



Wireless Gateway

User Guide



Table of Contents

About Your Wireless Gateway	1
Overview	2
Front Panel	2
Rear Panel	3
Top Panel	4
Bottom Panel	4
Bottom Label	5
Set Up	6
Step 1. Locate Your Wireless Network Info	6
Step 2. Connect Your WiFi Devices.....	7
Step 3. Secure Your Wireless Gateway Admin Tool	8
Network Settings.....	10
Setting up WiFi Connection Using WPS.....	11
Web Management Interface	13
At a Glance	14
Connection	15
Status.....	15
Local IP Configuration	16
Connection WiFi	17
XFINITY Network.....	19
Firewall	20
Software	21
Hardware	22
System Hardware	22
Battery	23
LAN Ethernet	24
Hardware WiFi	25
Wizard	26
Connected Devices	27

Computers	27
Parental Control	29
Managed Sites	29
Blocked Sites	30
Blocked Keywords	31
Managed Services	32
Blocked Services	33
Managed Devices	34
Reports	36
Advanced	37
Port Forwarding	37
Port Triggering (not available at this time)	38
DMZ	39
Device Discovery	40
Troubleshooting	41
Logs	41
Diagnostic Tools	42
Restore/Reset Gateway	43
Change Password	44
Appendix	45
Glossary	45
Table Reference	46
Figure Reference	47
Regulatory Information	49
Compliance Statements	49
FCC Interference Statement	49
FCC Part 68 Statement	50

About Your Wireless Gateway

The XFINITY Wireless Gateway is your all-in-one device that connects your Internet, phone, and home networking. It provides WiFi connectivity for your home, so there's no need for a separate wireless router.

Here's what you get when you subscribe to both XFINITY Voice and Internet services:

- **WiFi Access** — WiFi uses radio frequency to connect computers and other devices to a network without wires. Your Wireless Gateway can connect to b/g/n clients simultaneously.
- **Fast Download Speed** — Your Wireless Gateway is DOCSIS 3.0 compliant with speeds up to eight times faster than DOCSIS 2.0 cable modems.
- **Easy Connectivity** — Connect any WPS-compatible computer or device with just one button.
- **Security** — Because WiFi networks send information over radio waves, signals from your wireless network can be intercepted by unauthorized users. Use the simple Home Network Wizard to securely set up your WiFi broadband connection for WiFi enabled devices.
- **Convenience** — Simultaneously use four Ethernet ports for wired devices and 802.11b/g/n connectivity for wireless devices. Choice between wireless LAN (WLAN) or wired Ethernet LAN connections.
- **Flexibility** — Ability to support two lines of telephone service, as well as high-speed data; the ability to use your existing router with your Wireless Gateway.
- **Battery Back-up** — Lithium Ion battery back-up (up to 5 hours talk time and 8 hours standby time).
Note: Battery back-up is only available if you subscribe to XFINITY Voice service.
- **Advanced Features** — Advanced routing features of the Wireless Gateway include:
 - Parental Controls
 - WiFi Protected Setup (WPS)
 - Firewall
 - Port Forwarding & Blocking

Note: If you haven't already done so, please activate both XFINITY Voice and Internet services if you subscribe to both, or just XFINITY Internet services if you subscribe only to high-speed data services. Refer to the user guide you received with each of these services for activation instructions and information about XFINITY Voice and Internet features.

Overview

FRONT PANEL

The front panel, featuring a set of LED indicators, shows the status of your Wireless Gateway. Being familiar with these indicators can help with troubleshooting.



Fig. 1

Table 1

LED	Front Panel LED Indicators
Power	Blinking=power failure and during battery backup ON=power being supplied OFF=power is not being supplied
US/DS	Blinking=ranging is in progress ON=ranging is complete on 1 channel only OFF=scanning for DS channel
Online	Blinking=cable interface is acquiring IP address, Time of Day, Cable Modem configuration ON=device is online OFF=device is offline
WiFi	Blinking=transmitting data to the WiFi interface ON=WiFi is enabled OFF=WiFi is disabled
Tel1	Blinking=Tel line 1 is in use ON=Tel 1 port is online OFF=Tel 1 port is offline
Tel2	Blinking=Tel line 2 is in use ON=Tel 2 port is online OFF=Tel 2 port is offline
Battery	Solid Glow=battery is charging Blinking=battery power is low; use AC power as soon as possible ON=operating on AC power, battery not charging OFF=(a) If Battery LED is off and Power LED is blinking, then device is in battery backup mode. (b) When Battery LED is off and Power LED is solid, no battery is installed or is not functioning properly.

REAR PANEL

The rear panel of your Wireless Gateway features a Reset button, as well as ports for attaching the supplied power adapter and connecting additional devices.

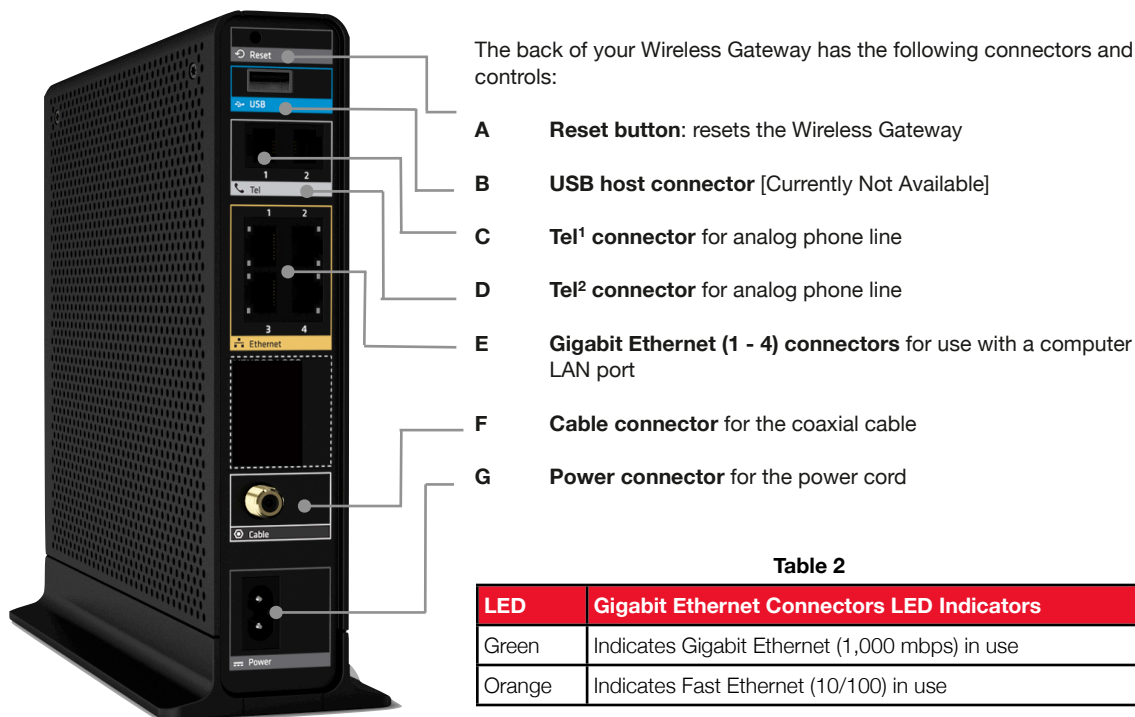


Fig. 2

Reset Button (Recessed to protect against accidental reset)

Pressing the Reset button for varying lengths of time performs two types of reset operations.

- **Normal Reset** – reboots the Wireless Gateway but retains current configuration settings.
Use a thin object, press the Reset button for 2-5 seconds and release.
- **Factory Reset** – deletes all changes made to the original configuration settings and restores the Wireless Gateway to the factory configuration.
Use a thin object, press and hold the Reset button for at least 15 seconds or more before releasing.

You can also reset your Wireless Gateway using the *Web Management Interface* at <http://10.0.0.1>.

Note: If you select Restore Factory Settings, be certain you want to reset ALL settings (such as passwords, parental controls and firewall settings) before proceeding! All customized settings made to your Wireless Gateway will be lost. Also, a Factory Restore will take your Wireless Gateway out of Bridge Mode if it had been previously enabled. Call 1.800.XFINITY to re-enable Bridge Mode.

TOP PANEL

The top panel of your Wireless Gateway features a **WPS** button (Fig. 3). **WPS** (or WiFi Protection Setup) enables you to securely set up a WiFi network without entering the Network Key.

BOTTOM PANEL

The bottom panel of your Wireless Gateway has a panel for the battery (for XFINITY Voice Service only). View battery status by accessing the Battery menu from the Web Management Interface at <http://10.0.0.1>. The battery will provide backup for voice service in case of a power outage, but is not intended to replace the AC power for an extended period.



Fig. 3

To install a battery, follow these steps:

1. Place the Wireless Gateway sideways on a table.
2. Remove the battery cover on the bottom panel and set it aside.
3. Insert the battery in the battery compartment with the corresponding polarity correctly in place.
4. Replace the battery cover.

A battery is needed to enable voice service availability in the event of a power outage. A battery is available for your Wireless Gateway *only if you subscribe to XFINITY Voice*. If you are an XFINITY Voice subscriber and you did not receive a battery, please call 1.800.XFINITY.

Note: Do not unplug the power cord of your Wireless Gateway for an extended period. If left unplugged and the battery power is drained, you will not be able to make any phone calls, including 911 emergency calls.

BOTTOM LABEL

The label on the underside of the Wireless Gateway provides important information you may need to manually connect wireless products to your home network.

Table 3

Network Name (SSID)	HOME - XXXX (where XXXX is the last 4 digits of the Cable Modem MAC)
Encryption	WPAWPA2-PSK (TKIP/AES)
Network Key	[Printed on the label]
WPS PIN	[Printed on the label]

DEFAULT CONFIGURATIONS

Following are the factory default configurations for the Wireless Gateway. You may want to change some settings (for advanced users).

Table 4

WPS	Enabled
Gateway IP	http://10.0.0.1
User Name	admin (not case-sensitive)
Password	password (case-sensitive)
Firewall Configuration	Low (allows most traffic)
UPnP	Enabled
All other features are disabled by default. In order to enable and modify other features, use the Administration site at http://10.0.0.1 .	

Set Up

The XFINITY Wireless Gateway is your all-in-one device that connects your Internet, phone, and home networking. It provides WiFi connectivity for your home, so there's no need for a separate wireless router. The Wireless Gateway includes the following advanced features:

- Parental Controls
- WiFi Protected Setup (WPS)
- Firewall
- Port Forwarding & Blocking

For WPS-compatible products, see *Setting up WiFi Connection Using WPS*.

If your computer is already connected to the Internet, skip this section.

STEP 1. LOCATE YOUR WIRELESS NETWORK INFO

Lift the Wireless Gateway and look for the white label located on the underside (Fig. 4).



Fig. 4

You'll need the Wireless Network Name (SSID) and Password to connect your various WiFi devices.

Once you've located the Wireless Network Name and Password, write them down for future reference:

Wireless Network Name (SSID) _____

Wireless Password (Network Key) _____

STEP 2. CONNECT YOUR WIFI DEVICES

Now that you've found your Network Name and Password (SSID and Network Key), it's time to connect your Wi-Fi enabled devices (laptops, smartphones, e-readers, gaming systems, etc). The following chart contains basic instructions on how to connect popular devices to a wireless network. However, keep in mind, certain devices may require different wireless connection steps.

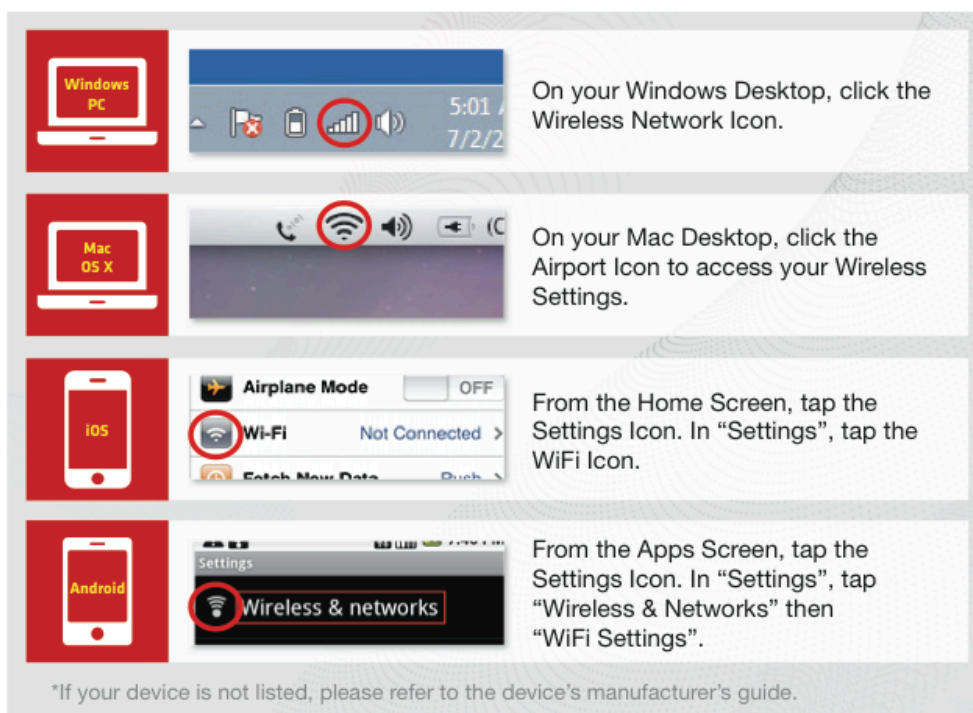


Fig. 5

1. In the list of available wireless networks, select the Wireless Network Name (SSID) you wrote down.
2. Enter the Wireless Network Password (case-sensitive) in the Network Key field (Windows) or Password field (Mac).
3. Click the confirmation button (typically labeled **OK**, **CONNECT**, or **JOIN**).
4. Test your Internet connection by opening a web browser and typing in a valid URL.
5. Repeat these steps for each wireless device you want to connect to your network.

If you need help with your WiFi connection, the following links to popular operating systems may help.

- Windows 7®
<http://windows.microsoft.com/en-US/windows7/Add-a-device-or-computer-to-a-network>
- Windows Vista®
<http://windows.microsoft.com/en-us/windows-vista/Setting-up-a-wireless-network>
- Apple Mac OS® X v10.5 or greater
<http://support.apple.com/kb/HT2497>

STEP 3. SECURE YOUR WIRELESS GATEWAY ADMIN TOOL

Using the Admin Tool, you can access your Wireless Gateway to update or change security settings and other advanced features. To ensure better security for your Wireless Gateway and home network, **we recommend changing the password in the Admin Tool.**

A. Log In Using the Default Gateway Name and Password

1. Open a web browser from a device connected to the Wireless Gateway and type `http://10.0.0.1` in the address line. The login page appears.
2. Enter **admin** and **password** as shown (Fig. 6).
3. Click **LOGIN**.

Please login to manage your router.

Username: **admin**

Password: **password**

LOGIN

Fig. 6

Note: Username CANNOT be changed and will always be 'admin'.

4. The *At a Glance* page will (Fig. 7) appear. Click **Change Password** on the top right.



Fig. 7

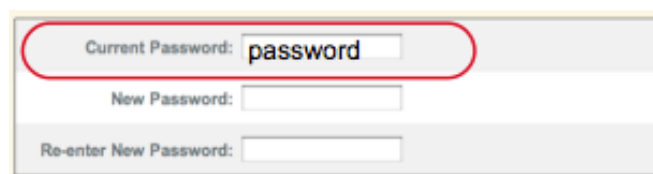
B. Change Admin Password for Better Security (Recommended)

By changing the default password for the Admin site, you'll secure the management of your Wireless Gateway. You'll need this personalized password to change your network settings in the future.

Note: If you forget your password, you'll need to do a Factory Reset and restore the Wireless Gateway default settings.

1. Enter **password** as shown (Fig. 8).
2. Create a new password of your choice.

Note: All passwords must be at least 8 characters. It should contain both upper and lower case letters and at least one number.



The screenshot shows a web form for changing the admin password. It has three input fields: 'Current Password:' with the text 'password' entered, 'New Password:', and 'Re-enter New Password:'. A red oval highlights the 'Current Password' field.

Fig. 8

3. Re-enter your new password.
4. Click **SAVE**.

Your settings should now be saved. To view or modify your Wireless Gateway settings in the future, go to <http://10.0.0.1>.

Write down your Admin Tool Password for future reference:

NETWORK SETTINGS

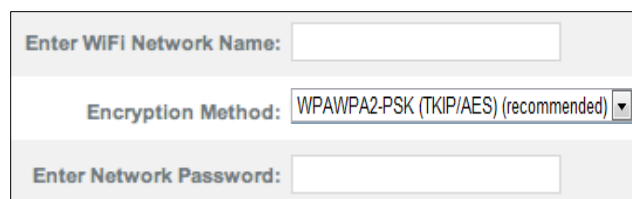
The Wireless Gateway has a uniquely generated WiFi Network Name (SSID) and Network Key (Password) for better wireless security. **Comcast recommends keeping the default settings.** If you forget them, you can find them on the bottom label of the Wireless Gateway.

Note: If you do change the settings, the SSID/Password on the bottom label of the device will no longer apply. If you forget this information, you'll need to do a Factory Reset.

The following provides information for changing the Wireless Gateway SSID/Password and Encryption Method settings.

WiFi Network Name (SSID)

- Enter a new *WiFi Network Name* (Fig. 9). The new name will appear in the list of available wireless networks.
- For future reference, write your *WiFi Network Name* (SSID) here:



The screenshot shows a web-based configuration interface for a wireless gateway. It contains three main sections: 'Enter WiFi Network Name:' with a text input field, 'Encryption Method:' with a dropdown menu currently set to 'WPAWPA2-PSK (TKIP/AES) (recommended)', and 'Enter Network Password:' with a text input field.

Fig. 9

Encryption Method

The encryption method secures data between your computers and the Wireless Gateway. The default setting, *WPAWPA2-PSK (TKIP/AES)*, is compatible with most computers and provides the **best security and performance**.

To view or modify your Wireless Gateway settings in the future, go to <http://10.0.0.1>.

This complete User Guide, as well as the Wireless Gateway Quick Start Guide, can be found at <http://customer.comcast.com/userguides>.

For help with your XFINITY services and features, refer to the appropriate user guide or call 1.800.XFINITY.

SETTING UP WIFI CONNECTION USING WPS

- WPS (WiFi Protected Setup) lets you easily set up secure WiFi networks without entering a Network Key.
- Most WPS-compatible devices will work with your Wireless Gateway. You can easily connect to your WiFi Network using either the default Push Button Configuration (PBC) or the Personal Identification Network (PIN) method. Both methods are described below.
- If you aren't sure if your computer supports WPS, look for a WPS sticker or label (Fig. 10) on your computer or device. If none is found, your computer is probably NOT compatible with WPS. In this case, follow the steps under WiFi Connection.



Fig. 10

WPS via PBC Connectivity/One Button Connectivity (Recommended)

1. Press the WPS button on your computer or wireless product. (If your computer doesn't have a physical button, refer to your computer's user guide to enable WPS.)
2. Within 2 minutes, press the WPS button on the top of your Wireless Gateway. (Fig. 11)
3. After a message displays that the connection was successful, your computer/device is connected to your home network.

Note: When the WPS button is pressed, it will stay lit for 5 minutes (regardless of whether or not the connection was successful). Please wait until the light turns off before retrying or connecting another WPS product.



Fig. 11

WPS via PIN Connectivity

1. Open your computer's WPS utility and acquire a PIN number. Make a note of the PIN number. The WPS utility will begin its countdown to 2 minutes.
2. Launch your web browser and type <http://10.0.0.1> in the address line.
3. Log in using **admin** as the username and the password (if you did not change it, use **password**).
4. Select *Gateway > Connection > WiFi*.
5. Before the WPS Utility finishes its countdown, enter the PIN number from Step 1 above in the *Enter Wireless Client's PIN* field.
6. Click **PAIR WITH MY WIFI CLIENT**.
7. Your computer will communicate with your Wireless Gateway and establish a connection.

Note: If your WPS client prompts you to enter the Wireless Gateway's PIN during the WPS Connection, enter the WPN printed on the label on the underside of your Wireless Gateway.

Table 5

Web Management Interface Menus

Access Menus and Submenus	Description
Gateway > At a Glance	Displays information about your home network, connected devices and recent network updates
Gateway > Connection > Status	Displays overall summary of XFINITY, Local IP, and WiFi networks
Gateway > Connection > XFINITY Network	View XFINITY network settings and initialization procedures for cable modem, downstream and upstream information
Gateway > Connection > Local IP Network	View and reset your local IPv4 settings
Gateway > Connection > WiFi	View and edit your wireless settings
Gateway > Firewall	Configure the security level of the internal firewall
Gateway > Software	View software information version information
Gateway > Hardware > System Hardware	View information about the system hardware
Gateway > Hardware > Battery	View information about the internal battery (for XFINITY Voice only)
Gateway > Hardware > LAN	View the link status and MAC address for each of the 4 Ethernet ports
Gateway > Hardware > Wireless	View the status and MAC address of the WiFi port
Gateway > Wizard	Helps you set up your home network
Connected Devices > Computers	View computers connected to the Gateway's LAN
Parental Control > Managed Sites	Blocked sites, blocked keywords and trusted computers
Parental Control > Managed Services	Blocked services and trusted computers
Parental Control > Managed Devices	Managed and blocked devices
Parental Control > Reports	Generate reports containing selected Log Messages
Advanced > Port Forwarding	Enable/disable the port forwarding feature
Advanced > Port Triggering	Enable/disable the port triggering feature
Advanced > DMZ	Enable/disable the demilitarized zone feature
Advanced > Device Discovery	Enable/disable the Universal Plug and Play (uPnP) feature
Troubleshooting > Logs	Configure log filters and download/print system logs
Troubleshooting > Diagnostic Tools	Test connectivity to an URL or IP address
Troubleshooting > Restore/Reboot Gateway	Reset the Wireless Gateway or restore to factory settings
Troubleshooting > Change Password	Change the password for the Web Management Interface

WEB MANAGEMENT INTERFACE

You can view or modify basic information about your Wireless Gateway by accessing the Web Management Interface.

Status Icons

- ▶ Percentage of battery power remaining
- ▶ Gateway's Internet
- ▶ Status of the Gateway's wireless connection
- ▶ Firewall security level access
 - ✗ indicates low/custom settings
 - ✓ indicates medium or high settings

- ▶ Log in/out
- ▶ Change password

Select a category to view or configure settings.

When you click a category from the left menu bar, related information appears here.

From the links at the bottom of the page, you can access XFINITY.com, Customer Central and this user guide.

Fig. 12

AT A GLANCE

View information about the Wireless Gateway and edit configurations of connected devices

Access from the left navigation menu:

Gateway > At a Glance

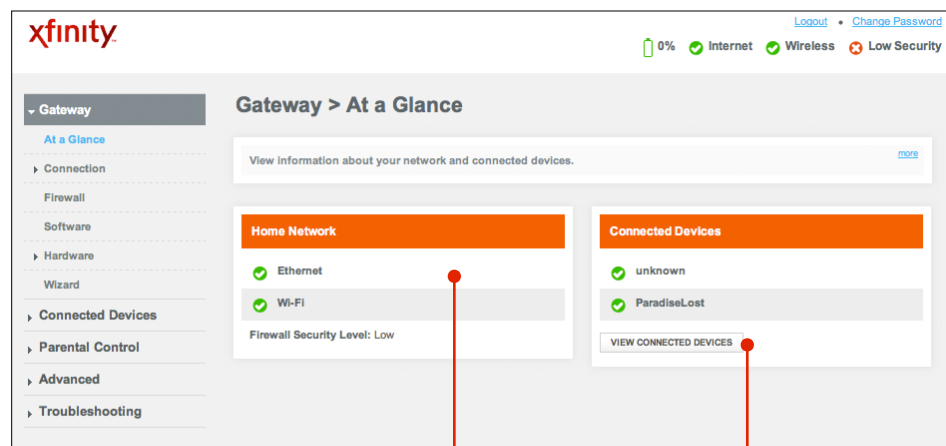


Fig. 13

The **Home Network** section displays the states of both the Ethernet (wired) and WiFi (wireless) networks. You can see connected computers and devices.

Click **View Connected Devices** to view online and offline devices that are connected to your Wireless Gateway.

If you would like to use your existing router instead of the routing functionality on your Wireless Gateway, the Bridge Mode on the Wireless Gateway will need to be enabled. A Comcast technician can do this during installation, or call 1.800.XFINITY to enable this functionality.

CONNECTION

View information about your Connection Status, such as Local Configuration, WiFi, and the XFINITY Network

Access from the left navigation menu:

Gateway > Connection

Status

Displays a summary of your Local IP, WiFi and XFINITY networks

Access from the left navigation menu:

Gateway > Connection > Status

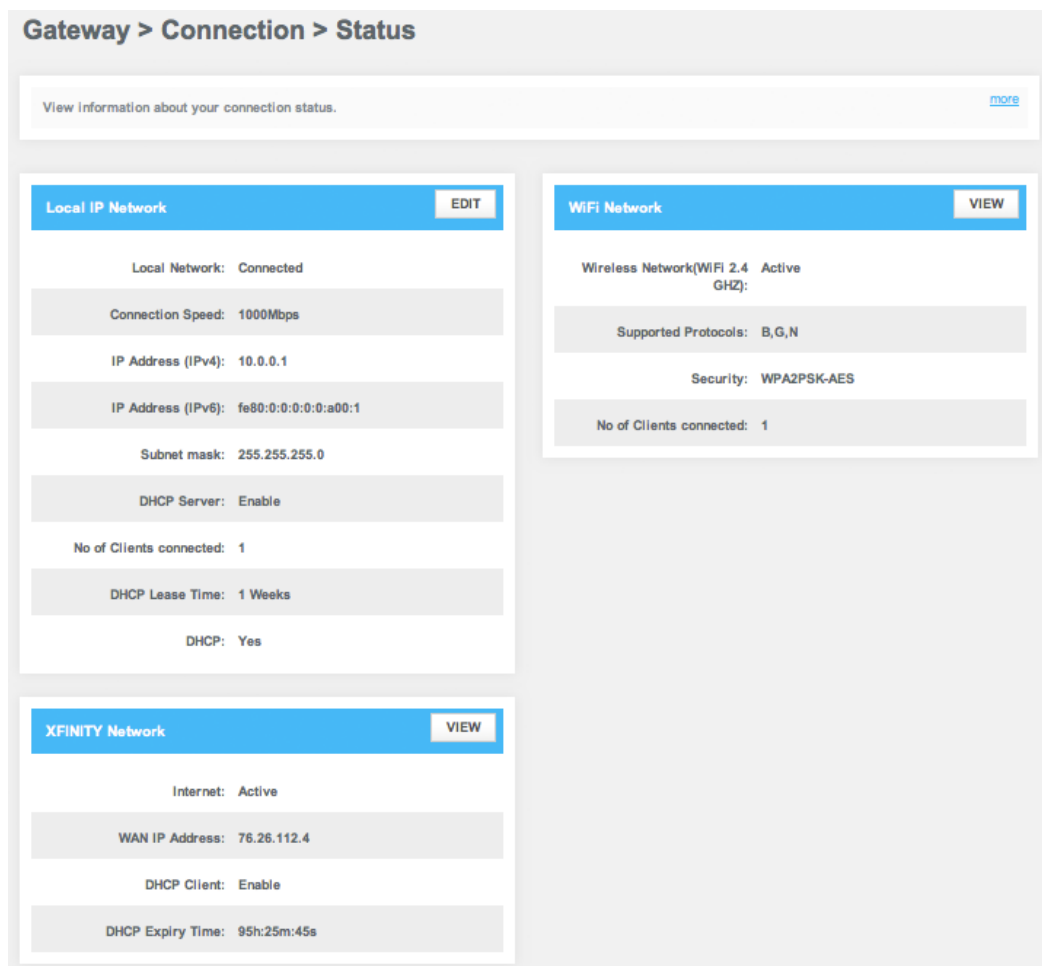


Fig. 14

Local IP Configuration

View information about your local network and edit the LAN DHCP settings (for advanced users)

Access from the left navigation menu:

*Gateway > Connection > Local IP Network (or click **EDIT** from Gateway > Connection > Status)*

Fig. 15

Table 6

Field	Description
IPv4	
Gateway Address	Local IP address of the router
Subnet Mask	Subnet address for the LAN (3 subnets to choose from)
DHCP Beginning Address	First available Local IP Address in the DHCP pool
DHCP Ending Address	Last available Local IP Address in the DHCP pool
DHCP Lease Time	Length of time a local device retains an IP Address before checking back with the DHCP Server on the Wireless Cable Modem

Note: IPv6 parameters are not configurable at this time.

Connection WiFi

Modify the WiFi settings of your network computers or add additional devices to your network

Access from the left navigation menu:

*Gateway > Connection > WiFi (or click **VIEW** from Gateway > Connection > Status)*



Fig. 16

Click **EDIT** to modify your 2.4 GHz Network settings.

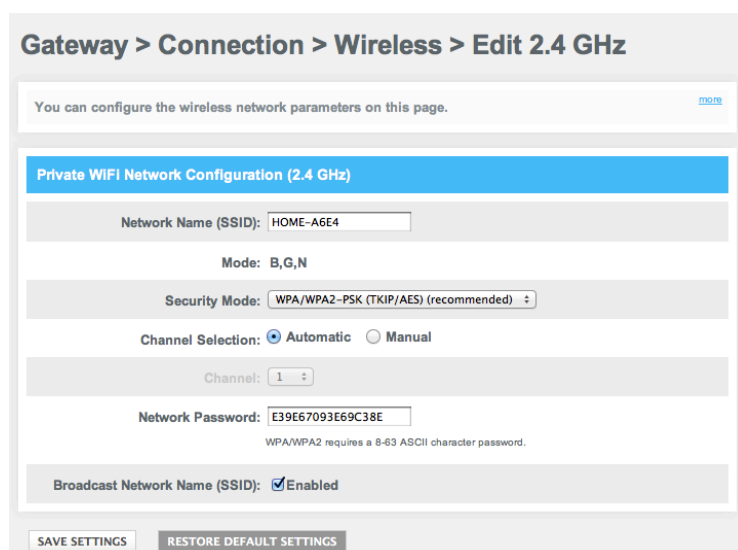


Fig. 17

Click **Add WiFi Protected Setup (WPS) Client** to connect a WiFi device (WPS-capable) to your network. The **Add Wireless Client** (Fig. 19) screen will appear.

Gateway > Connection > Wireless > Add Wireless Client

Use WPS (WiFi Protected Setup) to simplify your WiFi setup. [more](#)

Add Wireless Client (WPS)

WiFi Protected Setup (WPS): **Enabled** Disabled

Security: WPA2PSK

Encryption: AES

Network Password: comcast123

Connection Options: **Push Button** ▾

To pair, select the Pair button and your wireless device will connect within two minutes. You may also press the [pair] button on this device.

PAIR **CANCEL**

Fig. 18

XFINITY Network

View details (refreshed every 10 seconds) about the XFINITY Network, including initialization procedures, cable modem settings, downstream and upstream information

Access from the left navigation menu:
Gateway > Connection > XFINITY Network (or click **VIEW** from *Gateway > Connection > Status*)

Gateway > Connection > XFINITY Network

View technical information related to your XFINITY network connection.

XFINITY Network

Internet: Active

System Uptime: 000 days 01h:30m:17s

WAN IP Address: 76.26.112.4

DHCP Client: Enable

DHCP Expiry Time: 95h:01m:09s

WAN MAC: 00:22:2D:9D:B5:53

eMTA MAC: 00:22:2D:9D:B5:51

CM MAC: 00:22:2D:9D:B5:50

Initialization Procedure

Initialize Hardware: Complete

Acquire Downstream Channel: Complete

Upstream Ranging: Complete

DHCP Bound: Complete

Set Time-of-Day: Complete

Configuration File Download: Complete

Registration: Complete

Cable Modem

HW Version: 1A

Vendor: SMC Networks

BOOT Version: PSPU-Boot(BBU) 1.0.9.15-H2.6

Core Version: 2.1.2.5

Model: SMC-D3GNV

Product Type: SMC-D3GNV

Flash Part: 32 MB

Download Version: 2.1.2.5

Serial Num: H2A091D7A1

Downstream

	Channel Bonding Value							
Index	1	2	3	4	5	6	7	8
Lock Status	Locked	Locked	Locked	Not locked	Not locked	Not locked	Not locked	Not locked
Frequency	-1244.925 Mhz	-1238.924 Mhz	-1232.927 Mhz					
SNR	31.763 dB	32.321 dB	32.237 dB					
Power	8549913.000 dBmV	8254806.500 dBmV	7959927.000 dBmV					
Modulation	256 QAM	256 QAM	256 QAM					

Upstream

	Channel Bonding Value			
Index	1	2	3	4
Lock Status	Locked	Not locked	Not locked	Not locked
Frequency	23199634 Hz			
Symbol Rate	5120 KSym/sec			
Power Level	58.2100 dBmV			
Modulation	16QAM			
Channel ID	1			

If you need to contact XFINITY for support, you may be asked to provide information displayed on this screen.

Fig. 19

FIREWALL

View and modify Firewall settings to block unauthorized/unsafe traffic from accessing your network

Access from the left navigation menu:

Gateway > Firewall

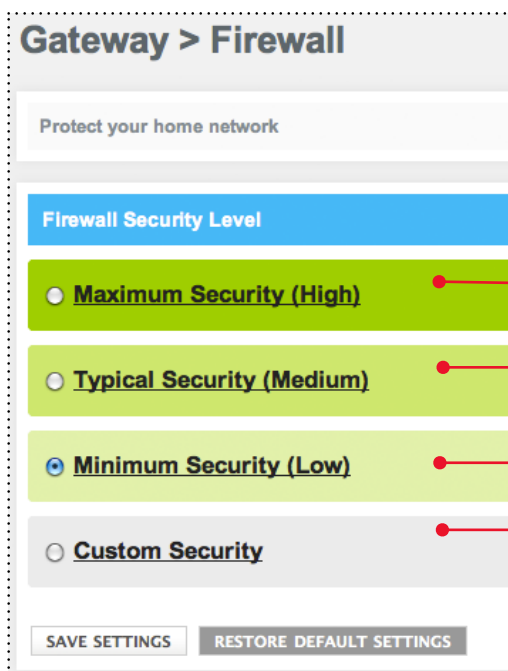
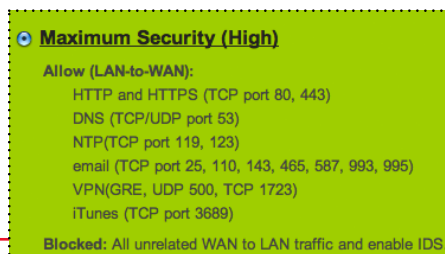
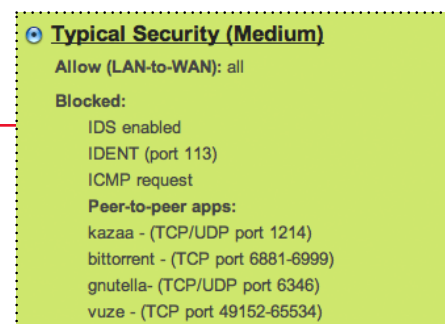


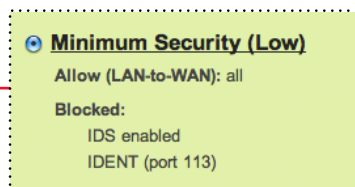
Fig. 20



Most applications are blocked except for browsing, email, iTunes and VPN. Fig. 21



All peer-to-peer apps are blocked. Fig. 22



Minimum Security is the default setting. All secure apps are enabled. Fig. 23

To block a specific TCP/UDP port, please use **Managed Services** under **Parental Control**.

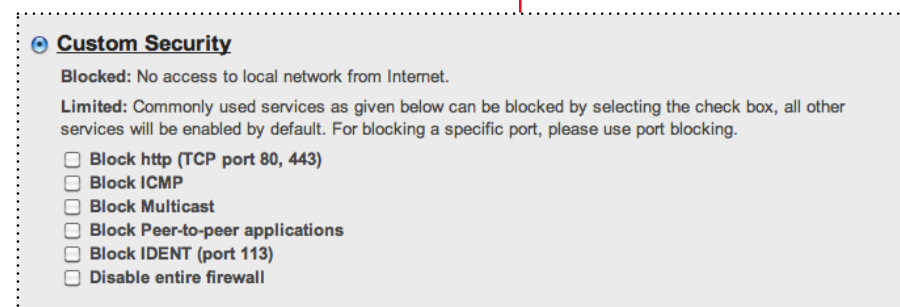


Fig. 24

SOFTWARE

View details about your Wireless Gateway's current software

Access from the left navigation menu:

Gateway > Software

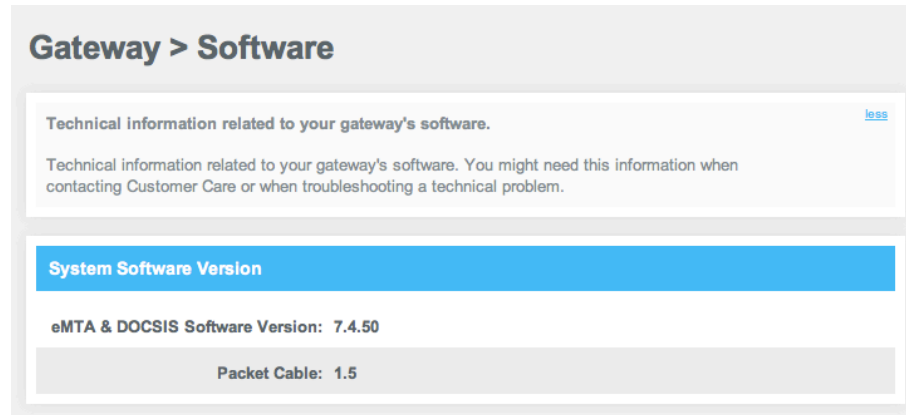


Fig. 25

HARDWARE

View your Wireless Gateway's hardware details: System Hardware, Battery, LAN Ethernet, and WiFi

System Hardware

Access from the left navigation menu:

Gateway > Hardware > System Hardware

Gateway > Hardware > System Hardware

Information related to the gateway hardware. [more](#)

System Hardware

Model: SMC-D3GNV

HW Identifier: 1A

Serial Number: H2A091D7A1

Processor Speed: 400 MHz

DRAM: 128 MB

Flash: 32 MB

Fig. 26

Battery

View the battery specifications

Access from the left navigation menu:

Gateway > Hardware > Battery

Hardware > Battery

View the battery status and details of your Wireless Gateway.

Battery

Power status:	AC Power
Battery Installed:	No
Battery Condition:	Unknown
Remaining Charge:	0 mAh
Remaining Time	1 min
Battery Model Identifier:	D3 DORY -Rev A
Battery Serial Number:	N/A

Fig. 27

LAN Ethernet

View information about all connected *wired* computers and devices

Access from the left navigation menu:

Gateway > Hardware > LAN

Gateway > Hardware > LAN Ethernet

Your Wireless Gateway supports 4 Gigabit Ethernet Ports (GbE) [more](#)

<div>LAN Ethernet Port 1</div> <div> LAN Ethernet link Active status: </div> <div>MAC Address: 00:22:2D:9D:B5:52</div>	<div>LAN Ethernet Port 2</div> <div> LAN Ethernet link Inactive status: </div> <div>MAC Address: 00:22:2D:9D:B5:52</div>
<div>LAN Ethernet Port 3</div> <div> LAN Ethernet link Inactive status: </div> <div>MAC Address: 00:22:2D:9D:B5:52</div>	<div>LAN Ethernet Port 4</div> <div> LAN Ethernet link Inactive status: </div> <div>MAC Address: 00:22:2D:9D:B5:52</div>

Fig. 28

Hardware WiFi

View information about all connected *wireless* devices

Access from the left navigation menu:

Gateway > Hardware > Wireless



Fig. 29

WIZARD

You can use the Home Network Wizard to walk you through the steps of:

- Changing the Admin password
- Personalizing the Network Name (SSID), Network Password, or Encryption Method

Access from the left navigation menu:

Gateway > Wizard

Gateway > Home Network Wizard - Step 1

To configure your home network, we need some basic information. [more](#)

Step 1 of 2

To configure your home network, we need some basic information

Current Password:

New Password:

Re-enter New Password:

8-20 characters. Letter and numbers only. No spaces. Case sensitive.

NEXT STEP

Fig. 30

Gateway > Home Network Wizard - Step 2

Configure your wireless network. Note that the network can be accessed by 2.4 GHz or 5 GHz (Wi-Fi B, G, N) compatible devices. [more](#)

Step 2 of 2

Next, we need to configure your wireless network. Note that your network can be accessed by both the 2.4 Ghz (Wireless B, G, N) and 5 Ghz (Wireless A, N) compatible devices.

Enter WiFi Network Name:

Encryption Method:

Enter Network Password:

WPA/WPA2 requires a 8-63 ASCII character password.

FINISH

Fig. 31

For more information about these fields, see the section *Network Settings* under *WiFi Connection*.

Connected Devices

View and edit information about all computers and devices that are currently connected

COMPUTERS

Access from the left navigation menu:

Connected Devices > Computers

Connected Devices > Computers

View the computers connected to the Gateway's LAN. [more](#)

Online Computers					
Host Name	IP Address	DHCP/Static IP	Connection	MAC Address	Comments
00.25.64.47.29.28	10.0.0.2	DHCP	Wireless	00:26:08:ea:78:cb	EDIT X
WNR1000v2	10.0.0.8	DHCP	Ethernet	00:24:b2:56:4e:79	EDIT X

[ADD COMPUTER WITH STATIC IP](#)

Offline Computers				
Host Name	IP Address	DHCP/Static IP	MAC Address	Comments
Comcasts-iPad	10.0.0.5	DHCP	e8:06:88:8e:44:57	X
unknown	10.0.0.6	DHCP	00:26:bb:48:74:17	X
ParadiseLost	10.0.0.3	DHCP	00:25:64:47:29:28	X
cch-131195	10.0.0.7	DHCP	00:0f:1f:ff:4d:b5	X

[ADD WIFI PROTECTED SETUP \(WPS\) CLIENT](#)

Fig. 32

Connected Devices > Computers > Edit Computer

Change the IP address assignment method for Online Computers. [more](#)

Edit Computer

Host Name: Phillip-PC

Connection: Ethernet

Configuration: ☒ DHCP ☐ Static IP

MAC Address: 00:22:5f:c3:ac:9b

Comments:

[SAVE](#) [CANCEL](#)

Fig. 33

Click **Edit** to modify the connection setting for the selected device.

Click **X** to block the device from accessing the Internet.

To manually add a computer with a static IP address to your wireless network:

1. Under Online Computers, click **Add Computer with Static IP**. The Add Computer menu appears.
2. The following table describes the fields on the Add Computer menu:

Table 7

Option	Description
Host Name	Host name of the computer you want to add
Connection	Read-only field that displays the network connection of Ethernet
MAC Address	MAC address of the computer you want to add (use a colon between each 2 character ID in the MAC address)
Static Address	Static IP address of the computer you want to add (use a period between each octet in the IP address)
Comments	Optional comments about the computer

3. Click **SAVE** to save your settings (or click **CANCEL** to discard them). If you click **SAVE**, the Computer menu reappears with the computer you added displayed under Offline Computers.
4. To add more computers with static IP addresses, repeat steps 1 through 3.
5. To edit an online computer, click the **EDIT** button next to the computer you want to modify, edit the settings on the Edit Computer menu and click **SAVE**.
6. To delete an online or offline computer, click **X** next to the computer. When the Delete Computer message appears, click **OK** to delete the computer or **CANCEL** to retain it. If you click **OK**, the computer will be removed from the Computers menu.

Parental Control

Parental Control lets you configure websites, keywords, and computers by blocking content or restricting access

MANAGED SITES

Using the Managed Sites menu, you can block access to certain websites from local computers

Access from the left navigation menu:

Parental Controls > Managed Sites

Parental Control > Managed Sites

Restrict access to specific websites for identified computers/devices on this network. [more](#)

Enable Managed Sites: Enabled Disabled

Blocked Sites

+ ADD

URL	When
-----	------

Blocked Keywords

+ ADD

Keyword	When
---------	------

Trusted Computers

	Computer Name	IP	Trusted
1	00.25.64.47.29.28	10.0.0.2	No Yes
6	WNR1000v2	10.0.0.8	No Yes

Fig. 34

If the Blocked Sites, Blocked Keywords and Trusted Computers are grayed out, click **Enable** (turns green) next to *Enable Managed Sites*. You can then add blocked sites or keywords.

Blocked Sites

Enter the URLs of the websites to be blocked and set up a time schedule

Access from the left navigation menu:

*Parental Control > Managed Sites > Click **Add** next to Blocked Sites*

Parental Control > Managed Sites > Add Blocked Domain

Add Site to be Blocked

URL:

Always Block?

No
Yes

Set Block Time

Start from:

12
00
AM

End on:

11
59
PM

Set Blocked Days

[Select All](#) | [Select None](#)

☒ Monday

☒ Tuesday

☒ Wednesday

☒ Thursday

☒ Friday

☒ Saturday

☒ Sunday

SAVE

CANCEL

Fig. 35

Enter the URL in www.xfinity.com format. The blocked website may be accessible using its IP address.

Blocked Keywords

Enter keyword(s) that appear on websites you want blocked and set up a time schedule

Access from the left navigation menu:

*Parental Control > Managed Sites > Click **Add** next to Blocked Keywords*

The screenshot shows a web interface for adding a blocked keyword. At the top, a blue header bar reads 'Add Keyword to be Blocked'. Below this, the form includes a 'Keyword:' text input field. Underneath is the 'Always Block?' section with two buttons: 'No' and 'Yes' (which is highlighted in green). The 'Set Block Time' section contains 'Start from:' and 'End on:' labels, each followed by three dropdown menus for hour, minute, and period (AM/PM). The 'Start from:' dropdowns are currently set to 12, 00, and AM. The 'End on:' dropdowns are set to 11, 59, and PM. Below the time settings is the 'Set Blocked Days' section, which includes links for 'Select All' and 'Select None'. A list of days from Monday to Sunday follows, each with a checked checkbox. At the bottom of the form are 'SAVE' and 'CANCEL' buttons.

Fig. 36

Trusted Computers

Specify the computers you do not want affected. If a computer is selected as a Trusted Computer, it bypasses the configured parental control settings. Under Trusted Computers, select **Yes** under *Trusted* to add a trusted device (and bypass parental controls) and **No** if a device is not trusted (and should adhere to parental control settings).

MANAGED SERVICES

Prevent access to applications and services

Access from the left navigation menu:

Parental Control > Managed Services

Parental Control > Managed Services

Prevent access to specific applications and services.
 [more](#)

Enable Managed Services:
 Enabled
Disabled

Blocked Services

+ ADD

Services	TCP/UDP	Starting Port	Ending Port	When

Trusted Computers

Computer Name	IP	Trusted
1 unknown	10.0.0.2	No Yes

Fig. 37

Trusted Computers

Specify the computers you do not want affected. If a computer is selected as a Trusted Computer, it will bypass the configured parental control settings. Under Trusted Computers, select **Yes** under *Trusted* to add a trusted device (and bypass parental controls) and **No** if a device is not trusted (and should adhere to parental control settings).

Blocked Services

Define services and ports to be blocked using Parental Control

Access from the left navigation menu:

*Parental Control > Managed Sites > Click **Add** next to Blocked Sites*

Parental Control > Managed Services > Add Blocked Service

Add Service to be Blocked

User Defined Service:

Protocol: TCP/UDP

Start Port:

End Port:

Always Block? No Yes

Set Block Time

Start from: 12 00 AM

End on: 11 59 PM

Set Blocked Days

Select All | Select None

☒ Monday

☒ Tuesday

☒ Wednesday

☒ Thursday

☒ Friday

☒ Saturday

☒ Sunday

SAVE CANCEL

Fig. 38

MANAGED DEVICES

Displays information about devices that can be managed by rules

Access from the left navigation menu:

Parental Control > Managed Devices



Fig. 39

Access Type

- When **Block All** is selected, **+Add Allowed Devices** displays on the lower right.
- When **Allow All** is selected, **+Add Blocked Devices** displays on the lower right

Add Allowed Devices

Choose which devices, if any, are exempt from Parental Control rules

Access from the left navigation menu:

*Parental Control > Managed Sites > Click **ADD ALLOWED DEVICE***

Parental Control > Managed Devices > Add Allowed Device

Add Device to be Allowed

Set Allowed Device

Auto-Learned Devices:

Computer Name	MAC Address
<input type="radio"/> unknown	00:26:08:ea:78:cb
<input type="radio"/> Comcasts-iPad	e8:06:88:8e:44:57
<input type="radio"/> 00.25.64.47.29.28	00:26:bb:48:74:17
<input type="radio"/> unknown	00:0F:1F:FF:4D:B5
<input type="radio"/> unknown	00:25:64:47:29:28
<input type="radio"/> unknown	00:24:B2:56:4E:79

Custom Device:

Computer Name	MAC Address
<input type="radio"/> <input type="text"/>	<input type="text"/>

Always Allow?

Set Allow Time

Start from:

End on:

Set Allow Days

[Select All](#) | [Select None](#)

☒ Monday
☒ Tuesday
☒ Wednesday
☒ Thursday
☒ Friday
☒ Saturday
☒ Sunday

Fig. 40

For example, if a new incoming FTP session arrives at the router, the router needs to know which server is responsible for this traffic. The Port Forwarding rules tell the router which server should get this traffic based on the incoming port number. To use port forwarding, use static IP addresses for the computers (servers) to which the traffic will be forwarded to.

Reports

Created reports display attempted violations of Parental Control rules

Access from the left navigation menu:

Parental Control > Reports

Parental Control > Reports

Generate reports which you can download or print.

Report Filters

Report Type: All Time Frame: Today GENERATE REPORT

All Reports

Reports for Today

[Firewall: RM-ACL]IN=wan1 OUT= MAC=00:22:2d:9d:b5:5SRC=222.208.183.218 SRC=222.208.183.218 DST=76.26.112.4	2010/06/07 07:34:50	Warning
---	------------------------	---------

PRINT
DOWNLOAD

Fig. 41

Advanced

PORT FORWARDING

Allows specific types of incoming connections to be directed to a certain computer or server

Access from the left navigation menu:

Advanced > Port Forwarding

Advanced > Port Forwarding

Permit communications from external hosts by forwarding them to a particular port. [more](#)

Enable Port Forwarding: ☒ Enabled ☐ Disabled

Service Name	Type	Public Port	Private Port	Server IP	Active
http	TCP/UDP	45000-50000	45631	10.0.0.8	<input checked="" type="checkbox"/>
ftp	TCP/UDP	21	21	10.0.0.8	<input checked="" type="checkbox"/>

ADD PORT FORWARD

Fig. 42

Advanced > Port Forwarding > Add Service

Add Port Forward

Service Name:

Service Type:

Server IP Address:

Start Public Port:

End Public Port:

Private Port(s):

Enable Port Range: ☒ Enable Private Port Range

Fig. 43

PORT TRIGGERING (NOT AVAILABLE AT THIS TIME)

Temporarily opens an incoming port to a particular computer when that computer initiates a particular outgoing connection (the trigger)

Access from the left navigation menu: *Advanced > Port Triggering*

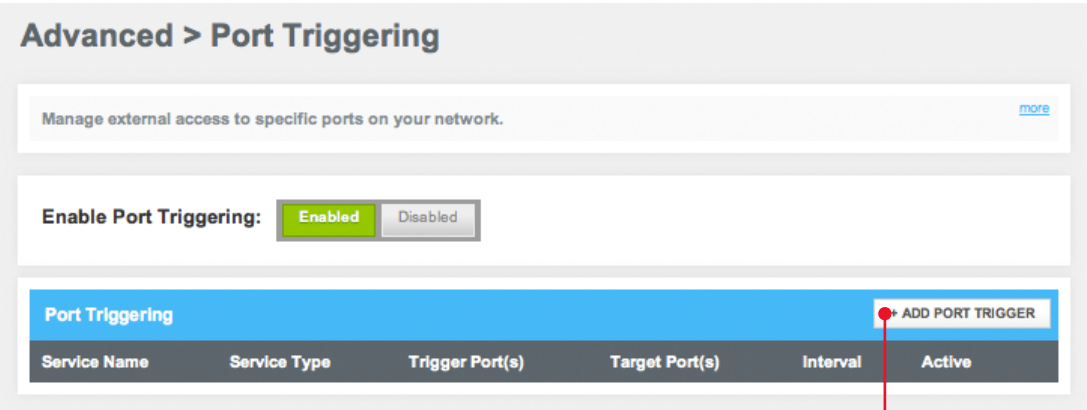


Fig. 44

The **Add Port Trigger** button can be clicked only when Enable Port Triggering is **Enabled**.

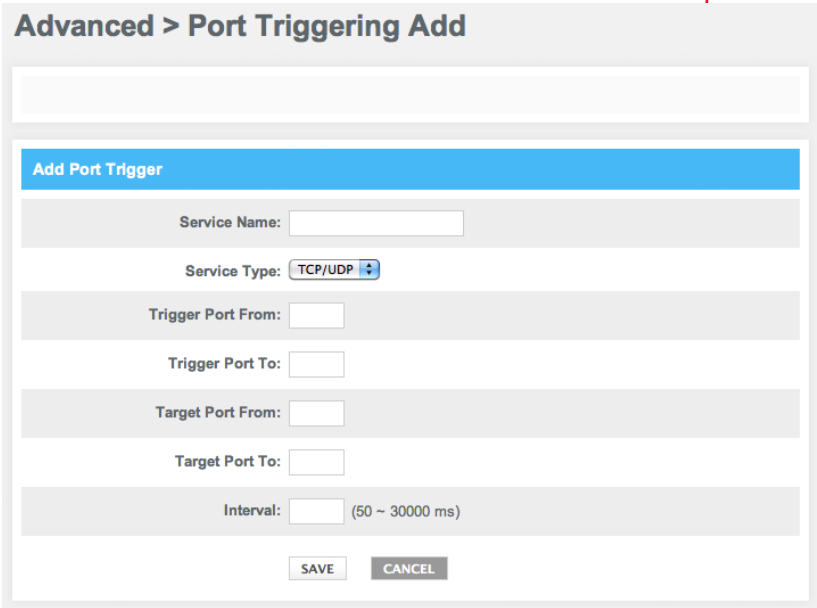


Fig. 45

You may not need to configure the interval for port triggering.

DMZ

Configure a single computer on your LAN to open all of its ports

Access from the left navigation menu:

Advanced > DMZ

Advanced > DMZ

DMZ allows a single computer on your LAN to open all of its ports.
[more](#)

DMZ (Demilitarized Zone)

Enable DMZ:

DMZ Host:

Fig. 46

DEVICE DISCOVERY

Displays the settings for automatic device discovery

Device Discovery uses Plug and Play (UPnP) to automatically configure the router and devices for various Internet applications, such as gaming, media sharing and video conferencing.

Access from the left navigation menu:

Advanced > Device Discovery



Advanced > Device Discovery

UPnP enabled Gateway discovers all UPnP enabled client devices. [more](#)

Device Discovery

Enable UPnP: **Enabled** Disabled

Advertisement Period: 30 minutes

Time To Live: 5 hops

Enable Zero Config: **Enabled** Disabled

SAVE

Fig. 47

Troubleshooting

Logs

View the System, Event and Firewall Logs (also available from *Parental Control > Reports*) to troubleshoot issues and to identify potential security risks

Access from the left navigation menu:

Troubleshooting > Logs

Troubleshooting > Logs

Use these logs to troubleshoot issues and to identify potential security risks. [more](#)

Log Filters

Log Type: System Logs Time Frame: Today SHOW LOGS

System Logs

All Logs for Today

No Ranging Response received - T3 time-out; CM-MAC=00:22:2d:9d:b5:50; CMTS-MAC=00:01:5c:22:ef:81; CM-QOS=1.1; CM-VER=3.0;	2010/07/06 00:53:38	critical
---	---------------------	----------

PRINT DOWNLOAD

Fig. 48

Logs can be printed or downloaded to help with troubleshooting. There are three types of logs:

- System Logs
- Event Logs
- Firewall Logs

DIAGNOSTIC TOOLS

Run a Connectivity/IP Address Check test to troubleshoot connectivity issues to a website URL or IP address

Access from the left navigation menu:

Troubleshooting > Diagnostic Tools

Troubleshooting > Network Diagnostic Tools

Troubleshoot your device issues using diagnostic tools. [more](#)

Test Connectivity Results

Connectivity to the Internet: Active

Packets Sent: 4

Packets Received: 4

Destination Address: Count:

TEST CONNECTIVITY

Check for IP Address Results

IP Address: Count:

Connectivity: OK

CHECK FOR IP ADDRESSES

Fig. 49

- *Test Connectivity Results* tests your Internet connection. Enter a URL, such as www.xfinity.com, in the *Destination Address* field. Click **Test Connectivity**. If there is no connectivity or the URL is invalid, then the test will fail.
- *Check for IP Address Results* determines if an IP address is accessible. Enter an IP address, then click **Check for IP Address**.

RESTORE/RESET GATEWAY

Enables the resetting of your Wireless Gateway and restoring of factory defaults

CAUTION: If you select **Restore Factory Settings**, be certain you want to reset ALL settings (passwords, parental controls and firewall settings) before proceeding! You will lose ALL customized settings made to your Wireless Gateway.

Please also note that a Factory Restore will take your Wireless Gateway out of Bridge Mode if it had been previously enabled. Call 1-800-XFINITY if you would like to enable Bridge Mode again.

Access from the left navigation menu:

Troubleshooting > Restore/Reset Gateway

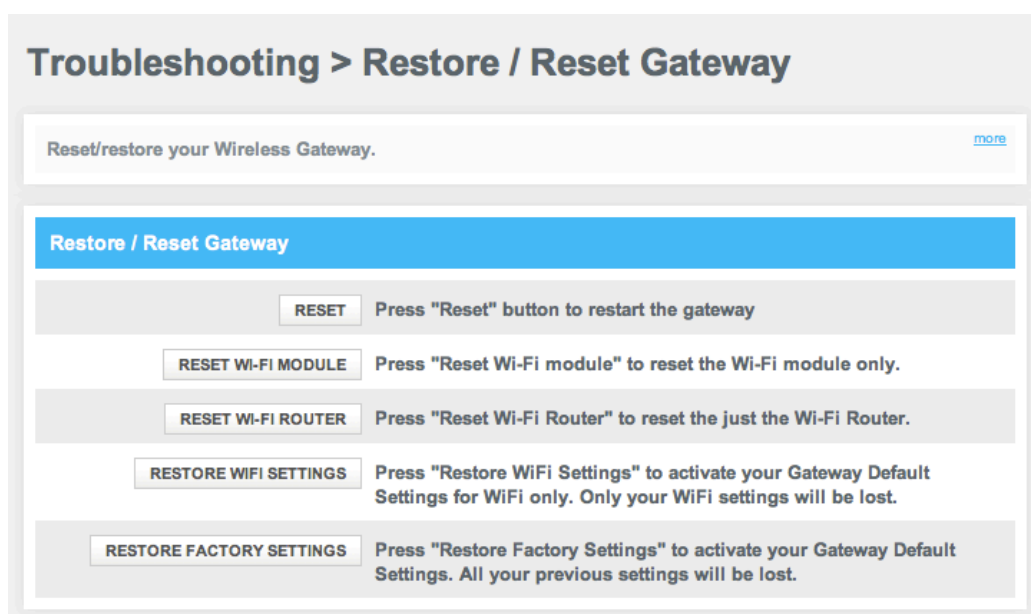


Fig. 50

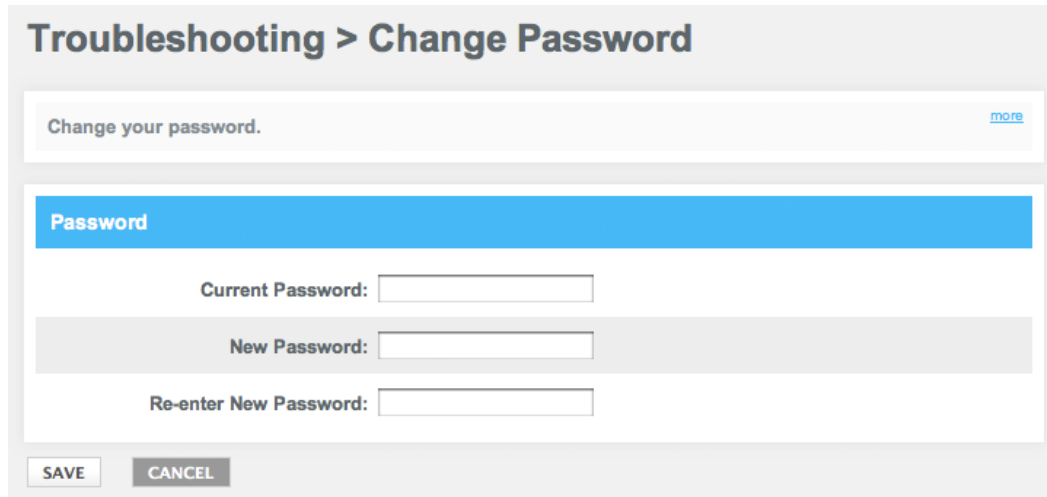
- If you click **Reset** when someone is using the phone, you'll see a warning message that a voice call is in progress and will be disconnected if the Wireless Gateway is rebooted.
- The Wireless Gateway will take a few seconds to reset. Internet connectivity through the Ethernet may be lost momentarily.

CHANGE PASSWORD

Change the password for your Wireless Gateway

Access from the left navigation menu:

Troubleshooting > Change Password



Troubleshooting > Change Password

Change your password. [more](#)

Password

Current Password:

New Password:

Re-enter New Password:

SAVE **CANCEL**

Fig. 51

- Enter your current password.
- Create a new password and re-enter to confirm.
- Click **SAVE**.

Appendix

GLOSSARY

Acronym	Description
D3	DOCSIS 3.0 - Data Over Cable System Interface Specifications
DHCP	Dynamic Host Configuration Protocol - IP protocol used to provide an IP address and location of services required by a network device
eMTA	Embedded Multimedia Terminal Adapter - MTA device with integrated cable modem
FTP	File Transfer Protocol -Standard for exchanging files across a network
IP Address	Internet Protocol - Assigned number used to identify your computer on the Internet
MAC Address	Media Access Control address - Number that uniquely identifies any device connected to a network.
PBC	Push Button Configuration - WPS method
PIN	Personal Identification Network
SSID	Service Set Identifier - String of up to 32 characters that uniquely identifies a wireless LAN
UPnP	Universal Plug and Play
WPS	WiFi Protected Setup

TABLE REFERENCE

Table No.	Description	Page No.
1	Front Panel LED Indicators	2
2	Gigabit Ethernet Connectors LED Indicators	3
3	Connection Information on Bottom Label	5
4	Default Configurations	5
5	Web Management Interface Menus	13
6	IPv4 Configuration Settings	17
7	Add a Computer with Static IP	29

FIGURE REFERENCE

Figure No.	Description	Page No.
1	Front Panel	2
2	Rear Panel	3
3	WPS Button	4
4	Lifting the Wireless Gateway	6
5	Connect Your WiFi Devices	7
6	Default Gateway Name & Password	8
7	At a Glance	8
8	Change Password	9
9	WiFi Network Name (SSID)	10
10	WPS Label	12
11	WPS Button	12
12	Web Management Interface	14
13	At a Glance	15
14	Connection Status	16
15	Local IP Configuration	17
16	WiFi Connection	18
17	Edit WiFi Connection	18
18	Add Wireless Client	19
19	XFINITY Network	20
20	Firewall Security Settings	21
21	Maximum Security	21
22	Typical Security	21
23	Minimum Security	21
24	Custom Security	21
25	Software	22
26	System Hardware	23

Figure No.	Description	Page No.
27	Battery	24
28	LAN Ethernet (Wired) Devices	25
29	WiFi Devices	26
30	Home Network Wizard - Step 1	27
31	Home Network Wizard - Step 2	27
32	Connected Computers	28
33	Edit Connected Devices	28
34	Parental Control Managed Sites	30
35	Add Blocked Domain	31
36	Add Blocked Keyword	32
37	Managed Services	33
38	Add Blocked Service	34
39	Managed Devices	35
40	Add Allowed Device	36
41	Parental Control Reports	37
42	Port Forwarding	38
43	Add Port Forwarding Service	38
44	Port Triggering	39
45	Add Port Triggering Service	39
46	DMZ	40
47	Device Discovery	41
48	Troubleshooting Logs	42
49	Network Diagnostic Tools	43
50	Restore/Reset	44
51	Change Password	45

Regulatory Information

COMPLIANCE STATEMENTS

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment.

This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

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.

The 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.

IEEE 802.11b or 802.11g operation of this product in the U.S.A is firmware-limited to channels 1 through 11.

IMPORTANT NOTE:**FCC Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Note to CATV System Installer - This reminder is provided to call the CATV systems installer's attention to Section 820-93 of the National Electric Code which provide guideline for proper grounding and, in particular, specify that the Coaxial cable shield shall be connected to the grounding system of the building, as close to the point of cable entry as practical.

FCC Part 68 Statement

This equipment complies with Part 68 of the FCC Rules. A label is attached to the equipment that contains, among other information, its FCC registration number and ringer equivalence number. If requested, this information must be provided to the telephone company.

This equipment uses the following USOC Jack: RJ-11.

An FCC-compliant telephone cord and modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack, which is FCC Part 68 compliant. Connection to the telephone network should be made by using the standard modular telephone jack.

The REN is useful to determine the quantity of devices that may be connected to the telephone line and still have all of those devices ring when your telephone number is called. In most, but not all areas, the sum of RENs should not exceed 5. To be certain of the number of devices that may be connected to the line, as determined by the total RENs, contact the telephone company to determine the maximum REN for the calling area.

If this equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone

company will provide advance notice in order for you to make the necessary modifications in order to maintain uninterrupted service.

In the event this equipment should fail to operate properly, disconnect the unit from the telephone line. Try using another FCC approved device in the same telephone jack. If the trouble persists, call the telephone company repair service bureau. If the trouble does not persist and appears to be with this unit, disconnect the unit from the telephone line and discontinue use of the unit until it is repaired.

Please note that the telephone company may ask that you disconnect the equipment from the telephone network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

The user must use the accessories and cables supplied by the manufacturer to get optimum performance from the product.

No repairs may be done by the customer. If trouble is experienced with this equipment, please contact your authorized support provider for repair and warranty information. If the trouble is causing harm to the telephone network, the telephone company may request you remove the equipment from the network until the problem is resolved.

This equipment cannot be used on telephone company provided coin service. Connection to Party Line Service is subject to state tariffs.