#### Bridge

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

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

Verify the following information:

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

#### **IP Address Distribution**

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

Once enabled and configured, the DHCP server automatically assigns IP addresses to any network devices which are set to obtain their IP address dynamically.

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

*To set up the Fios Router's network bridge to function as a DHCP server:* 

- In the IP Address Distribution section, select the DHCP server. Once enabled, the DHCP server provides automatic IP assignments (also referred to as IP leases) based on the preset IP range defined below.
  - Start IP Address Enter the first IP address in the IP range that the Fios Router will automatically begin

assigning IP addresses from. Since your Fios Router's IP address is 192.168.1.1, the default Start IP Address is 192.168.1.2.

- End IP Address Enter the last IP address in the IP range that the Fios Router will automatically stop the IP address allocation at. The maximum end IP address range that can be entered is 192.168.1.254.
- 2. If Windows Internet Naming Service (WINS) is being used, enter the **WINS Server** address.
- 3. In the Lease Time in Minutes field, enter the amount of time a network device is allowed to connect to the Fios Router with its currently issued dynamic IP address.

# **IP Address Distribution According to DHCP option 60 (vendor class Identifier)**

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

Click Save Changes to save changes.

### **Routing Table**

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

• **Static routing** – specifies a fixed routing path to neighboring destinations based on predetermined metrics.

• **Dynamic routing** – automatically adjusts how packets travel on the network. The path determination is based on network/device reachability and the status of the network being traveled.

To configure routing:

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

verizon Basic	Advanced	1	Hele	8~
Network Device		Network Settings > Network	Connections > Network (Home/Office) > Route Settings	
Fios Router	$\sim$	D		
Home		Route Sett	ings	
WI-FI	~	Routing Entry:	IPv4 ~	
Devices	~	Name:	Hetwork (Home/Office)	
Parental Controls	0	Destination:	0 0 0 0	
Status	~	Netmask:	0 0 0 0	
Firewall	~	Gateway:		
Utilities	~			
Network Settings	^	Metric:	0	
Network Objects		Apply		
Network Connections				
Universal Plug & Play				

2. To save your changes click Apply.

### **Wi-Fi Access Point Connection**

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

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

To view the connection settings:

- 1. From the Advanced menu, select Network Settings from the left pane and then click Network Connections.
- On the Network Connections page, click the Network (Home/Offiffice) connection link. The Network (Home/ Offiffice) Properties page displays.
- To access the 5 GHz 1 Wi-Fi Access Point, 5 GHz 2 Wi-Fi Access Point or 2.4 GHz Wi-Fi Access Point Enable Settings page, click the 5 GHz 1 Wi-Fi Access Point, 5 GHz 2 Wi-Fi Access Point or 2.4 GHz Wi-Fi Access Point link listed under the Underlying Device section.

letwork Device		Network Settings > Network Conne	ections > 5 GHz 1 Wi-Fi Access Point	
Fios Router	$\sim$			
Home	A		Access Point	
WI-FI	~	Enable Settings.		Enabled
Devices	~	Important: Only advanced technic	al users should use this feature.	
Parental Controls	o	Name:	5 GHz 1 Wi-Fi Access Point	
Status	~	Status:	Disconnected	
Firewall	~	Network:	Network (Home/Office)	
Utilities	×	Connection Type:	5.0 GHz 1 Wi-Fi Access Point	
Network Settings	Ŷ	MAC Address:	78.DD:12.C9:9D:A6	
Network Connections		IP Address Distribution:	Disable	
Universal Plug & Play		Received Packets:	0	
Port Forwarding Rules		Sent Packets:	559	
IPv6		Time Span:	0.03.58	
Routing				

4. To enable or disable the connection, move the selector to **on** or **off**.

- 5. To rename the connection, enter a name in the **Name** field.
- 6. Click Apply to save the changes.
- 7. Reboot your Fios Router.

### **CONFIGURING Wi-Fi ACCESS POINT PROPERTIES**

To configure the connection:

1. On the bottom of the Access Points specific **Enable Settings** page, click **Settings**. The configuration page displays.

verizon	Baelc	Advanced			Help	8~
Network Device			Network Settings > Network C	onnections > 5 GHz 1 Wi-Fi Access Point		
Fios Router		~	5 CH- 1W	Fi Access Point		
Home			5 GH2 I WI-	FI Access Point		
WI-FI		~	General			
Devices		•	Important: Only advanced teo	chnical users should use this feature.		
Parental Controls	•	0	Status:	Disconnected		
Status		•	Network:	Network (Home/Office)		
Firewall		×				
Utilities		•	Connection Type:	5.0 GHz 1 Wi-Fi Access Point		
Network Settings	5	~	Physical Address:	78:DD:12:C9:9D:A6		
Network Objects			MTU:	Automatic ~ 1500		
Network Connec	tions					
Universal Plug & F	Play		Apply			

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

- **Physical Address** displays the physical address of the network card used for the network.
- **MTU** specifies the largest packet size permitted for internet transmissions:
  - Automatic: set the MTU (Maximum Transmission Unit) at 1500.
  - Automatic by DHCP: sets the MTU according to the DHCP connection.
  - Manual: allows you to manually set the MTU.
- 3. Click **Apply** to save changes.

### **Ethernet Connection**

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

To view the connection settings:

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



verizon Basic	Advance	d		Help (8)
letwork Device		Network Settings > Network Conne	ctions > Ethernet	
Fios Router	$\sim$			
Home		Ethernet		
WI-FI	~	Important: Only advanced technic	al users should use this feature.	
Devices	~	Name:	Ethernet	
Parental Controls	0	Status:	Connected	
Status	~	Network:	Network (Home/Office)	
Firewall	×	Connection Type:	Hardware Ethernet Swlich	
Utilities Network Settings	×	MAC Address:	78.DD.12.C9.9D.A4	
Network Objects		IP Address Distribution:	Disable	
Network Connections	- 1	Received Packets:	33213	
Universal Plug & Play		Sent Packets:	57796	
Port Forwarding Rules		Time Span:	1:33:43	
IPv6				
Routing		Apply Setting		
IPv4 Address Distribution		(b)		

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

### **CONFIGURING ETHERNET PROPERTIES**

To configure the connection:

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

verizon <sup>/</sup> Basic	Advanc	ed	Hele (
letwork Device		Network Settings > Network (	Connections > Ethernet
Fios Router	~	Ethermost.	
Home		Ethernet	
Wi-Fi	~	General	
Devices	~	Important: Only advanced te	echnical users should use this feature.
Parental Controls	0	Status:	Connected
Status	×	Network:	Network (Home/Office)
irewall	~	Connection Type:	Hardware Ethernet Switch
Jtilities	ř	Physical Address:	78:00:12:C9:90:A4
Network Settings	^		
Network Objects		MTU:	Automatic ¥ 1500
Network Connections		HW Switch Ports:	
Universal Plug & Play			
Port Forwarding Rules		Port:	Status
IPv6		Port1:	Disconnected
Routing		Port2:	Connected 100 Mbps Full-Duplex
IPv4 Address Distribution		Port3:	Disconnected
IPv6 Address Distribution		Port4:	Connected 1000 Mbps Full-Duplex
Port Configuration			

2. Configure the following settings, as needed.

#### General

Verify the following information:

- Status displays the connection status of the network.
- **Network** displays the type of network connection.
- Connection Type displays as Hardware Ethernet Switch.
- **Physical Address** displays the physical address of the network card used for the network.

- MTU specifies the largest packet size permitted for
  - Automatic: sets the MTU (Maximum Transmission Unit at 1500).
  - Automatic by DHCP: sets the MTU according to the DHCP connection.
  - **Manual**: allows you to manually set the MTU.
- HW Switch Ports displays the status of each LAN port.
- **3**. Click **Apply** to save the changes.

### **Broadband Connection (Ethernet/Coax)**

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

To view the connection settings:

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

verizon Basic	Advanced	d	Hele ®
Network Device		Network Settings > Network Co	onnections > Broadband Connection (Ethernet/Coax)
Fios Router	~		• ···
Home		Broadband	Connectio
WI-FI	v	Enable Settings.	
Devices	~	Important: Only advanced tech	hnical users should use this feature.
Parental Controls	o	Name:	Broadband Connection (Ethernet/Cos
Status	×	Status:	Disconnected
Firewall	×	Network:	Network (Home/Office)
Utilities Network Settings	×	Connection Type:	Disconnected
Network Objects		MAC Address:	
Network Connections		IPv4 WAN Address:	0.0.0
Universal Plug & Play		Subnet Mask:	0.0.0
Port Forwarding Rules		Default Gateway:	0.0.0
IPv6			
Routing		IPv4 DNS Address 1:	
IPv4 Address Distribution		IPv4 DNS Address 2:	

		_	
letwork Device		Network Settings > Network Connections > Broadband Connection (Ethernet/Coax)	
Fios Router	~	Broadband Connectio	
Home	i i	Broauband Connectio	
WI-FI	v	IPv4 DNS Address 2:	
Devices	÷	IP Address Distribution: DHCP	
Parental Controls	0	IPv6 WAN Address:	
Status	×	IPv8 Link Local Address:	
Firewall	ř	IPv6 DNS Address 1: 0	
Utilities	×	· · · · · · · · · · · · · · · · · · ·	
Network Settings	^	IPv6 DNS Address 2:	
Network Objects		Received Packets:	
Network Connections		Sent Packets:	
Universal Plug & Play		Time Span:	
Port Forwarding Rules		Coax Channels: Cable Disconnected	
IPv6		Vuox viiamiets. Caure usuumievieu	
Routing		Apply Settings	



### **Coax - Enable Settings**

verizon Basic	Advanced			Hele & -
Network Device		Network Settings > Network Connect	ions > Coax	
Fios Router	~	Coax		
Home		Enable Settings.		Enabled
WI-FI	•			
Devices	×	Important: Only advanced technical	users should use this feature.	
Parental Controls	0	Name:	Coax	
Status	÷	Status:	Cable Disconnected	
Firewall	×	Network:	Network (Home/Office)	
Utilities	×	Connection Type:	Hardware MoCA	
Network Settings	î	MAC Address:	78:DD:12:C9:9D:A4	
Network Connections		IP Address Distribution:	Disable	
Universal Plug & Play		Received Packets:	0	
Port Forwarding Rules		Sent Packets:	0	
IPv6		Time Span:		
Routing				
IPvd Address Distribution work/networkconnections/co	axsettings	Apply Settings		,

- 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.

erizon Basic	Advanced		Help 🛞 🗸
work Device		Network Setlings > Network Connections > Network Connection Broadband Setlings	
Fios Router	~	Broadband Connection (Ethernet/	
me	•	Broadband Connection (Ethernet/	
FI	•	General	
lices	•	Important: Only advanced technical users should use this feature.	
ental Controls	0	Status: Disconnected	
us	v	Network: Broadband Connection (Ethernet/Coax)	
wall	×	Connection Type:	
tles	×		
work Settings	^	Physical Address:	
twork Objects		MTU: Automatic ~ 1500	
twork Connections		Coax Link	
versal Plug & Play		Privacy: Z Enable	
t Forwarding Rules		Automatically connect	
6		O Manual entry of privacy password	
uting			
Pv4 Address Distribution Prizon <sup>v/</sup> Baalc		Coase Link:	Hele 🛞 -
Pv4 Address Distribution		Coss Link:	Hala 🛞 V
4 Address Distribution	Advanced		Holig 🛞 v
4 Address Distribution rizon Basic ark Device Dis Router		Network Bettings 3 Network Connections 3 Network Connection Broadband Settings	Hala 🕲 🗸
4 Address Distribution		Network Bettings 3 Network Connections 3 Network Connection Broadband Settings	Hale ® ~
4 Address Distribution rizon / Basic ark Device os Router Fi		Noteen Satings 3 Noteen Connections 3 Noteen Connection Bradiand Settings Broadband Connection (Ethernet/	нык ⊗∽
44 Address Distribution rizon / Basic os Router  re  ri  ne  ri  ne  ental Controls		Referent Stellings 2 Meteoric Connections 2 Meteoric Connection Bisadiland Betlings Broadband Connection (Ethernet/ Voir stells Coas Connection States: Coas Connection Speeds WAN Coas Connection Speeds	ных 🛞 -
4 Address Distribution  tzon / Basic  sk Decks  sk Decks sk Decks  sk Decks  sk Decks sk	* * *	Noteen's Sattings 3 Verseu's Connection Breathand Sattings  Broachband Connection (Ethernet/  Coas Connection Speeds  MAN Coas Connection Speeds  Reder TxMNppi 200	ны (8) -
4 Address Distribution rtzon / Besic rt Device rst Device rst Device rst Device rst Device rst Locs sental Controls tus wall	* * *	Network Setting: ) Network Connection Connection Baselised Settings   Broaciband Connection (Ethernet/  Cosx Connection States:  Cosx Connection Speeds  Roder TxIMappi 0.00  Roder RxIMappi 0.00	ны (),
rizon / Basic st. Deska os Router Fi tices ental Controls tus wall tites	* * *	Noteen's Sattings 3 Verseu's Connection Breathand Sattings  Broachband Connection (Ethernet/  Coas Connection Speeds  MAN Coas Connection Speeds  Reder TxMNppi 200	ша () -
rizon / Besic st. Desks os Router Fi fices ental Controls tus wall tites work Settings	* * *	Network Setting: ) Network Connections (Ethernet/ Broadband Connection (Ethernet/ Coax Connection States: <u>On to WAH Coax States</u> WAN Coax Connection Speeds Router TxMbpol 0.00 Router Ruffligs1 0.00 WAN IP Address Interset Protocol: Ottain IP-4 Address Automatically	ны () -
rizon / Besic sit Desise os Router Fi fices ental Controls tus woall titles tus tus titles tus tus tus tus tus tus tus tu	* * *	Network Setting: 3 Network Connections 5 Network Connection Breakbard Settings   Broadband Connection (Ethernet/  Coss Connection Stetes:  Coss UNAI Coss States    WAN Coss Connection Speeds   Rouder RußRapsi 0.00  WAN IP Address  Internet Protocol: Costain TP-4 Address Automatically N DP-4 Address	на () -
rizon / Besic crizon / Besic crizon / Besic con Duter Fi fes ental Controls tus www.settings etwork Objects etwork Connections	* * *	Network Settings 3 Network Connection Exactland Settings  Broadband Connection (Ethernet/  Coas Connection Speeds  WAN Coas Connection Speeds  Router TutMaps 000  Router TutMaps 000  WAN IP Address Internet Protocol:  0 0 Prive Address Automatically  10 Prive Address	ша ®-
4 Address Distribution rfzon / Basic bits Desice bits Desice re r r r r r r r r r r r r r r r r r	* * *	Network Setting: 3 Network Connections 5 Network Connection Breakbard Settings   Broaciband Connection (Ethernet/  Cosx Connection States: Cosx Connection Speeds  Router XriMlapsi 0.00  WANIP Address  Network Rridlapsi Obtain IP-4 Address Automatically NetP-4 Address Obtain IP-4 Address Obtain IP-4 Address Obtain IP-4 Address	ша ©-
rizon / Basic rizon / Basic an Dente Basic Inter Fi Inter Fi Inter Fi Inter Model	* * *	Network Setting: 3 Network Connection: 3 Network Connection Blastland Berrings	ша ©-
4 Address Distribution rfzon / Basic bits Desice bits Desice re r r r r r r r r r r r r r r r r r	* * *	Network Setting: 3 Network Connection: 3 Network Connection (Ethernet/ Broadbaad Connection (Ethernet/ Cess Connection States: WAN Coas Connection Speeds Rover TxMBpoi 0.00 Rover TxMBpoi 0.00 WANIP Address Internet Protocol: Oranin Subart Rask: Decinin States: Decinin States: D	

2. Configure the following settings, as needed.

### General

Verify the following information:

- Status displays the connection status of the network.
- **Network** displays the type of network connection.
- **Connection Type** displays the type of connection interface.
- **Physical Address** displays the physical address of the network card used for the network.
- **MTU** specifies the largest packet size permitted for internet transmissions:
  - Automatic: sets the MTU (Maximum Transmission Unit at 1500).
  - Automatic by DHCP: sets the MTU according to the DHCP connection.
  - **Manual**: allows you to manually set the MTU.

### **Coax Link**

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

- In the Internet Protocol section of WAN IP Address, specify one of the following:
  - No IPv4 Address: the connection has no IP address. This is useful if the connection operates under a bridge.
  - Obtain an IPv4 Address Automatically: the network connection is required by Verizon to obtain an IP address automatically. The server assigning the IP address also assigns a subnet mask address, which can be overridden by entering another subnet mask address.
  - Use the Following IP Address: the network connection uses a permanent or static IP address and Subnet Mask address, provided by Verizon or experienced network technician.
- To override the subnet mask, select the **Override Subnet Mask** check box, then enter the new subnet mask.
- Click **Release/Renew** in the **DHCP Lease** field to drop/ get an IP address from the DHCP server.
- In the **Expires In** field, enter the amount of time a network device is allowed to connect to the Fios Router with its currently issued dynamic IP address.

- IPv4 DNS selects Obtain IPv4 DNS Address Dynamically for using Dynamic DNS. Each time the public IP address changes, the DNS database is automatically updated with the new IPv4 address. In this way, even though the IP address changes often, the domain name remains constant and accessible.
- Internet Connection Firewall allows you to enable or disable the firewall configuration on this interface.
- 3. Click Apply to save changes.

### 6.2c/ UNIVERSAL PLUG AND PLAY

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

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

UPnP services are not deleted when disconnecting a computer without proper shutdown of the UPnP applications, such as messenger. Services may often not be deleted and eventually this leads to the exhaustion of rules and services. No new services can be defined. The cleanup feature locates the invalid services and removes them, preventing services exhaustion.

#### To access this setting:

1. Select Universal Plug & Play in the Network Settings section.



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

### 6.2d/ PORT FORWARDING RULES

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

To access the rules:

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



twork Device		Network Settings > Port Forwar	ding Rules	
Fios Router	$\sim$			
	*	Port Forwar	ding Rules	
etwork Settings	^	Below is a list of currently cont	igured Protocols that are implemented in the router.	
Network Objects		Protocols	Ports	
Network Connections		FTP	TCP Any $ ightarrow$ 21	Edit Remove
Universal Plug & Play		HTTP	TCP Any $\rightarrow$ 80	Edit Remove
Port Forwarding Rules		HTTPS	TCP Any $\rightarrow$ 443	Edit Remove
-	- 1	IMAP	TCP Any $\rightarrow$ 143	Edit Remove
	- 1	L2TP	UDP Any $\rightarrow$ 1701	Edit Remove
Routing	- 1	Eina	ICMP Echo Request	Edit Remove
Pv4 Address Distribution	- 1	POP3	TCP Any $ ightarrow$ 110	Edit Remove
Pv6 Address Distribution	- 1	SMTP	TCP Any $ ightarrow$ 25	Edit Remove
Port Configuration	- 1	SNMP	UDP Any $\rightarrow$ 161	Edit Remove
ate & Time		Telnet	TCP Any $\rightarrow$ 23	Edit Remove
NS Settings	÷	TETP	UDP 1024 - 65535 $ ightarrow$ 69	Edit Remove
to serninge	Ť	Traceroute	UDP 32769 - 65535 $\rightarrow$ 33434 - 33523	Edit Remove

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

verizon Basic Advanced	d	<u>Help</u>	® ~
Network Device	Network Settings > Port Forwarding Rules > Edit Service		
Fios Router V	Edit Service		
Network Settings	Edit Service		
Network Objects	Service Name		-
Universal Plug & Play	Service Description		
Port Forwarding Rules	Service Ports		
IPv6	Protocols Ports		_
Routing	ba		
IPv4 Address Distribution			
IPv6 Address Distribution	Cancel Apply		

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

verizon Basic	Advanced				Help	<mark>®</mark> ~
Network Device		Network Settings > Port Forwarding	Rules > Edit Service			
Fios Router	×	Edit Service				
Network Settings	^	Edit Service Server Port	ts			
Network Objects		Protocol	тср			
Universal Plug & Play		Source Ports	Any	·		
Port Forwarding Rules	- 1	Destination Ports	Any	-		
IPv6	- 1					
Routing	- 1	Cancel	Apply			
IPv4 Address Distributio	n					

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

#### 6.2e/ IPv6

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

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



verizon Basic Advance	ced		Hola 🔕 -
Network Device	Network Settings > IPv6 Configura	tion Controls	
Flos Router V	IPv6 Configu	ration Controls	
Network Settings ^	1. Enable IPv6 Support		Enabled
Network Objects			
Network Connections	2. Specify the method t	to be used to obtain your WAN IPv6 Address	
Universal Plug & Play	IPv6 WAN Configuration:	DHCPv6-PD	
Port Forwarding Rules	Delegated Prefix:	None	
IPv6	Expires In:	DHCPv6-PD	
Routing		Static (Auto-Configure)	
IPv4 Address Distribution	Prefix Lifetime:	Static (Manually Configure)	
IPv6 Address Distribution	WAN Link-Local Address:	0	
Port Configuration	Obtain IPv6 DNS Server ad	ddress automatically	
Date & Time v	Use the following IPv6 DN:	\$ Server addresses	
DNS Settings v			
Monitoring ~	3. Specify the method	to be used to assign LAN IPv6 addresses	
System	IPv6 LAN Configuration:	Stateless ~	
	LAN Prefix:		

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

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

- To disable the IPv6 service, click on the Disable option in the Enable IPv6 Support field.
- 6. Click **Apply changes** to have changes take effect.

Once configured using valid IPv6 WAN and LAN configurations, you should not see any errors when you click on the **Apply changes** button and the **Status** page on the main menu will reflect the router's new IPv6 address.

You should also see the IPv6 address for all IPv6 supported devices on your local network displayed on the **Basic/Devices/ Devices** page by selecting **Expanded List** from the dropdown list.

		Devices > All			
	~	Devices All (2) Primary (2) Guest (0) IoT	(0)		
	~	Sort A to Z	Show All	~	Expanded List
	^	Device Name	Parental Controls	Connection	Compact List
	2	Online			Expanded List
ols	0				
	Ŷ	Ac005-NB2  Device: PC  Connected to: G3100  Mac Address: 48.5b.39.4f:56.08  IPv4 Address: 192.168.1153	None	🖾 Ethernet	
			None	Ethernet	
		Device: Extender Connected to: G3100 Mac Address: b8:48:53:84:e6:68 IPv4 Address: 192.168.1100			

### Static - WAN IPv6 Address Connection

The IPv6 WAN Static configurations are IPv6 settings that you enter manually. These specific IPv6 addresses and settings are not expected to change frequently.

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



verizon <sup>/</sup> Basic Advance	ed		Helo Q ~
Network Device	Network Settings > IPv6 Configurat	tion Controls	
Fios Router V	IPv6 Configu	ration Controls	Apply Changes
Network Settings	î vo comiga		
	1. Enable IPv6 Support		Enabled
Network Objects	2 Specify the method t	to be used to obtain your WAN IPv6 Address	
Network Connections	2. Specify the method t		
Universal Plug & Play	IPv6 WAN Configuration:	Static (Auto-Confi	
Port Forwarding Rules	Assigned Prefix:	None	
IPv6	IPv6 WAN Address:	DHCPv6-PD	
Routing		Static (Auto-Configure)	
IPv4 Address Distribution	Default Gateway:	Static (Manually Configure)	
IPv6 Address Distribution	IPv6 DNS Address 1:		
Port Configuration	IPv6 DNS Address 2:		
Date & Time v	3. Specify the method t	to be used to assign LAN IPv6 addresses	
DNS Settings 🗸 🗸	IPv6 LAN Configuration:	Stateless	
Monitoring ~			
System	LAN Prefix:		
	IPv6 LAN Address:	fec0::1 / 0	-

- 2. Specify the **Static** method to be used to obtain your WAN IPv6 Address by entering:
  - IPv6 WAN Configuration (select Static)
  - Assigned Prefix (A numeric value between 16 and 128)
  - IPv6 WAN Address
  - Default Gateway: Fios Router
  - IPv6 (Primary) DNS Address 1
  - IPv6 (Secondary) DNS Address 2
- 3. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

#### Static WAN with LAN IPv6 Stateful Settings

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

verizon Basic Ad	ivanced		Hale 🕲 🗸
Network Device		Network Settings > IPv6 Configuration	1 Controls
Fios Router	~	IPv6 Configur	ration Controls
Network Settings	^		
Network Objects		Default Gateway:	
Network Connections		IPv8 DNS Address 1:	
Universal Plug & Play		IPvő DNS Address 2:	
Port Forwarding Rules			
IPv6		3. Specify the method to I	be used to assign LAN IPv6 addresses
Routing		IPv6 LAN Configuration:	Stateful (DHCPv6)
IPv4 Address Distribution		LAN Prefix:	Stateless Stateful (DHCPv6)
IPv6 Address Distribution		IPvő LAN Address:	fec0:1 /
Port Configuration		DHCPv6 Client Address Range:	1000 - 2000
	Ť	LAN Link-Local Address:	0
	Ť	Router Advertisement Lifetime:	15 minutes (0-150)
•	ř		
System		IPv6 Address Lifetime:	60 minutes (3-150)

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

- Subnet ID set the site topology for your internal site
- Router Advertisement Lifetime (minutes between 0-150)
- IPv6 Address Lifetime (minutes between 3-150)
- Option: Allow ICMPv6 Echo Request for LAN devices using their Global IPv6 Address from WAN side requesting an IPv6 address from any available DHCPv6 servers available on the ISP
- **3**. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

### Static WAN with LAN IPv6 Stateless Settings

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

verizon <sup>/</sup> Basic Advan	ced		Help 🛞 ~
Network Device	Network Settings > IPv6 Configuration	Controls	
Fios Router 🗸			
	, IPv6 Configur	ation Controls	Apply Changes
Network Settings ^			<b>^</b>
Network Objects	Default Gateway:		
Network Connections	IPv6 DNS Address 1:		
Universal Plug & Play	IPv6 DNS Address 2:		
Port Forwarding Rules			
IPv6	3. Specify the method to	be used to assign LAN IPv6 addresses	
Routing	IPv6 LAN Configuration:	Stateless	
IPv4 Address Distribution	LAN Prefix:	Stateless Stateful (DHCPv6)	
IPv6 Address Distribution	IPv8 LAN Address:	fec0::1 / 0	
Port Configuration	LAN Link-Local Address:	0	
Date & Time 🗸 🗸	LAN LINK-Local Address:	U	
DNS Settings ~	Router Advertisement Lifetime:	15 minutes (0-150)	
Monitoring ~	Option		
System	Allow ICMPv6 Echo Requests	for LAN devices using their Global IPv6 Address from WAN side	

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

### DHCPv6 PD - WAN IPv6 Address Connection

The IPv6 WAN DHCPv6 configurations are IPv6 settings that you enter that will allow your IPv6 connection to be updated by the ISP as needed.

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



verizon <sup>v</sup> Basic Advanced		Hele 🕲 ~
Network Device	Network Settings > IPv6 Configuration Controls	
Fios Router 🗸		Apply Changes
*	IPv6 Configuration Cont	rois Apply Changes
Network Settings ^	1. Enable IPv6 Support	Enabled
Network Objects		
Network Connections	2. Specify the method to be used to obtain y	Sur WAN IPV6 Address
Universal Plug & Play	IPv6 WAN Configuration: DHCPv6-PD	
Port Forwarding Rules	Delegated Prefix:	0
IPv6	DHCPv6-PD	
Routing	Static (Auto-Configu	ire)
IPv4 Address Distribution	Prefix Lifetime: Static (Manually Cor	nfigure)
IPv6 Address Distribution	WAN Link-Local Address: 0	
Port Configuration	Obtain IPv8 DNS Server address automatically	
Date & Time v	O Use the following IPv6 DNS Server addresses	
DNS Settings v		
Monitoring ~	3. Specify the method to be used to assign L	AN IPv6 addresses
System	IPv6 LAN Configuration: Stateless	~
	LAN Prefix:	

- 2. Check to either Obtain IPv6 DNS Server address automatically, or Use the following IPv6 DNS Server addresses
- 3. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

### DHCPv6 WAN with LAN IPv6 Stateful (DHCPv6) Settings

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

verizon <sup>4</sup> Basic Advance	d	Helo (8)
Network Device	Network Settings > IPv6 Configuration Controls	
Fios Router 🗸 🗸	D.C.O. financian Ocastad	Apply Changes
	IPv6 Configuration Controls	S Apply changes
Network Settings ^		
Network Objects	Default Gateway:	
Network Connections	IPvő DNS Address 1:	
Universal Plug & Play	IPv8 DNS Address 2:	
Port Forwarding Rules		
IPv6	3. Specify the method to be used to assign LAN IP	v6 addresses
Routing	IPv6 LAN Configuration:	
IPv4 Address Distribution	LAN Prefix:	
IPv6 Address Distribution	Stateful (DHCPv6) IPv6 LAN Address: fec0::1	1
Port Configuration		
Date & Time 🗸 🗸	DHCPv6 Client Address Range: 1000 . 200	10
DNS Settings ~	LAN Link-Local Address: 0	
Monitoring ~	Router Advertisement Lifetime: 15	minutes (0-150)
System	IPv6 Address Lifetime: 60	minutes (3-150)

- 2. Specify the **Stateful (DHCPv6)** settings to be used to assign LAN IPv6 addresses by entering the following details:
  - IPv6 LAN Configuration (select Stateful from the dropdown list)
  - LAN Prefix (automatically populated)
  - IPv6 LAN Address (automatically populated)
  - DHCPv6 Client Address Range (start and end)
  - LAN Link Local Address (automatically populated)
  - Subnet ID set the site topology for your internal site
  - Router Advertisement Lifetime (minutes between 0-150)

- IPv6 Address Lifetime (minutes between 3-150)
- Option: Allow ICMPv6 Echo Request for LAN devices using their Global IPv6 Address from WAN side requesting an IPv6 address from any available DHCPv6 servers available on the ISP
- 3. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

### DHCPv6 WAN with LAN IPv6 Stateless Settings

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

verizon Basic Advance	d		Helo & ~
Network Device	Network Settings > IPv6 Configuration	Controls	
Fios Router V	IPv6 Configura	ation Controls	Apply Changes
Network Settings			*
Network Objects	Default Gateway:		
Network Connections	IPv6 DNS Address 1:		
Universal Plug & Play	IPv6 DNS Address 2:		
Port Forwarding Rules			
IPv6	3. Specify the method to b	be used to assign LAN IPv6 addresses	
Routing	IPv6 LAN Configuration:	Stateless	
IPv4 Address Distribution	LAN Prefix:	Stateless	
IPv6 Address Distribution	IPv6 LAN Address:	Stateful (DHCPv6) fec0::1 / 0	
Port Configuration	LAN Link-Local Address:	0	
Date & Time ~			
DNS Settings ~	Router Advertisement Lifetime:	15 minutes (0-150)	
Monitoring ~	Option		
System	Allow ICMPv8 Echo Requests	for LAN devices using their Global IPv8 Address from WAN side	

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

### LAN IPv6 Configuration without An IPv6 WAN Connection

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



verizon Basic Advanced			Help & ~
Network Device	Network Settings > IPv6 Configuration Contr	rols	
Fios Router V	IPv6 Configurati	ion Controls	
Network Settings	1. Enable IPv6 Support		Enabled
Network Objects	2. Specify the method to be us	sed to obtain your WAN IPv6 Address	
Universal Plug & Play	IPv6 WAN Configuration:	DHCPv6-PD	
Port Forwarding Rules	Delegated Prefix:	None	
IPv6	Expires In:	DHCPv6-PD	
Routing	Prefix Lifetime:	Static (Auto-Configure)	
IPv4 Address Distribution	WAN Link-Local Address: 0	Static (Manually Configure)	
Port Configuration	Obtain IPv6 DNS Server address au	atomatically	
Date & Time ~	Use the following IPv8 DNS Server	addresses	
DNS Settings v	3. Specify the method to be u	sed to assign LAN IPv6 addresses	
System	IPv6 LAN Configuration:	ilateless ~	
	LAN Prefix:		

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

### LAN IPv6 Stateful (DHCPv6) with No WAN Settings

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

verizon√ Basic Ad	ivanced		1	tele Ø
Network Device		Network Settings > IPv6 Configuratio	n Controls	
Fios Router	~	IPv6 Configu	ration Controls Apply cha	inges
Network Settings	· ^ -	•		
Network Objects		Default Gateway:		
Network Connections		IPv6 DNS Address 1:		
Universal Plug & Play		IPvő DNS Address 2:		
Port Forwarding Rules				
IPv6		3. Specify the method to	be used to assign LAN IPv6 addresses	
Routing		IPv6 LAN Configuration:	Stateful (DHCPv6)	
IPv4 Address Distribution		LAN Prefix:	Stateless Stateful (DHCPv6)	
IPv6 Address Distribution		IPv6 LAN Address:	fec0:1 /	
Port Configuration		DHCPv6 Client Address Range:	1000 - 2000	
Date & Time	×	oner to orient Address hanger		
DNS Settings	•	LAN Link-Local Address:	0	
Monitoring	<b>~</b>	Router Advertisement Lifetime:	15 minutes (0-150)	
System		IPv6 Address Lifetime:	60 minutes (3-150)	

- 2. Specify the **Stateful (DHCPv6)** settings to be used to assign LAN IPv6 addresses by entering the following details:
  - IPv6 LAN Configuration (select Stateful from the dropdown list)
  - LAN Prefix (automatically populated)
  - IPv6 LAN Address (automatically populated)
  - DHCPv6 Client Address Range (start and end)
  - LAN Link Local Address (automatically populated)
  - Subnet ID set the site topology for your internal site
  - Router Advertisement Lifetime (minutes between 0-150)
  - IPv6 Address Lifetime (minutes between 3-150)

- Option: Allow ICMPv6 Echo Request for LAN devices using their Global IPv6 Address from WAN side requesting an IPv6 address from any available DHCPv6 servers available on the ISP
- 3. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

#### LAN IPv6 Stateless with No WAN Settings

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

verizon Basic	Advanced				Hele & ~
Network Device		Network Settings > IPv6 Configuration	Controls		
Fios Router	~	IDv6 Configure	ation Control	-	Apply Changes
Network Settings	^	IPv6 Configura	ation Control	5	
Network Objects		Default Gateway:			
Network Connections		IPv6 DNS Address 1:			
Universal Plug & Play	- 1	IPv6 DNS Address 2:			
Port Forwarding Rules					
IPv6		3. Specify the method to b	e used to assign LAN IP	v6 addresses	
Routing		IPv6 LAN Configuration:	Stateless		
IPv4 Address Distribution		LAN Prefix:	Stateless Stateful (DHCPv6)		
IPv6 Address Distribution		IPv6 LAN Address:	fec0::1	/ 0	
Port Configuration		LAN Link-Local Address:	0		
DNS Settings	č	Router Advertisement Lifetime:	15	minutes (0-150)	
Monitoring	•	Option			
System		Allow ICMPv6 Echo Requests	for LAN devices using their Glob	al IPv6 Address from WAN side	
	-				

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

### 6.2f/ ROUTING SETTINGS

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

### **Routing Table**

To view the rules:

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



verizon <sup>/</sup> Basic	Advan	nced	Hele 🛞 ~
Network Device		Network Settings > Routing	
Fios Router	~	Routing	
Network Settings	^	This page provides the ability to add, edit, or delete routing rules.	
Network Objects		Routing Table	
Network Connections		Name Destination Gateway Netmask Metric	Status
Universal Plug & Play		New Route	
Port Forwarding Rules			
IPv6		Internet Group Management Protocol (IGMP)	
Routing		Enable Ethernet	
IPv4 Address Distributio	n	Enable MoCA - Coax	
IPv6 Address Distributio	n	Enable 2.4 GHz Wi-Fi	
Port Configuration		Enable 5 GHz Wi-Fi	
Date & Time	~		

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

verizon Basic	Advanced	I.	Hele	8
Network Device		Network Settings > Routing	g > Route Settings	
Fios Router	~	D		
		Route Set	tings	
Network Settings	^	Routing Entry:	IPv4	
Network Objects		Name:	IPv4	
Network Connections			IPv6	
Universal Plug & Play		Destination:	0 0 0 0	
Port Forwarding Rules	- 1	Netmask:	0 0 0 0	
IPv6	- 1	Gateway:	0 0 0	
Routing	- 1	Metric:	0	
IPv4 Address Distribution	- 1			
IPv6 Address Distribution	- 1	Apply		
Port Configuration	- 1			

- 3. Specify the following parameters:
  - Routing Entry select the IP address type.
  - Name the network connection type.

- **Destination** enter the destination IP of the destination host, subnet address, network address, or default route. The destination for a default route is 0.0.0.0.
- **Netmask** enter the network mask. This is used in conjunction with the destination to determine when a route is used.
- Gateway enter the IP address of your Fios Router.
- **Metric** enter a measurement preference of the route. Typically, the lowest metric is the most preferred route. If multiple routes exist to a specific destination network, the route with the lowest metric is used.
- 4. Click Apply changes to save changes.

### Internet Group Management Protocol (IGMP)

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

#### To enable this function:

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

### 6.2g/ IPv4 ADDRESS DISTRIBUTION

You can easily add computers configured as DHCP clients to the network. The DHCP server provides a mechanism for allocating IP addresses to these hosts and for delivering network configuration parameters to the hosts.

For example, a client (host) sends a broadcast message on the network requesting an IP address for itself. The DHCP server then checks its list of available addresses and leases a local IP address to the host for a specific period of time and simultaneously designates this IP address as taken. At this point, the host is configured with an IP address for the duration of the lease.

The host can renew an expiring lease or let it expire. If it renews a lease, the host receives current information about network services, as it did during the original lease, allowing it to update its network configurations to reflect any changes that occurred since the first connection to the network.

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

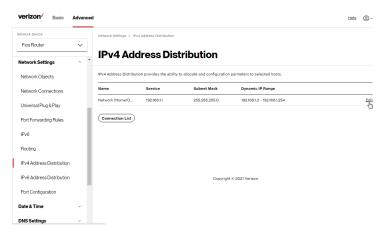
The DHCP server performs the following functions:

- Displays a list of all DHCP host devices connected to your Fios Router
- Defines the range of IP addresses that can be allocated in the network
- Defines the length of time the dynamic IP addresses are allocated

- Provides the above configurations for each network device and can be configured and enabled or disabled separately for each network device
- Assigns a static lease to a network computer to receive the same IP address each time it connects to the network, even if this IP address is within the range of addresses that the DHCP server may assign to other computer
- Provides the DNS server with the host name and IP address of each computer connected to the network

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

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



 You can edit the DHCP server settings for a device. On the IPv4 Address Distribution page, click the Edit icon in the Action column. The DHCP Settings page opens with the device information displayed.

- 3. To enable the DHCP server, select **DHCP Server** in the **IPv4** Address Distribution field.
- Once enabled, the DHCP server provides automatic IP assignments (IP leases) based on the preset IP range defined below.

verizon <sup>,/</sup> Basic Advan	ced		Help & ~
Network Device	Network Settings > IPv4 Address D	Distribution > DHCP Settings	
Fios Router 🗸 🗸			
Network Settings	<sup>^</sup> DHCP Setting	gs for Network (Home/Office)	
Network Objects	Service		Î
Network Connections	IPv4 Address Distribution:	DHCP Server	
Universal Plug & Play	DHCP Server	Disabled	
Port Forwarding Rules	Start IP Address:	DHCP Server	
IPv6			- 1
Routing	End IP Address:	192 168 1 254	
IPv4 Address Distribution	WIN Server:	0 0 0 0	
IPv6 Address Distribution	Lease Time in Minutes:	1440	
Port Configuration	IPv4 Address Distribution Ac	ccording to DHCP Option 60 (Vendor Class Identifier)	
Date & Time ~	Vendor Class Id	IP Address MAC Address QoS	
DNS Settings v	MSFT 5.0	192.168.1.153 48.5B.39:4F.56.08	
Monitoring ~	Verizon BHRx1 DHCP Detect	192.168.1100 B8.F8.53.84.E6.68	
System	Apply		

- 5. To configure the DHCP server, complete the following fields:
  - Start IP Address enter the first IP address that your Fios Router will automatically begin assigning IP addresses from. Since your Fios Router's default IP address is 192.168.1.1, the default start IP address should be 192.162.1.2.
  - End IP Address enter the last IP address that your Fios Router will stop at for the IP address allocation. The maximum end IP address range that can be entered is 192.168.1.254.

## **NETWORK SETTINGS**

- WINS Server determines the IP address associated with a network device.
- Lease Time in Minutes assigns the amount of time in minutes that each device is assigned an IP address by the DHCP server when it connects to the network.

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

6. Click **Apply** to save changes.

## IPv4 Address Distribution According to DHCP option 60 (Vendor Class Indentifier)

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

#### **DHCP Connection List**

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

To view a list of computers:

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

#### 06 / CONFIGURING ADVANCED SETTINGS



verizon Basic	Advanced							Help	8-
etwork Device		Network Settings > IPv4	Address Distribution >	DHCP Connections					
Fios Router	~								
Network Settings	^ <b>*</b>	DHCP Co	onnection	าร					
Network Objects		IPv4 Address Distributio	on provides the ability t	o allocate and configuration p	irmeters to sel	lected hosts.			
Network Connections		Host Name	IP Address	Physical Address	Lease Type	Connection Name	Status	Expired in	
Universal Plug & Play		E3200-b8/85384e	192.168.1.100	88:F8:53:84:E6:68	Dynamic	Network (Home/O	Active	1312	Search Edi
Port Forwarding Rules	- 1	A0005-NB2	192.168.1.153	48:58:39:4F:56:08	Dynamic	Network (Home/O	Active	1312	Searc Ed
IPv6	- 1								
Routing	- 1	Add static connecti	lon						
IPv4 Address Distribution	- 1								
IPv6 Address Distribution	- 1								

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

verizon <sup>,/</sup> Basic Advanced				Hele 🛞 -
Network Device Fios Router	Network Settings > IPv4 Address Distrib			
Network Settings	DHCF Connec	uon Settings	)	
Network Objects	Host name:			
Network Connections	IP Address:	0 0 0	0	
Universal Plug & Play	MAC Address:	00 00 00	00 00 00	
Port Forwarding Rules				
IPv6	Apply			
Routing				
IPv4 Address Distribution				
IPv6 Address Distribution				

- 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.

## **NETWORK SETTINGS**

#### 6.2h/ IPv6 ADDRESS DISTRIBUTION

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

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

verizon <sup>v</sup> Basic	Advanced					Helo (Q
Network Device		Network Settings > IP	6 Address Distribution			
Fios Router	~		droce Die	tribution		
Network Settings	^ ^	IFVOAu	11633 013			
Network Objects		IPv6 Address Distribu	tion provides the ability	to allocate and configuration	n parmeters to selected hosts.	
Network Connections		Name	Service	Prefix	IP Range	
Universal Plug & Play	1	Network (Home/Office)	Stateless	0/0		
Port Forwarding Rules		Connection List				
IPv6	- 1					
Routing						
IPv4 Address Distribution	- 1					
IPv6 Address Distribution	- 1			Copyrigh	t © 2021 Verizon	

- 2. You can edit the DHCP server settings for a device. On the IPv6 Address Distribution page, click the Edit icon in the Action column. The DHCP Settings page opens with the device information displayed.
- **3**. To configure the DHCP server complete the following fields:
  - Start IPv6 Address the starting IPv6 address in the consecutive list of addresses that makes up this LAN pool for the DHCPv6 server.
  - End IPv6 Address the ending IPv6 address in the consecutive list of addresses that makes up this LAN pool for the DHCPv6 server.

• Lease Time in Minutes – assigns the amount of time in minutes that each device is assigned an IP address by the DHCP server when it connects to the network.

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

4. Click Apply to save changes.

#### **DHCP Connection List**

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

To view a list of computers:

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

## **NETWORK SETTINGS**

#### 6.2i/ PORT CONFIGURATION

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

To configure the ports:

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

etwork Device	Network Settings	> Port Configuration			
Fios Router 🗸		at Davit Carifier	ation		
letwork Settings	Êthern	et Port Configu	auon		
Network Objects	Port	Service			Status
Network Connections	WAN Port		Auto	~	Disconnected
Universal Plug & Play	LAN Port 1		Auto	~	Disconnected
Port Forwarding Rules	LAN Port 2	Full-Duplex 100 Mbps	Auto	~	Connected
IPv6	LAN Port 3		Auto	÷	Disconnected
Routing					
IPv4 Address Distribution	LAN Port 4	Full-Duplex 1000 Mbps	Auto		Connected
IPv6 Address Distribution			Auto 10 Half-Duplex		
Port Configuration			10 Full-Duplex		
ate & Time ~			100 Half-Duplex		
NS Settings ~			Co 100 Full-Duplex		
Aonitoring ~			1000 Full-Duplex		

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

#### 6.3/ DATE & TIME

You can configure the following settings:

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

#### 6.3a/ DATE & TIME SETTINGS

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

To configure the settings:

- 1. From the Advanced menu, select Date & Time.
- 2. Select Date & Time in the Date & Time section.

verizon Basic	Advanc	ed		Hele (8)
Network Device		Date & Time → Date & Time		
Fios Router	~			
Status		Date & Time		Refresh
	Ť	Press the Refresh button to upda	te the status.	
Firewall	ř			
Utilities	~	Localization		
Network Settings	~	Local Time:	Dec 31, 1969 08:29:32pm	Edit
Date & Time	^	Time Zone:	Eastern_Time (Default)	
Date & Time		Automatic Time Update	e	Enable
Scheduler Rules			-	•
DNS Settings	~	Protocol:	Network Time Protocol (NTP)	
Monitoring	~	Time Server		bba
System		0.north-america.pool.ntp.org		Edit Remove
		1.north-america.pool.ntp.org		Edit Remove
		Last updated:		

## DATE & TIME

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

verizon <sup>v</sup>	Basic	Advance	d	Help	<u>®</u> ~
Network Device			Date & Time > Date & Time		
Fios Router		~	Edit Time Server	pply Changes	
Status		. *	Edit Time Server	ppry changes	
Firewall			Enter Server IP address or domain name.		
Utilities			Time Server:		
Network Settings					
Date & Time		^			
Date & Time					

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

#### 6.3b/ SCHEDULER RULES

**Scheduler Rules** are used for limiting the activation of firewall rules to specific time periods. The time periods are either for days of the week or for hours of each day based on activity or inactivity.

To define a rule:

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

#### 06 / CONFIGURING ADVANCED SETTINGS



verizon Basic	Advanced	Hale 🛞 -
Network Device		Date & Time > Scheduler Rules
Fios Router	~	
		Scheduler Rules
Status	*	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.
Firewall	~	Rule Name Settings Status
Utilities	v	Add
Network Settings	~	( Add )

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

verizon Basic	Advanced			Help 🛞 🗸
Network Device		Date & Time > Scheduler Rules > Rul	ie scheduler	
Fios Router	~			Apply Changes
Status	v *	Rule Schedule	er (	Apply Changes
Firewall	v	Rule name:		
Utilities	÷	Rule days:	Sun Mon Tue Wed Thu Fri Sat	
Network Settings	× 1	Rule time:	Start Time         End Time           9:00 pm         12:00 am         ^	

- 4. Enter the name of the rule, select the active or inactive days of the week and the start and end time range.
- 5. Specify if the rule is active at the scheduled time or inactive at the scheduled time.
- 6. Click Apply changes to save changes.

#### 6.4/ DNS SETTINGS

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

## **DNS SETTINGS**

#### 6.4a/ DYNAMIC DNS

Typically, when connecting to the internet, your router is assigned an unused public IP address from a pool, and this address changes periodically.

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

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

To set up dynamic DNS:

- 1. From the Advanced menu, select DNS Settings.
- 2. Select **Dynamic DNS** in the **DNS Settings** section.

verizon Basic	Advanced				Help 🛞 -
Network Device		DNS Settings > Dynamic DNS			
Fios Router	~	Dynamic DN	e		Refresh
Statue	v *	-			
Firewall	*	Dynamic DNS (Domain Name Se accessible from the Internet.	erver) is a dynamic IP Address t	o be aliased to a static hostname, allowing a computer on y	our network to be more easily
Utilities	*	Host Name	Status	Last Update	
Network Settings	~	bba			
Date & Time	~				
DNS Settings	^				
Dynamic DNS	- 1				

3. To set up a new entry, click the **Add** button.

#### 06 / CONFIGURING ADVANCED SETTINGS



Network Device		
Flot Router		
Status Dynamic DNS Dynamic DNS Dynamic DIS IDenami Hame Server) is a dynamic P Address to be attained to a static hostmame, allowing a computer on your network to it	e more	^
Firewall         eisily accessible from the Internet.           Utilities         Setup Dynamic DNS (Domain Name Server)		
Network Settings V Host name		
Date & Time Provider chargelp.com		-
Dynamic DNS Initials and manage advaceden dyndra.com dyndra.com DNS Server User name easydra.com		-
Monitoring v Password no-tp.com		
System		

- 4. Configure the following parameters:
  - Host Name enter the full domain name for your Dynamic DNS domain.
  - **Provider** select the Dynamic DNS account provider from the menu.
  - User Name enter your user name for your Dynamic DNS account.
  - **Password** enter the password for your Dynamic DNS account.
  - SSL Mode select if your Dynamic DNS service supports SSL.
- 5. Click **Apply** to save your changes.

## **DNS SETTINGS**

To edit the host name or IP address:

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

#### 6.4b/ DNS SERVER

You can edit the host name and/or IP address, if the host was manually added to the DNS table. If not, you can only modify the host name.

To access the DNS server:

1. Select DNS Server in the DNS section.

verizon Basic	Advanced	1			Hele &
Network Device		DNS Settings > DNS Server			
Fios Router	~				
Status	. *	DNS Server			
Firewall	•	Add, edit, or delete computers known	n by the router's DNS server		
Utilities	÷	Host Name	IP Address	Source	
		E3200-b8/85384e668	192.168.1.100	DHCP	
Network Settings	×	A040025-NB2	192.168.1.151	DHCP	
Date & Time	×	Add DNS Entry			
DNS Settings	^				
Dynamic DNS		Enable DNS Rebind Protection	n		
DNS Server		To disable DNS Rebind Protection for To disable DNS Rebind Protection for	r all devices connected to this router, r specific IP addresses, create an exc	unlick the checkbox above. eption with the dropdown below.	
Monitoring	×	Exceptions to DNS Rebind	Protection		
System		IP/Netmask			
		Add Exceptions Entry +	~		
	. 1				

2. To disable DNS rebind protection, untick the checkbox of Enable DNS Rebind Protection.

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

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

verizon Basic	Advanc	ed	<u>Help</u>	® ~
Network Device		DNS Settings > DNS Server > DNS Server Setting		
Fios Router	~			
Statue		DNS Server		
Firewall	•	DNS Entry		
Utilities	×	Host Name:		
Network Settings	×	IP Address:		
Date & Time	~			
DNS Settings	^	Apply		
Dynamic DNS				
DNS Server				

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

## MONITORING

#### 6.5/ MONITORING

You can view the details and status of:

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

#### 6.5a/ SYSTEM LOGGING

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

To view the system log:

- 1. From the Advanced menu, select Monitoring.
- 2. In the **Monitoring** section, click the **System Logging** link.

letwork Device		Monitoring > System L	.ogging > System Log			
Fios Router	~	System	ogging		Options	Refresh Save
Statue	· *	-	curity Log Advance	d Log Firewall Log	WAN DHCP Log LAN DHCP Log	
Firewall	~	Time	Event type	Log Level	Details	Clear
Jtilities	~	Mar 18 05:52:53 2019	named[32671]	err<139>	client 192.168.1251#59390 (onecs-live. clients.query failed (SERVFAIL) for one query.c.7837	
Network Settings	~				query.c:7837	
Date & Time	÷	Mar 18 05:52:53 2019	named[32671]	err<139>	client 192.168.1251#61785 (www.bing.c clients:query failed (SERVFAIL) for www query.c.7837	
ONS Settings	~				client 192.168.1.251#53589 (beacons5.)	tenetri uniu (mon 21 m
Monitoring	^	Mar 18 05:52:52 2019	named[32671]	err<139>	clients:query failed (SERVFAIL) for bea query.c:7837	
System Logging		Mar 18 05:52:50	named[32671]	err<139>	client 192.168.1.251#60570 (time.windo clients:query failed (SERVFAIL) for time	
System-wide Connections	5				query.c:7837	
Bandwidth Monitoring		Mar 18 05:52:49 2019	named[32671]	err<139>	client 192.168.1.251#55845 (edf.eset.co failed (SERVFAIL) for edf.eset.com/IN/	
System	- 1	Mar 18 05 52-48	named[32671]	err<139>	client 192.168.1.251#52457 (time.windor clients.guery failed (SERVFAIL) for time	



**3**. To view a specific time of log event, click on the **options** button.

verizon Basic	Advanced		Help	8-
Network Device		Monitoring > System Logging > System Log		
Fios Router	× ^	System Logging		
WI-FI	v	SystemLog SecurityLog AdvancedLog FirewallLog WANDHCPLog LANDHCPLog Log viewing options		
Devices	×			-
Parental Controls	0	O Past day		
Status	×	O Past week		
Firewall	×	Custom range		
Utilities	~	Start Date Start Time		
Network Settings	~	at 12/31/00 12:00 am ~		
Date & Time	v	End Date End Time		
DNS Settings	÷	III 12/31/00 t2:00 am ♥		
Monitoring	^	Cancel Save		
System Logging				

- 4. Click **Save** to save changes.
- 5. To view a specific type of log event such as Security Log, WAN DHCP Log, etc., click the appropriate link in the menu on the top.
- 6. To update the data, click **Refresh**.

## MONITORING

#### 6.5b/ SYSTEM-WIDE CONNECTIONS

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

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

1. In the Monitoring section, click System-wide Connections.

letwork Device		Monitoring > System-v	ide Traffic Connections				
Fios Router	~	Contorn					
Statue	÷	System-			Auto-ref	resh 💽	
Firewall	÷	Name	Network (Home/Office)	Broadband Connection (Ethernet/Coax)	5 GHz 1 Wi-Fi Access Point	5 GHz 2 Wi-Fi Access Point	2.4 GHz WI-FI Access Point
Jtilities	*			Disconnected			
letwork Settings	~	Status	Connected	Disconnected	Disconnected	Disconnected	Disconnected
Date & Time	÷	Underlying Device	Network (Home/Office)	Broadband Connection (Ethernet/Coax)	Network (Home/Office)	Network (Home/Office)	Network (Home/Office)
ONS Settings	•		5 GHz 1 Wi-Fi Access Point				
Monitorina			5 GHz 2 Wi-Fi Access Point	Broadband	5 GHz 1 Wi-Fi	5 GHz 2 Wi-Fi	2.4 GHz Wi-Fi
wonitoring		Connection Type	2.4 GHz Wi-Fi Access Point	Connection (Ethernet/Coax)	5 GHz 1 Wi-Fi Access Point	5 GHz 2 Wi-Fi Access Point	2.4 GHz Wi-Fi Access Point
System Logging			Ethernet				
System-wide Connections		· · · · ·	<u>Coax</u>				
Bandwidth Monitoring		MAC Address	78:DD:12:C9:9D:A4	78:DD:12:C9:9D-A3	78:DD:12:C9:9D:A6	78:DD:12:C9:9D:A7	78:DD:12:C9:9D:A5
System		IPv4 Address	192.168.1.1			-	
		Subnet Mask	255.255.255.0				
		IPv4 Default Gateway	19216811				

#### 06 / CONFIGURING ADVANCED SETTINGS



etwork Device	Monitoring		Connections			
Fios Router	$\sim$					
	Syst	tem-widenections	•		Auto-refresh	
Status	Con	nections	5			
irewall						
Itilities	IPv4 Defa Gateway	ult 192.161	8.1.1	-	-	-
	Pv4 DNS	Address				
letwork Settings	×					
late & Time	<ul> <li>IPv4 Addr</li> <li>Distritn.</li> </ul>	ess DHCP	Server Disabl	e Disable	Disable	Disable
INS Settings	Y IPv6 Prefi	x 0/0	0/0			
Monitoring	^ IPv6 Addr	ess	0	-		
System Logging	IPv6 Link-	1 1				
System-wide Connections	Address	Local	0			
Bandwidth Monitoring	IPv6 DNS	Address	0			
System	IPv6 Addr Distrbtn.	ess Statek	ss Disabl	e Disable	Disable	Disable
	Rec'd Pac	kets 57355	0	0	0	0
erizon <sup>v</sup> Basic	Sent Pack	ets 19915	0	19096	19096	19102 <u>Ho</u> le
	Advanced	ets 19915		19096	19096	
twork Device	Advanced	> System-wide Traffic i	Jonnections	19096	19096	
twork Device Flos Router	Advanced	> System-wide Trattice	Connections	19096	19096 Auto-refresh	Helt
twork Device Flos Router	Advanced	> System-wide Traffic i	Connections	19096		Helt
terrizon <sup>4</sup> Basto 4 territe Device Flos Router tatus Irewall	Advanced	> system-wide Traffic tem-wide nections	Connections	0		Helt
twork Device Flos Router	Advanced Monitoring Sysi Con	> System-wide Traffic i tem-wide nections kets 57355	Connections		Auto-refresh	Hale
twork Device Flos Router Itatus Irewall	Advanced Monstoring Syssi Con Red Pac	> System-wide Traffic tem-wide nections kets 57355 ets 19915	Connections	0	Auto-refreah	Here 0
twork Device Flos Router Itatus Irewall Hillities Lietwork Settings	Advanced Monstoring Systi Con Red Pac Sent Pack Recd Byt	> System-wide Traffic f tem-wide mections kets 57355 ets 19915 ss 10344	0 0 0 0 0 0 0 0	0 19096 0	Auto-refreah 0 0 19096 0	0 1902 0
twork Device Fios Router tatus irewall tilities ietwork Settings ate & Time	Advanced Monitoring Syssi Com Rectil Pack	> System-wide Traffic f tem-wide mections kets 57355 ets 19915 ss 10344	0 0 0 0 0 0 0 0	0 19096	Auto-refreah 0 0 19096 0	0 1902 0
Itersk Devke Flos Router Itatus Irevali Ulities etwork Settings ate & Time NS Settings	Advanced Montoring Syssi Con Rectil Pack Rectil Pack Sent Pack Sent Byte	> System-wide Tailfiel tem-wide nections sete 57355 set 10344 s 10723	0 0 0 0 0 0 0 0	0 19096 0	Auto-refreah 0 0 19096 0	0 1902 0
teoris Device Filos Router tatus tatus titewall tillites tetwork Settings teste & Time NKS Settings tonitoring	Advanced Monstoring Syssi Con Recid Pac Sent Pack Sent Byte Sent Byte Sent Byte	> bysterwulde Tiatlic teen-wilde mections kets 57355 set 19915 se 19923 set 19923	Connections	0 19096 0 527937	Auto-refresh 0 0 19096 0 4 927957	0 19102 0 19 5280162
teoric Device Filos Router tatus tervenal tervenal tervenal tervenas tervenik Settings tervenik Settings NIS Settings System Logging	Advanced Monstoring Syssi Con Recid Pace Sent Pace Sent Byte Sent Byte Sent Byte Sent Byte	> System wide Tailfier teem-wide meetions sets 1995 s 1935 s 0 4 s 0 2 s 0 0	connections	0 19006 0 527657 0	Auto-refreah 0 0 10096 0 4 527857 0	0 19102 0 1 1 2280162 0
teach Dextor Filos Router Itatus Itewall Itellites Ietwork Settings Iset a Time NIS Settings System Logging System Logging	Advanced Mentoring Sysii CCON Redd Pack Sent Pack Sent Byte Redd Byt Redd Byt Redd Byt	> System wide Tailfier teem-wide meetions sets 1995 s 1935 s 0 4 s 0 2 s 0 0	connections	0 19096 0 527957 0 0	Auto-refreah 0 0 19996 0 4 527957 0 0 0	6 19102 19102 1 5280162 0 1 0
teach Dextue Files Router Teach Teac	Advanced Mentoring Sysii CCON Redd Pack Sent Pack Sent Byte Redd Byt Redd Byt Redd Byt	> System wide Tailfier teem-wide meetions sets 1995 s 1935 s 0 2 2 2 2 2 2 0	connections	0 19096 0 527957 0 0	Auto-refreah 0 0 19996 0 4 527957 0 0 0	6 19102 19102 1 5280162 0 1 0
twork Device Fics Router status	Advanced Mentoring Sysii CCON Redd Pack Sent Pack Sent Byte Redd Byt Redd Byt Redd Byt	> System wide Tailfier teem-wide meetions sets 1995 s 1935 s 0 2 2 2 2 2 2 0	connections	0 19096 0 527957 0 0	Auto-refreah 0 0 19996 0 4 527957 0 0 0	6 19102 19102 1 5280162 0 1 0

verizon.com/fios | ©2021 Verizon. All Rights Reserved

## MONITORING

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

#### 6.5c/ BANDWIDTH MONITORING

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

To view the bandwidth:

1. In the Monitoring section, select Bandwidth Monitoring.

twork Device		Monitoring > Ba	ndwidth Monitoring							
Fios Router	~									
itatus	~ <b>*</b>	Bandy	vidth M	onitori	ng		Auto-ref	resh 🕎		Refresh
irewali	~	Last min	1min	2min	3min	4min	5min	6min	7min	8min
Itilities	~	Tx Rate	0 kb/s	0 kb/s	0 kb/s	0 kb/s	0 kb/s	0 kb/s	0 kb/s	0 kb/s
letwork Settings	~	Rx Rate	0 kb/s	0 kb/s	0 kb/s	0 kb/s	0 kb/s	0 kb/s	0 kb/s	0 kb/s
late & Time	~	Last Hr	1hr	2hr	3hr	4hr	5hr	6hr	7hr	8hr
INS Settings		Tx Rate	0 kb/s	0 kb/s	0 kb/s	0 kb/s	0 kb/s	0 kb/s	0 kb/s	0 kb/s
Ionitoring	~	Rx Rate	0 kb/s	0 kb/s	0 kb/s	0 kb/s	0 kb/s	0 kb/s	0 kb/s	0 kb/s
System Logging	. 1									
System-wide Connection										

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

#### 6.6/ SYSTEM SETTINGS

You can configure various system and management parameters.

To configure system settings:

1. From the Advanced menu, select System.

verizon	Basic	Advanced	l .		Help	® ~
Network Device		_	System Settings			
Fios Router		~	System Settings			
Devices		v *	oystemoettings			
Parental Contr	olo	0	Router Status			î
Statue		v	Router's Hostname:	G3100		- I.
Firewall		×	Local Domain:			-1
Utilities		×	Local Domain:	myfiosgateway.com		- 1
Network Settin	ngo	~	Router			
Date & Time		~	Automatic Refresh of System Monitoring We	b Pages		
DNS Settings		~	Prompt for Password When Accessing via LA	N		
Monitoring		÷	✓ Warn User Before Configuration Changes			
System		- 1				
		- 1	Session lifetime:	7200 seconds		
			Number of concurrent users that can be logged into the router:	5 ~		
			Remote Administration			
		w	Primary HTTPS Management Port:	443		-

## SYSTEM SETTINGS

Network Device		System Settings	
Fios Router	~		
Devices	^ *	System Settings	Apply Changes
Parental Controls	o	Number of concurrent users that can be logged into the router:	s ~
Status	~		
Firewall	v	Remote Administration	
Utilities	~	Primary HTTPS Management Port:	443
Network Settings	÷	System Logging:	Enabled
Date & Time	~	Remote System Notify Level:	Error ~
DNS Settings	×	Remote System Host IP Address:	0 0 0 0
Monitoring	~		
System		Remote Security Notify Level:	None
	- 1	DHCP Timeout:	None seconds
	- 1		Warning
			Information

- 2. In the **Router Status** section, configure the following:
  - Fios Router's Hostname enter the host name or URL address of your Fios Router. Both names are the same.
  - Local Domain view the local domain of the network.
- 3. In the **Router** section, configure the following by selecting the check box:
  - Automatic Refresh of System Monitoring Web Pages activates the automatic refresh of system monitoring web pages.

- Prompt for Password when Accessing via LAN causes your Fios Router to ask for a password when trying to connect to the network.
- Warn User Before Configuration Changes activates user warnings before network configuration changes take effect.
- 4. In the **Session Lifetime** field, specify the length of time required before re-entering a user name and password after your Fios Router has been inactive.
- 5. In the Number of concurrent users that can be logged into the router field, select the number of users that can access your Fios Router at the same time.
- 6. Select **Remote Administration** to configure the remote administration to your Fios Router.
- Enter the Primary HTTP Management Port.
   Refer to 6.1p Remote Administration for using this feature.
- 8. In the **System Logging** section, configure the following system log options:
  - Enable Logging move the selector to on to activate system logging.
  - **Remote System Notify Level** specify the type of information, such as none, error, warning, and information, received for remote system logging.

## SYSTEM SETTINGS

- **Remote Security Notify Level** specify the type of information, such as none, error, warning, and information, received for remote system logging.
- **Remote System Host IP Address** enter the IP address of system log server for Security Logging messages.
- 9. In the **DHCP Timeout** section, specify the DHCP timeout.
- 10. Click Apply changes to save changes.

# 

- **7.0** Troubleshooting Tips
- 7.1 Frequently Asked Questions

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

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

## **TROUBLESHOOTING TIPS**

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

#### 7.0/ TROUBLESHOOTING TIPS 7.0a/ IF YOU ARE UNABLE TO CONNECT TO THE INTERNET:

- The first thing to check is whether your Fios Router is powered on and is connected to the internet. Check the Router Status LED on the front of the Fios Router. Be sure to refer to the "1.3a/ FRONT PANEL" on page 9 to determine status of the Fios Router. Check the WAN cable (Ethernet or coaxial) connecting your Fios Router to the internet to make sure it is properly connected on both ends.
- If the prior tips do not resolve your connection issue, try restarting (rebooting) the router portion of the Fios Router by manually pressing the 'red' reset power button on the rear panel of the Fios Router for 2-4 seconds (the Router Status LED should go off) to begin rebooting your Fios Router. Your Fios Router will begin rebooting and will return to service in 3 5 minutes depending on your network connection. Check Router Status LED and if it is solid white, try again to access the internet.

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

#### 7.0b/ IF YOU ARE UNABLE TO CONNECT TO YOUR FIOS ROUTER USING WI-FI:

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

## **TROUBLESHOOTING TIPS**

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

#### 7.0c/ ACCESSING YOUR FIOS ROUTER IF YOU ARE LOCKED OUT

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

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

- Scheduler If a schedule has been created that applies to the computer over the connection being used, your Fios Router will not be accessible during the times set in the schedule.
- Access Control If the access control setting for the computer is set to block the computer, access to your Fios Router is denied.

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

#### 7.0d/ RESTORING YOUR FIOS ROUTER'S DEFAULT SETTINGS

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

For additional information regarding the Restore Defaults feature, refer to section 6.1/ Utilities/Save And Restore.

- Using the tip of a ballpoint pen or pencil, press and hold the Reset button on the back of your Fios Router for three seconds.
- Access the UI and navigate to the Advanced Settings page. Select the 6.1j Save and Restore option. After saving your configuration, if desired, click the Restore Factory Defaults radio button. For additional details, refer to the 6.1/ Utilities/Save And Restore section of this guide.

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

#### 7.0e/ LAN CONNECTION FAILURE

#### To troubleshoot a LAN connection failure:

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

## **TROUBLESHOOTING TIPS**

• Confirm that the computer and Fios Router are both on the same network segment.

If unsure, let the computer get the IP address automatically by initiating the DHCP function, then verify the computer is using an IP address within the default range of 192.168.1.2 through 192.168.1.254. If the computer is not using an IP address within the correct IP range, it will not connect to your Fios Router.

• Verify the subnet mask address is set to 255.255.255.0.

#### 7.0f/ TIMEOUT ERROR OCCURS WHEN ENTERING THE URL OR IP ADDRESS

#### Verify the following:

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

For connections experiencing lag or a slow response:

- Check for other devices on the network utilizing large portions of the bandwidth and if possible temporarily stop their current utilization and recheck the connection.
- If lag still exists, clear the cache on the computer and if still needed, unplug the Ethernet cable or disable the Wi-Fi connection to the computer experiencing the slow connection and then reconnect or enable the Wi-Fi connection and try the connection again.

In rare cases you may also need to:

- Unplug the Ethernet cable to Fios Router and restart the Fios Router, wait 1-2 mins. and insert the Ethernet cable again.
- Under limited circumstances you may use a port forwarding configuration on the router, based on the application you are using (refer to the 6.0d/ Port Forwarding section or Verizon's support online help for more details).

#### 7.0g/ FRONT UNIFIED BUTTON

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

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

## **TROUBLESHOOTING TIPS**

#### 7.0h/ REAR LIGHTED INDICATORS

#### **Flash Speed**

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

#### **WAN Ethernet**

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

#### LAN Ethernet – Upper LED

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

#### LAN Ethernet – Lower LED

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

#### LAN Coax

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

#### **WAN Coax**

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

#### 7.1/ FREQUENTLY ASKED QUESTIONS

#### 7.1a/ I'VE RUN OUT OF ETHERNET PORTS ON MY FIOS ROUTER. HOW DO I ADD MORE COMPUTERS OR DEVICES?

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

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

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

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

## **FREQUENTLY ASKED QUESTIONS**

#### 7.1b/ HOW DO I CHANGE THE PASSWORD ON MY FIOS ROUTER UI?

To change the password:

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

#### 7.1c/ IS THE WI-FI OPTION ON BY DEFAULT ON MY FIOS ROUTER?

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

## 7.1d/ IS THE WI-FI SECURITY ON BY DEFAULT WHEN THE WI-FI OPTION IS ACTIVATED?

Yes, with the unique WPA2 (Wi-Fi Protected Access II) key that is printed on the sticker on the rear panel of your Fios Router.

#### 7.1e/ ARE MY FIOS ROUTER'S ETHERNET PORTS AUTO-SENSING?

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

## 7.1f/ CAN I USE AN OLDER WI-FI DEVICE TO CONNECT TO MY FIOS ROUTER?

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

#### 7.1g/ CAN MY WI-FI SIGNAL PASS THROUGH FLOORS, WALLS, AND GLASS?

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

#### 7.1h/ HOW DO I LOCATE THE IP ADDRESS THAT MY COMPUTER IS USING?

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

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

## **FREQUENTLY ASKED QUESTIONS**

To find the IP address from the router GUI:

- 1. From the **Basic** menu, select **Devices** from the left pane.
- 2. Select **Expanded List** from the dropdown list to view detailed IP address information for all connected devices.

#### 7.1i/ I USED DHCP TO CONFIGURE MY NETWORK. DO I NEED TO RESTART MY COMPUTER TO REFRESH MY IP ADDRESS?

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

## 7.1j/ I CANNOT ACCESS MY FIOS ROUTER UI. WHAT SHOULD I DO?

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

#### 7.1k/ I HAVE A FTP OR WEB SERVER ON MY NETWORK. HOW CAN I MAKE IT AVAILABLE TO USERS ON THE INTERNET?

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

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

#### 7.11/ HOW MANY COMPUTERS CAN BE CONNECTED THROUGH MY FIOS ROUTER?

Your Fios Router is capable of 254 connections, but we recommend having no more than 132 connections. As the number of connections increase, the available speed for each computer decreases.

## 08/ Specifications

- 8.0 General Specifications
- 8.1 LED Indicators
- 8.2 Environmental Parameters

181

The specifications for your Fios Router are as follows.

This includes standards, cabling types and environmental parameters.

## **GENERAL SPECIFICATIONS**

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

#### **8.0/ GENERAL SPECIFICATIONS**

Model Number:	G3100
Standards:	IEEE 802.3x, 802.3u
	IEEE 802.11a/b/g/n/ac/ax
IP:	IP versions 4 and 6
MoCA WAN:	975 - 1025 MHz 175 Mbps
MoCA LAN:	1125 – 1675 MHz 2500 Mbps
Speed:	Wired WAN Ethernet: 10/100/1000 Mbps auto-sensing
	Wired LAN Ethernet: 10/100/1000 Mbps auto-sensing
	Cabling Type: Ethernet 10BaseT: UTP/STP Category 3 or 5
	Ethernet 100BaseT: UTP/STP Category 5
	Ethernet 1000BaseT: UTP/STP Category 5e
Firewall:	ICSA certified

#### 183

#### 8.1/ LED INDICATORS

Front Panel: Unified Button: Router Status LED

Rear Panel:

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

#### 8.2/ ENVIRONMENTAL PARAMETERS DIMENSIONS AND WEIGHT

Fios Router (unit only):

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

Weight: 2.50 lbs / 1.138 kg

Complete System (inc. packaging):

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

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

Power:

External, 12V, 3.5A al): PH TP+N: 0.157" x 0.984"

Screws (optional):

Certifications:

FCC, UL 60950-1

Anchor PE: 0.197" x 0.984"

### **ENVIRONMENTAL PARAMETERS**

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

## 09/ Notices

9.0 Regulatory Compliance Notices

09 / NOTICES



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

#### 9.0/ REGULATORY COMPLIANCE NOTICES 9.0a/ Class B Equipment

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

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

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

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

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

RF Exposure:

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

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

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

This device is restricted for indoor use.

## **REGULATORY COMPLIANCE NOTICES**

#### 9.0b/ Safety Warning:

- 1. The circuit of cable distribution system under consideration is TNV-1 circuit.
- 2. The common sides or earthed side of the circuit are connected to the screen of the coaxial cable through an antenna connector of tuner and to all accessible parts and circuits (SELV, LCC and accessible metal parts).
- 3. The screen of the coaxial cable is intended to be connected to earth in the building installation.

#### 9.0c/ Alerte de sécurité:

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

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

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

#### 9.0d/ NEBS (Network Equipment Building System) Statement

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

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

## **REGULATORY COMPLIANCE NOTICES**

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

#### 9.0e/ GENERAL PUBLIC LICENSE

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

http://verizon.com/opensource/

All open source software contained in this product is distributed WITHOUT ANY WARRANTY. All such software is subject to the copyrights of the authors and to the terms of the applicable licenses included in the download.

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

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

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