# Table of Contents

## About Your Wireless Gateway

Overview .............................................................................................................................. 2

- Front Panel .................................................................................................................... 2
- Rear Panel ..................................................................................................................... 3
- Top Panel ...................................................................................................................... 4
- Bottom Panel ................................................................................................................ 4
- Bottom Label ................................................................................................................ 5

## Set Up

- 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

- Setting up WiFi Connection Using WPS ....................................................................... 11
- Web Management Interface ......................................................................................... 13

## At a Glance

- Connection .................................................................................................................. 14
- Status ............................................................................................................................ 15
- Local IP Configuration .................................................................................................. 16
- Connection WiFi ........................................................................................................... 17
- XFINITY Network ......................................................................................................... 19

## Firewall

- Firewall ......................................................................................................................... 20

## Software

- Software ....................................................................................................................... 21

## Hardware

- Hardware ....................................................................................................................... 22
- System Hardware ......................................................................................................... 22
- Battery .......................................................................................................................... 23
- LAN Ethernet ............................................................................................................... 24
- Hardware WiFi ............................................................................................................... 25

## Wizard

- Wizard ............................................................................................................................ 26

## Connected Devices

- Connected Devices ...................................................................................................... 27
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.
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.

The front of your Wireless Gateway has the following LED indicators:

A  WPS button: WPS (WiFi Protected Setup) is active (Button with light ring is located on top panel)
B  Power: AC power status
C  US/DS: Upstream and downstream connectivity
D  Online: Internet connectivity status
E  WiFi: Status of the wireless LAN
F  Tel1: Status of telephone line 1
G  Tel2: Status of telephone line 2
H  Battery: Battery status

Table 1

<table>
<thead>
<tr>
<th>LED</th>
<th>Front Panel LED Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>Blinking=power failure and during battery backup</td>
</tr>
<tr>
<td>US/DS</td>
<td>Blinking=ranging is in progress</td>
</tr>
<tr>
<td>Online</td>
<td>Blinking=cable interface is acquiring IP address, Time of Day, Cable Modem configuration</td>
</tr>
<tr>
<td>WiFi</td>
<td>Blinking=transmitting data to the WiFi interface</td>
</tr>
<tr>
<td>Tel1</td>
<td>Blinking=Tel line 1 is in use</td>
</tr>
<tr>
<td>Tel2</td>
<td>Blinking=Tel line 2 is in use</td>
</tr>
<tr>
<td>Battery</td>
<td>Solid Glow=battery is charging</td>
</tr>
</tbody>
</table>
**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.

The back of your Wireless Gateway has the following connectors and controls:

- **A** Reset button: resets the Wireless Gateway
- **B** USB host connector [Currently Not Available]
- **C** Tel¹ connector for analog phone line
- **D** Tel² connector for analog phone line
- **E** Gigabit Ethernet (1 - 4) connectors for use with a computer LAN port
- **F** Cable connector for the coaxial cable
- **G** Power connector for the power cord

### Table 2

<table>
<thead>
<tr>
<th>LED</th>
<th>Gigabit Ethernet Connectors LED Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Indicates Gigabit Ethernet (1,000 mbps) in use</td>
</tr>
<tr>
<td>Orange</td>
<td>Indicates Fast Ethernet (10/100) in use</td>
</tr>
</tbody>
</table>

**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](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](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.

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>
<thead>
<tr>
<th><strong>Table 3</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Name (SSID)</strong></td>
</tr>
<tr>
<td><strong>Encryption</strong></td>
</tr>
<tr>
<td><strong>Network Key</strong></td>
</tr>
<tr>
<td><strong>WPS PIN</strong></td>
</tr>
</tbody>
</table>

**DEFAULT CONFIGURATIONS**

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

<table>
<thead>
<tr>
<th><strong>Table 4</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WPS</strong></td>
</tr>
<tr>
<td><strong>Gateway IP</strong></td>
</tr>
<tr>
<td><strong>User Name</strong></td>
</tr>
<tr>
<td><strong>Password</strong></td>
</tr>
<tr>
<td><strong>Firewall Configuration</strong></td>
</tr>
<tr>
<td><strong>UPnP</strong></td>
</tr>
</tbody>
</table>

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](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
- Firewall
- WiFi Protected Setup (WPS)
- 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).

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) __________________________

Fig. 4
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.

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®
• 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.

![Fig. 6](image)

**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](image)
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.

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:

  _______________________________________________________

**Encryption Method**

The encryption method secures data between your computers and the Wireless Gateway. The default setting, WPA/WPA2-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.

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.

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.
# Web Management Interface Menus

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

Select a category to view or configure settings.

Fig. 12

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

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

Log in/out  Change password

96%  Internet  Wireless  Low Security
**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*

![Gateway > At a Glance](image)

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*
**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*)

![Gateway > Connection > Local IP Configuration](image)

**Table 6**

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

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)

---

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.

---

Click Edit to modify your 2.4 GHz Network settings.

---

Fig. 16

Fig. 17
Gateway > Connection > Wireless > Add Wireless Client

Use WPS (WiFi Protected Setup) to simplify your WiFi setup.

Add Wireless Client (WPS)

- **WiFi Protected Setup (WPS):** Enabled
- **Security:** WPA2PSK
- **Encryption:** AES
- **Network Password:** comcast123

**Connection Options:** Push Button

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

[PAIR]  [CANCEL]
**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*)

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

---

### Downstream Channel Bonding Value

<table>
<thead>
<tr>
<th>Index</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock Status</td>
<td>Locked</td>
<td>Locked</td>
<td>Locked</td>
<td>Not locked</td>
<td>Not locked</td>
<td>Not locked</td>
<td>Not locked</td>
<td>Not locked</td>
</tr>
<tr>
<td>Frequency</td>
<td>-1244.955 MHz</td>
<td>-1246.964 MHz</td>
<td>-1242.927 MHz</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNR</td>
<td>31.763 dB</td>
<td>32.321 dB</td>
<td>32.237 dB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power</td>
<td>-106.004 dBm</td>
<td>-106.005 dBm</td>
<td>-105.997 dBm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modulation</td>
<td>256 QAM</td>
<td>256 QAM</td>
<td>256 QAM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Upstream Channel Bonding Value

<table>
<thead>
<tr>
<th>Index</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock Status</td>
<td>Locked</td>
<td>Not locked</td>
<td>Not locked</td>
<td>Not locked</td>
</tr>
<tr>
<td>Frequency</td>
<td>25.9985 MHz</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symbol Rate</td>
<td>5130 Kbps</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power Level</td>
<td>16.210 dBm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modulation</td>
<td>16QAM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Channel ID</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**FIREWALL**

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

Access from the left navigation menu:

*Gateway > Firewall*

---

**Gateway > Firewall**

- **Firewall Security Level**
  - **Maximum Security (High)**
  - **Typical Security (Medium)**
  - **Minimum Security (Low)**
  - **Custom Security**

**Save Settings**  **Restore Default Settings**

---

**Maximum Security (High)**
- Allow (LAN-to-WAN):
  - HTTP and HTTPS (TCP ports 80, 443)
  - DNS (TCP/UDP port 53)
  - NTP (TCP port 123)
  - email (TCP ports 25, 110, 143, 465, 587, 993, 995)
  - VPN/GRE, UDP 500, TCP 1723
  - iTunes (TCP port 3689)
- Blocked: All unrelated WAN to LAN traffic and enable IDS.

---

**Typical Security (Medium)**
- Allow (LAN-to-WAN): all
- Blocked:
  - IDS enabled
  - IDENT (port 113)
  - ICMP request
  - Peer-to-peer apps:
    - kazaa - (TCP/UDP port 1214)
    - bitTorrent - (TCP port 6881-6999)
    - gnutella - (TCP/UDP port 6346)
    - Vuze - (TCP port 48152-66534)

---

**Minimum Security (Low)**
- Allow (LAN-to-WAN): all
- Blocked:
  - IDS enabled
  - IDENT (port 113)

---

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

---

*Fig. 20*

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

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

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

*Fig. 24*
SOFTWARE
View details about your Wireless Gateway's current software

Access from the left navigation menu:

Gateway > Software

![Gateway > Software](image)

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*

---

Fig. 26

---
**Battery**

View the battery specifications

Access from the left navigation menu:

*Gateway > Hardware > Battery*
LAN Ethernet

View information about all connected wired computers and devices

Access from the left navigation menu:

*Gateway > Hardware > LAN*

---

**Fig. 28**

![LAN Ethernet Section](image)
**Hardware WiFi**

View information about all connected *wireless* devices

Access from the left navigation menu:

*Gateway > Hardware > Wireless*

---

*Gateway > Hardware > WiFi*

Your Wireless Gateway provides 2.4 GHz WiFi for connecting to the WiFi LAN.

**WiFi LAN port (2.4 GHZ)**

**WIFI link status:** Active

**MAC Address:** 00:22:2D:3D:B5:58

---

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*

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*

---

**Fig. 32**

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

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

---

**Fig. 33**

*Connected Devices > Computers > Edit Computer*

Change the IP address assignment method for Online Computers.
To manually add a computer with a static IP address to your wireless network:


2. The following table describes the fields on the Add Computer menu:

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

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 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*

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](image)

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*

**Parental Control > Managed Sites > Add Blocked Keyword**

![Add Keyword to be Blocked Form](image)

**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*

---

**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*

---

**Fig. 38**

**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**
- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday
- Sunday

**Save** **Cancel**
**MANAGED DEVICES**
Displays information about devices that can be managed by rules

Access from the left navigation menu:
*Parental Control > Managed Devices*

**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.

![Managed Devices Diagram](image)
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**

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

Fig. 41
**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](image)

**Fig. 42**

![Advanced > Port Forwarding > Add Service](image)

**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

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

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*

---

*[Image of DMZ configuration screen]*

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.

Device Discovery

- **Enable UPnP:** Enabled
- **Advertisement Period:** 30 minutes
- **Time To Live:** 5 hops
- **Enable Zero Config:** Enabled

![Device Discovery Screen](image)

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*

Log Filters

- Log Type: System Logs
- Time Frame: Today

System Logs

No Ranging Response received - T3 time-out; CM-MAC=00:22:22:2d:9d:65:50; CMTS-MAC=00:01:5c:22:f8:31; CM-QOS=1.1; CM-VER=3.0; 2010/07/06 00:53:38 critical

[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**

- **Test Connectivity Results** tests your Internet connection. Enter a URL, such as [www.xfinity.com](http://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

* 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*

![Fig. 51 Wireless Gateway User Guide 44](image)

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

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

<table>
<thead>
<tr>
<th>Table No.</th>
<th>Description</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Front Panel LED Indicators</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>Gigabit Ethernet Connectors LED Indicators</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>Connection Information on Bottom Label</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>Default Configurations</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>Web Management Interface Menus</td>
<td>13</td>
</tr>
<tr>
<td>6</td>
<td>IPv4 Configuration Settings</td>
<td>17</td>
</tr>
<tr>
<td>7</td>
<td>Add a Computer with Static IP</td>
<td>29</td>
</tr>
<tr>
<td>Figure No.</td>
<td>Description</td>
<td>Page No.</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>1</td>
<td>Front Panel</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>Rear Panel</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>WPS Button</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>Lifting the Wireless Gateway</td>
<td>6</td>
</tr>
<tr>
<td>5</td>
<td>Connect Your WiFi Devices</td>
<td>7</td>
</tr>
<tr>
<td>6</td>
<td>Default Gateway Name &amp; Password</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>At a Glance</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td>Change Password</td>
<td>9</td>
</tr>
<tr>
<td>9</td>
<td>WiFi Network Name (SSID)</td>
<td>10</td>
</tr>
<tr>
<td>10</td>
<td>WPS Label</td>
<td>12</td>
</tr>
<tr>
<td>11</td>
<td>WPS Button</td>
<td>12</td>
</tr>
<tr>
<td>12</td>
<td>Web Management Interface</td>
<td>14</td>
</tr>
<tr>
<td>13</td>
<td>At a Glance</td>
<td>15</td>
</tr>
<tr>
<td>14</td>
<td>Connection Status</td>
<td>16</td>
</tr>
<tr>
<td>15</td>
<td>Local IP Configuration</td>
<td>17</td>
</tr>
<tr>
<td>16</td>
<td>WiFi Connection</td>
<td>18</td>
</tr>
<tr>
<td>17</td>
<td>Edit WiFi Connection</td>
<td>18</td>
</tr>
<tr>
<td>18</td>
<td>Add Wireless Client</td>
<td>19</td>
</tr>
<tr>
<td>19</td>
<td>XFINITY Network</td>
<td>20</td>
</tr>
<tr>
<td>20</td>
<td>Firewall Security Settings</td>
<td>21</td>
</tr>
<tr>
<td>21</td>
<td>Maximum Security</td>
<td>21</td>
</tr>
<tr>
<td>22</td>
<td>Typical Security</td>
<td>21</td>
</tr>
<tr>
<td>23</td>
<td>Minimum Security</td>
<td>21</td>
</tr>
<tr>
<td>24</td>
<td>Custom Security</td>
<td>21</td>
</tr>
<tr>
<td>25</td>
<td>Software</td>
<td>22</td>
</tr>
<tr>
<td>26</td>
<td>System Hardware</td>
<td>23</td>
</tr>
<tr>
<td>Figure No.</td>
<td>Description</td>
<td>Page No.</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>27</td>
<td>Battery</td>
<td>24</td>
</tr>
<tr>
<td>28</td>
<td>LAN Ethernet (Wired) Devices</td>
<td>25</td>
</tr>
<tr>
<td>29</td>
<td>WiFi Devices</td>
<td>26</td>
</tr>
<tr>
<td>30</td>
<td>Home Network Wizard - Step 1</td>
<td>27</td>
</tr>
<tr>
<td>31</td>
<td>Home Network Wizard - Step 2</td>
<td>27</td>
</tr>
<tr>
<td>32</td>
<td>Connected Computers</td>
<td>28</td>
</tr>
<tr>
<td>33</td>
<td>Edit Connected Devices</td>
<td>28</td>
</tr>
<tr>
<td>34</td>
<td>Parental Control Managed Sites</td>
<td>30</td>
</tr>
<tr>
<td>35</td>
<td>Add Blocked Domain</td>
<td>31</td>
</tr>
<tr>
<td>36</td>
<td>Add Blocked Keyword</td>
<td>32</td>
</tr>
<tr>
<td>37</td>
<td>Managed Services</td>
<td>33</td>
</tr>
<tr>
<td>38</td>
<td>Add Blocked Service</td>
<td>34</td>
</tr>
<tr>
<td>39</td>
<td>Managed Devices</td>
<td>35</td>
</tr>
<tr>
<td>40</td>
<td>Add Allowed Device</td>
<td>36</td>
</tr>
<tr>
<td>41</td>
<td>Parental Control Reports</td>
<td>37</td>
</tr>
<tr>
<td>42</td>
<td>Port Forwarding</td>
<td>38</td>
</tr>
<tr>
<td>43</td>
<td>Add Port Forwarding Service</td>
<td>38</td>
</tr>
<tr>
<td>44</td>
<td>Port Triggering</td>
<td>39</td>
</tr>
<tr>
<td>45</td>
<td>Add Port Triggering Service</td>
<td>39</td>
</tr>
<tr>
<td>46</td>
<td>DMZ</td>
<td>40</td>
</tr>
<tr>
<td>47</td>
<td>Device Discovery</td>
<td>41</td>
</tr>
<tr>
<td>48</td>
<td>Troubleshooting Logs</td>
<td>42</td>
</tr>
<tr>
<td>49</td>
<td>Network Diagnostic Tools</td>
<td>43</td>
</tr>
<tr>
<td>50</td>
<td>Restore/Reset</td>
<td>44</td>
</tr>
<tr>
<td>51</td>
<td>Change Password</td>
<td>45</td>
</tr>
</tbody>
</table>
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.