SURFBOARD®

SURFboard® G20/G18 DOCSIS® 3.1 Wi-Fi® Cable Modems

User Guide, Revision 1.0

P/N VA-Retail-2024-05-0002

Safety and regulatory information

Important safety instructions

- The model number, serial number, and electrical rating are on a label on the base of the device.
- Do not locate the device near water.
- Do not locate the device in direct sunlight or near a heat source.
- Do not use liquids, aerosols, or forced air to clean the device. It may be cleaned using a dry, lint-free cloth.
- Do not block the ventilation holes on this device. Do not stand it on soft furnishings or carpets.
- Do no use the device in an environment that exceeds 104º F (40º C).
- Use only the power supply and cord provided with the device. Do not use the power supply with any other devices.
- Ground coaxial cable shield at building/residence either close to point of entrance or at point of attachment. Ground as close as practical to building/residence to minimize grounding connector length and reduce potential voltage differences between coaxial cable and other grounding system.

FCC compliance

Vantiva USA LLC, 4855 Peachtree Industrial Blvd., Suite 200 Norcross, GA 30093.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: Reorient or relocate the receiving antenna. Increase the separation between the equipment and set-top. Connect the equipment into an outlet on a circuit different from that to which the set-top is connected. Consult the dealer or an experienced radio/TV technician for help.

CAUTION: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Wireless LAN information

Note: This applies to devices that provide Wi-Fi capability.

This device is a wireless network product that uses Direct Sequence Spread Spectrum (DSSS) and Orthogonal Frequency-Division Multiple Access (OFDMA) radio technologies. The device is designed to be interoperable with any other wireless DSSS and OFDMA products that comply with:

- The IEEE 802.11 Standard on Wireless LANs (Revision AC, Revision B, Revision G, Revision N, and Revision ax), as defined and approved by the Institute of electrical electronics engineers.
- The wireless fidelity (Wi-Fi) certification as defined by the Wireless Ethernet Compatibility Alliance (WECA).

Caring for the environment by recycling

When you see this symbol on a product, do not dispose of the product with residential or commercial waste.

Please recycle product packaging and this document.

Recycling your equipment

Some countries or regions have set up systems to collect and recycle electrical and electronic waste items. Recycling information can be obtained from the WEEE recycling section at *https://www.vantiva.com/corporate-social-responsibility/*.

Table of contents

Introduction

Welcome to the next generation of ultra, high-speed ARRIS ® DOCSIS 3.1® G20/G18. Your Wi-Fi cable modem G20/G18 is a combination of DOCSIS 3.1 cable modem and multi-port Ethernet router with Wi-Fi. It uses DOCSIS 3.1 technology to provide ultra, high-speed Internet access in your home or small business network. Using the connection capabilities of your G20/G18, you can upgrade your entire existing Wi-Fi network by connecting your computer and other network-enabled devices using the two 1Gbps Ethernet ports or the 2.4 GHz and 5 GHz wireless connections. Your G20/G18 connects to the existing coaxial cable connection in your home.

The ARRIS SURFboard Central mobile app assists you with your Wi-Fi cable modem setup and functions. It takes you through the steps to install your home Wi-Fi network using your iOS or Android mobile device and lets you manage your home network access, Parental Control, Guest Access, and more on all your connected devices (e.g., smartphones, cameras, tablets, computers, smart TVs, gaming consoles, and more) across your home Wi-Fi network.

This guide provides instructions for installing and configuring your G20/G18, setting up secure Wi-Fi network connections for your network devices, and managing your Wi-Fi home network configuration.

In your G20/G18 box

Before installing your G20/G18 Wi-Fi cable modem, check that the items listed in the table below are included in your G20/G18 product box. If any items are missing, visit our ARRIS Support website *https://arris.com/selfhelp* for assistance.

Table 1: G20/G18 packaging contents

Item	Description
G20/G18 	High-speed DOCSIS 3.1 Wi-Fi cable modem, wireless access point, and two-port Ethernet router.

Item		Description
Wall power supply		Power supply for an electrical wall outlet connection.
A Quick Start Card		Provides information on how to install your G20/G18 and setting up a secure Wi-Fi network connection in your home or small business network.

System requirements

- High-speed Internet access account
- Web browser access – Microsoft Edge, Google Chrome, Firefox, or Safari
- Compatible operating systems:
  - Windows® 11
  - Windows® 10
  - Windows 8
  - Windows 8.1
  - Windows 7 service pack 1 (SP1)

  Note: Although older versions of Microsoft Windows operating systems are no longer specifically supported, they should still function with your G20/G18.
- Mac® 10.4 or higher
- UNIX®
- Linux®

Contact information

For technical support and additional ARRIS product information, you may visit ARRIS Support website: *https://arris.com/selfhelp*.

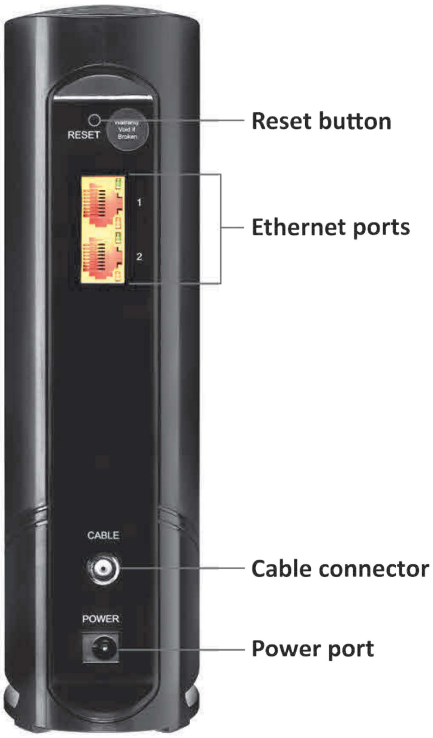
Front panel and LED behavior

LED behavior

LED behavior	Description
Amber (Solid)	Power is initially applied.
Amber (OFF)	No power. Check the power and cable connections. You may have to restart your G20/G18 using the reset button. For details, see *Rebooting your G20/G18* (page 56).
Amber (Flashing)	Firmware download is in progress
White (Flashing five times)	Series of white flashes while holding down the reset PIN indicates a factory reset has been initiated
Green (Blinking)	Downstream/upstream channel search (unlocked status)
Green (Solid)	Online status is in DOCSIS 3.0 mode
Blue (Solid)	Online status is in DOCSIS 3.1 mode
Blue (Blinking)	Error mode. Verify all the cable connections and reset your modem.

LED behavior	Description
Light Blue (Blinking)	WAN over Ethernet mode, cable is unplugged or no Internet
Light Blue (Solid)	WAN over Ethernet mode, Internet is connected
Blue and Green (Alternating colors)	Error mode. Check the power and cable connections. You may have to restart your G20/G18 using the reset button. For details, see *Rebooting your G20/G18* (page 56).

Rear panel and connectors



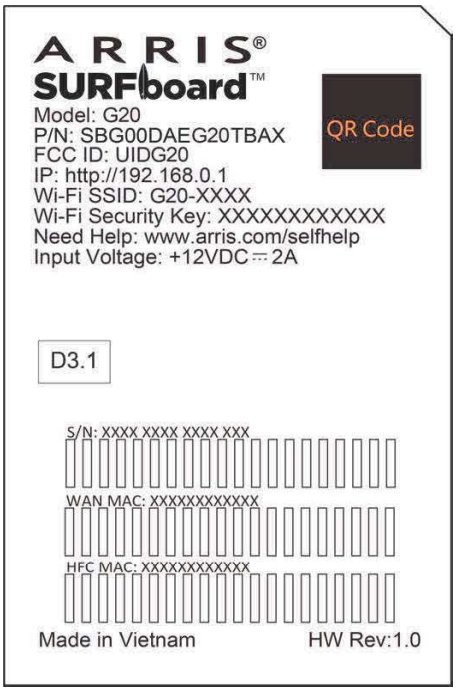
G20/G18 Rear view

Rear panel and connectors

Port name	Description
Reset button	The Reset button located on the rear panel of your cable modem G20/G18 can be used to either reboot or reset your G20/G18 configuration settings.
ETHERNET	Two one-gigabit Ethernet ports for RJ-45 network cable connections: ■ Green: LED is ON - Indicates a data transfer rate of one gigabit per second ■ Green: LED is Blinking - Indicates data traffic is in progress

Port name	Description
10/100/1000	■ Amber: LED is ON - Indicates a data transfer rate of 10 or 100 megabits per second ■ Amber: LED is Blinking - Indicates data traffic is in progress
CABLE	Coaxial cable connector
Power port	100 - 240 VAC Power connector must reflect a 12 VDC @2A power adapter. **Warning:** To avoid any damage to your cable modem, only use the power supply included in your G20/G18 box.

Sample G20/G18 Product label



The product label is located on the bottom of your cable modem . The labels contain the information you need to activate your cable modem for your home Internet service or technical support issues.

To activate your Internet service, contact your service provider for assistance. When contacting your service provider or *ARRIS Technical Support* (page 8), you may have to provide the following information listed on the product labels:

- Model name (G20)
- Serial number (SN)
- MAC address (HFC MAC)

Getting started

This product is for indoor use only. Do not route the Ethernet cable(s) outside of the building. Exposure of the cables to lightning could create a safety hazard and damage the product.

Before installing your G20/G18, check with your service provider (or local cable company) to ensure broadband cable service is available in your area.

The images used in this document are for references only and may contain images of a different model. The SBC app on your mobile device should represent the model you are configuring.

You can set up your G20/G18 home Wi-Fi network in one of the following ways.

- **Using the SURFboard Central app (SBC app): It is recommended that you set up your home Wi-Fi network using the SBC app. For details on how to set up, refer to the SURFboard Central User Guide for Wi-Fi Cable modems available on the** *https://arris.com/selfhelp*.
- Using client device (laptop/desktop): If you are using your client device (laptop/Desktop) with a wired Ethernet connection to set up your home Wi-Fi network then perform the following task.
  - *Setting up your G20/G18 home Wi-Fi network using your client device* (page 12)

Setting up your G20/G18 home Wi-Fi network using your client device

To set up Internet connection in your home network using your client device (laptop/desktop):

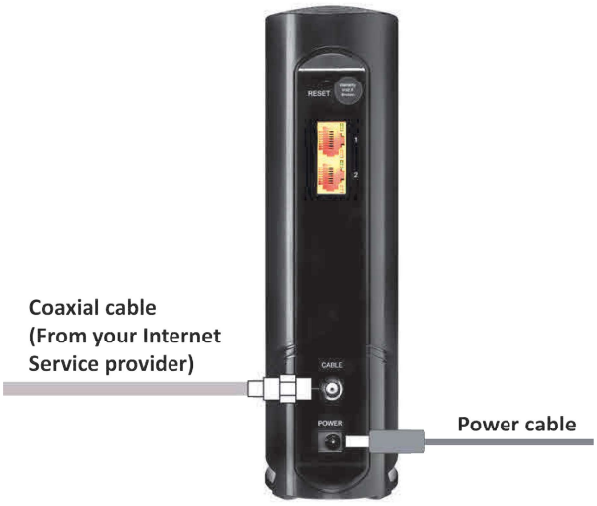
- Ensure to choose a location in your home where your computer and your G20/G18 are preferably near existing cable and electrical wall outlets.
- Ensure to keep the information such as your G20/G18 model name, HFC MAC, and the serial number (SN) listed on your cable modem label (available on the bottom of your modem and on the last page of the Quick Start Card) ready as you may need them while contacting your service provider. For more information, see *Sample G20/G18 Product label* (page 11).

Note: You can use the top-most 1Gbps Ethernet port on your G20/G18 as the WAN input in place of the RF cable connection. You should be able to connect to an alternate Internet connection and use your G20/G18 as your router and a Wi-Fi source. This is a useful feature if you choose to change your Internet service to a

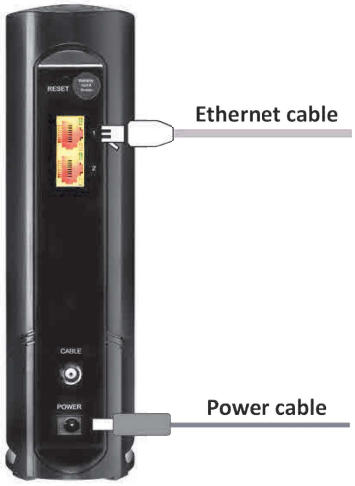
provider that is not a cable operator. You can still use your G20/G18 as your Wi-Fi router.

Note: .

You can enable or disable this feature which is available for the 1Gbps as WAN over Ethernet. For more information, see *Managing WAN configuration settings* (page 54).



G20/G18 connection diagram using the RF cable



G20/G18 connection diagram using an Ethernet cable

1. You can choose to connect using one of the following ways:
   - If you are using a coaxial cable, then follow step 2 and proceed with step 4 onwards (skip step 3).

- If you are using WAN via an Ethernet cable, then perform step 3 onwards.

2. If you are connecting through a coaxial cable, connect one end of a coaxial cable to the **Cable** connector on the rear panel of your G20/G18 and the other end to a cable wall outlet or RF splitter (not included).
3. If you are using WAN via Ethernet cable, connect the other end of the Ethernet cable (not included) from the WAN provider to the top-most **1Gbps** Ethernet port on the rear panel of your G20/G18.
4. Connect one end of the included power supply to the **Power** port on the rear panel of your G20/G18 and the other end to an electrical outlet.

   Warning: To avoid any damage to your cable modem, use only the power supply included in your G20/G18 box.

   Note: This setup requires a Cable/DSL modem or fiber ONT device connected to the ISP.

   This automatically powers ON your G20/G18.

   Although your computer may be configured to automatically access the Internet, you should still perform the following connectivity test to verify that the devices are connected.
5. To proceed further with setting up your G20/G18, follow the on-screen instructions on your SBC app. For more information, refer to the SURFboard Central Mobile App User Guide for Wi-Fi Cable modems.

   Note: You can also use the WEB GUI interface to complete the set up of your G20/G18.
6. To activate (provision) your G20/G18, contact your service provider, you may have to provide the HFC MAC listed on the Wi-Fi cable modem label.

   Note: For Xfinity Internet, download the Xfinity app for modem activation. For Cox or Spectrum Internet, enter your service provider's web browser URL:

   - Cox: *http://www.cox.com/activate*
   - Spectrum: *http://spectrum.net/selfinstall*
7. Open a web browser (such as Microsoft Edge, Google Chrome, Firefox, or Safari) on your computer and type www.surfboard.com or type a valid URL in the address bar and then press `Enter`.

   The ARRIS website or the URL of your choice must open. If the website fails to open, please contact your service provider for assistance.
8. To ensure you are connected successfully to your G20/G18 Wi-Fi network, you can check for the front panel LED on your G20/G18 lights up in a sequential order. Refer to the section *Front panel* for LED status information.

   Note:

   - If the LED does not light up and you do not have an Internet connection, you may have to contact your service provider to reactivate your G20/G18 or check for signal issues.
   - If you still cannot connect to the Internet, visit the ARRIS Support website at *https://arris.com/selfhelp* for assistance.

Adding devices to your home Wi-Fi network

Note: You can prefer to modify the default SSID details using the SBC app or from the WEB GUI interface. However, we recommended you way to set up your SSID using the SBC app. For more information about setting up your Wi-Fi network, refer to the SURFboard Central Mobile App for Wi-Fi Cable Modems User Guide.

Note: The **Wi-Fi Network Name (SSID)** and the **Wi-Fi Security Key (Network Password)** details are required to connect your client devices to your home network. The default network name and network password are listed on your G20/G18 *Sample G20/G18 Product label* (page 11).

Choose from one of the options listed here for setting up a Wi-Fi network connection on your home network using the default SSID. Repeat for each additional device.

- **Windows Computer** – You can connect using the Windows task bar or using the Windows control panel. For more details, refer to your Windows OS documentation.
- **Android device**

  From any screen on your Android device:

  1. Select ⚙ to open the ⚙ Settings screen.
  2. Select ⚙ to open the Wi-Fi settings screen.
  3. Slide to turn on the **Wi-Fi** option.

     Your device will automatically start searching and then display a list of available Wi-Fi networks.
  4. Select your Wi-Fi network name (SSID) from the list.
  5. If prompted, type your Wi-Fi Security Key (network password). Note that your network password may be case-sensitive.
  6. Select **Connect**. If your Wi-Fi network connection is successful, "Connected" message displays below the selected Wi-Fi network name.
- **Apple computer (for example: A MacBook)**

  From any screen on your apple computer:

  1. Click (Wi-Fi icon) to display a list of available Wi-Fi networks.
  2. Select the Wi-Fi network name (SSID) for your home network from the list.
  3. If prompted, enter your network password in the Password field.

     Note: Select **Remember this network** if you want your Mac device to automatically connect to your home network when you log on. Ensure your device must be within range of your Wi-Fi network to connect to it.
  4. *Click **OK**.*

- **Apple mobile device**

  From the Home screen on your Apple device:

  1. Select **Settings** to open the Wi-Fi screen.
  2. Select **Wi-Fi** to turn it ON.

     Your device will automatically start searching and then list the available Wi-Fi networks.
  3. Select the Wi-Fi network name (SSID) for your home network from the list to connect.
  4. If prompted, enter your network password in the Password field.

     If your Wi-Fi connection is successful, # will display next to the Wi-Fi network name.

     Note: For more information on setting up your Wi-Fi network connections, refer to the user documentation for your specific client device.

Quick connect using the Windows task bar

1. From the Windows taskbar on your computer, click the **Wi-Fi Link** icon to open the list of available Wi-Fi networks.

Sample Microsoft Windows taskbar icons

Note: If the **Wi-Fi Link** icon is not visible, left click on the **Show hidden icons** button on the Windows taskbar to open the list of additional icons.

2. Locate and left-click on the G20/G18 Wi-Fi network name or SSID (for example, G20-#### or G18-####) for your G20/G18 from the list of available Wi-Fi networks.

   Note: You must use the default SSID listed on the product label when installing your G20/G18 and setting up your first Wi-Fi network connection. You can change the SSID after your network connections are up and running. For more information, See *Configuring your Wi-Fi network* (page 28).

   Note: The SSID or the Wi-Fi network names that you connect to varies depending on your product.

Sample Wi-Fi network connection screen

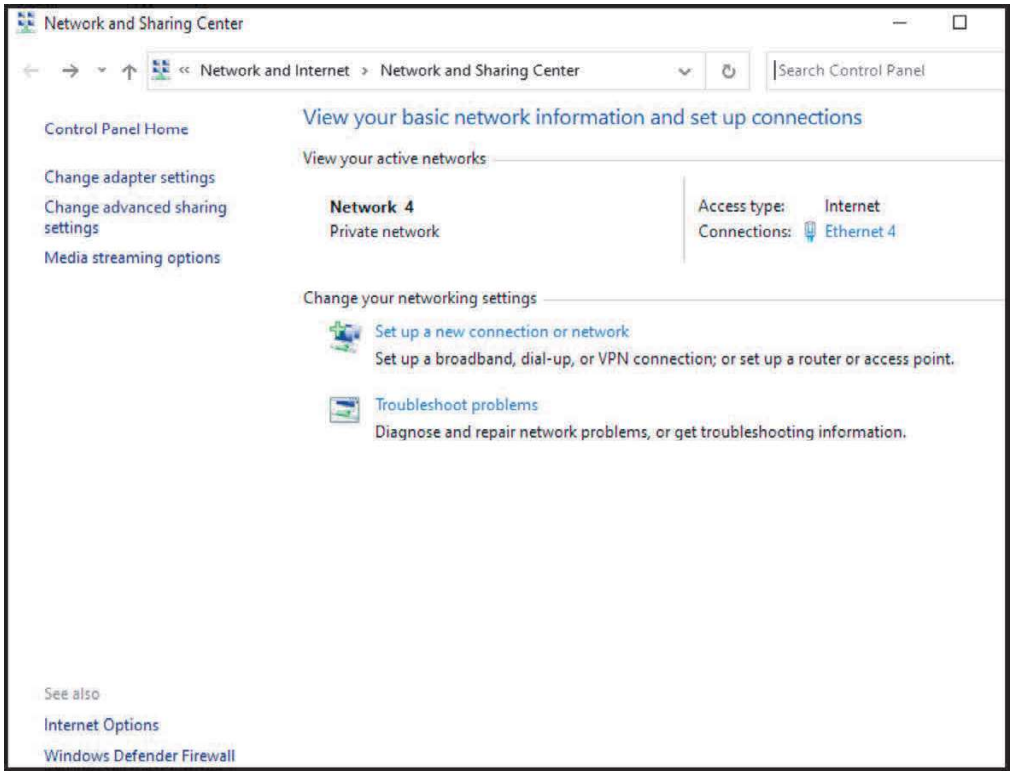
3. Select **Connect automatically** to set up your Wi-Fi devices to automatically connect to your Wi-Fi network without having to log on using a user password.
4. Click **Connect** to open the Connect to a Network window and set up your new network password.
5. Enter the **Network Security Key** (your Wi-Fi network password) in the **Security key** field.

   Note: You can use the default Wi-Fi Security Key code listed on the product label or enter your own personal Wi-Fi network password.

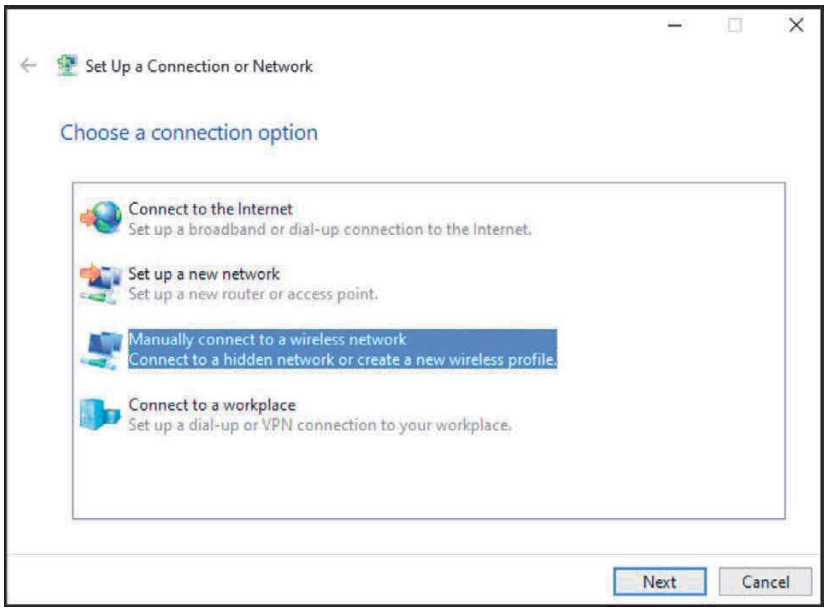
   If you have already changed your Wi-Fi network password using the G20/G18 Web Manager, enter that password in the **Enter the network security key** field and then click **Next**.

Connecting using the Windows control panel

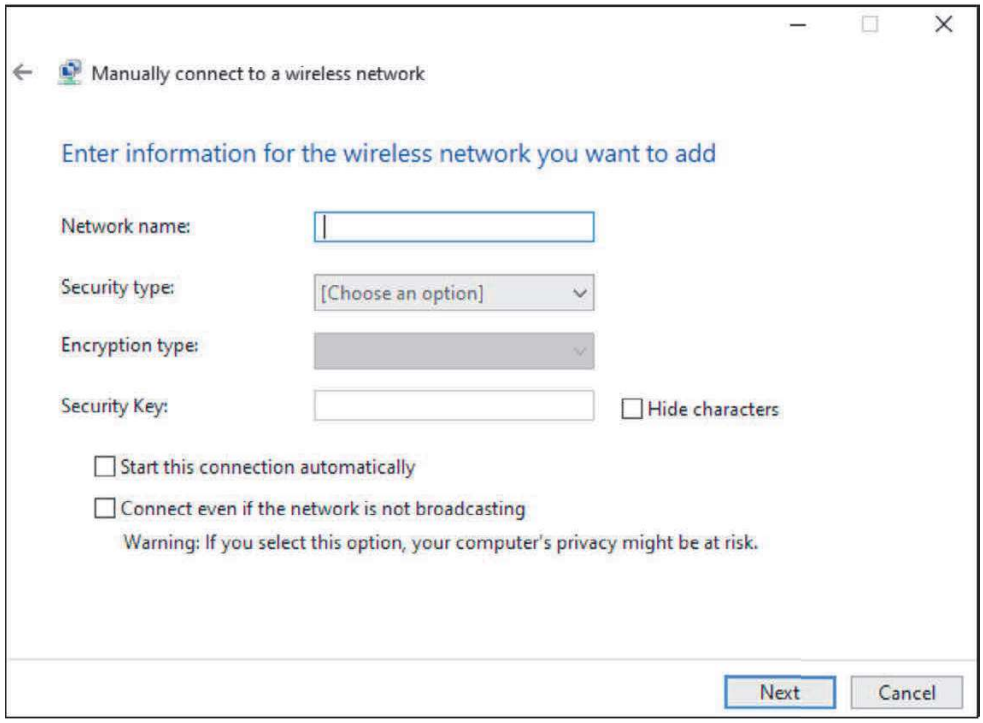
1. From the Windows taskbar on your computer, click **Start** button and then click **Control Panel**.
2. Click **Network and Sharing Center** to open the Network and Sharing Center window.



3. Click **Set up a new connection or network** under Change your networking settings panel.



4. Click **Manually connect to a wireless network** and then click **Next**.



5. Enter the G20/G18 Wi-Fi network name or SSID (G20-#### or G18-####) in the **Network name** field.

   The default SSID is listed on the product label on the bottom of your G20/G18 modem.

   Note: You have the option to change your Wi-Fi network name or SSID after setting up your Wi-Fi network connection. However, you must use the default SSID listed on the product label after installing your G20/G18.

6. Select the wireless Security level for your Wi-Fi network from the **Security type** drop-down list.

   Note: WPA2/WPA3 Mixed Personal(AES/SAE) is the default security level and **WPA3 Personal(SAE)** is the highest security level for your Wi-Fi home network.

7. Select the password encryption type from the **Encryption type** drop-down list.

   This is used for securing your Wi-Fi network.

   - TKIP – Temporal Key Integrity Protocol
   - AES – Advanced Encryption Standard (recommended). AES is the default encryption type for your G20.

8. Enter a security code (passphrase) for your Wi-Fi network password in the **Security Key** field.

   You can use the default **WI-FI SECURITY KEY** listed on the product label or create your own personal network password.

   Note: Remember to use a unique combination of letters, numbers, and special characters to create a more secure password.

9. Select **Hide characters** checkbox to prevent your Security Key (network password) from displaying in the field.
10. Select **Start this connection automatically** so that your Wi-Fi devices will automatically connect to your Wi-Fi network when they are powered on.

11. Click **Next** to complete the Wi-Fi network setup.

    The `Successfully added <Network name>` message for your new Wi-Fi network should appear.

12. Click **Close** to exit.

Testing your Wi-Fi network connectivity

Perform the following connectivity test to check your Wi-Fi network is established and you are able to connect your devices to your G20/G18 home Wi-Fi network.

1. Check if your Wi-Fi devices are successfully connected to your G20/G18 Wi-Fi network and then disconnect the Ethernet cable from your computer and your G20/G18.
2. Check that the LED on your G20/G18 front panel is lit SOLID Green in DOCSIS 3.0 mode and SOLID Blue in DOCSIS 3.1 mode.
3. Open a web browser on your device (computer) and Type a valid URL (such as *www.surfboard.com*) in the address bar and then press **Enter**.

   If the website fails to open, then contact your service provider or visit the ARRIS Support website at *https://arris.com/selfhelp*.

Using the Wi-Fi Cable Modem Web Manager

You can view, monitor, and modify the network configuration settings of your G20/G18 using the SBC app and the WEB GUI option. We recommend you to use the SBC app to modify the network settings. For more information, refer to the SURFboard Central Mobile App for Wi-Fi Cable Modems User Guide.

To configure the network settings using the WEB GUI option, see *Protecting and monitoring your Wi-Fi network* (page 35).

To ensure that your Wi-Fi home network is secure, we recommend that you follow the following best practices for creating your login password:

- Always create a secure password or pass phrase that is not easily guessed.
- Use phrases instead of names so that it may be easier for you to remember.
- Use a combination of upper and lowercase letters, numbers, and symbols.

Starting your G20/G18 Web Manager (first-time login)

Note: To ensure the safety of your network, we recommend you to set up your login password the first time you log on to your G20/G18 Web Manager, the Gateway Home Network Wizard opens for you to set up your login password. Your G20/G18 Home Network wizard walks you through a set of instructions.

1. Open a web browser (such as Internet Explorer, Google Chrome, Firefox, or Safari) on your client device (for example, a computer or a laptop) that is connected to your G20/G18.
2. Type the default LAN IP address, `192.168.0.1`, in the Address bar and then press Enter to log onto your G20/G18.

   The Home Network Wizard Step-1 screen displays.

3. Enter your password in the **New Password** field.

   Note:

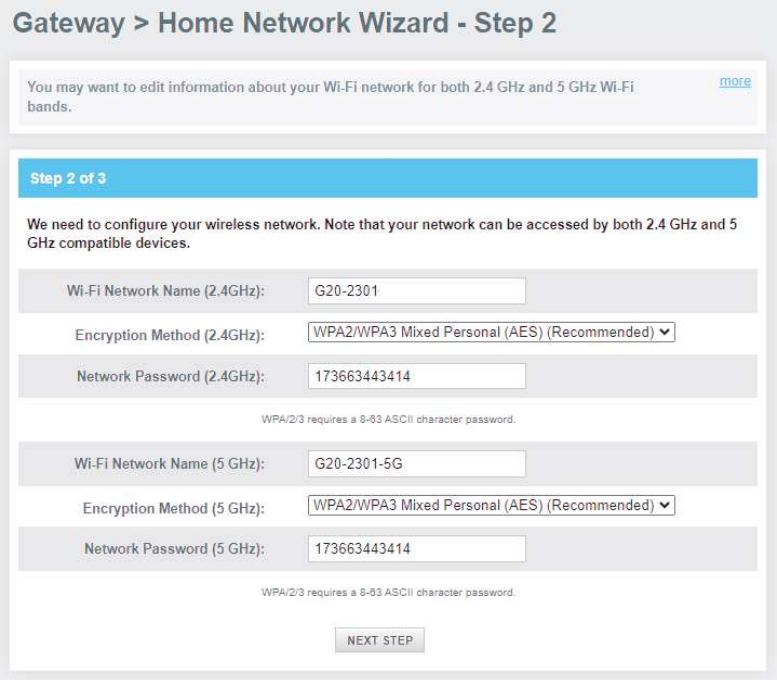
   The password is case-sensitive and must include each of the following:

   - Minimum of eight characters
   - At least one uppercase alphabetic character: A through Z
   - At least one number: 0 to 9
   - One of the following special characters:
     ~ ! @ # $ % ^ * ( ) - _ = + [ ] { } | ; : , . / ?

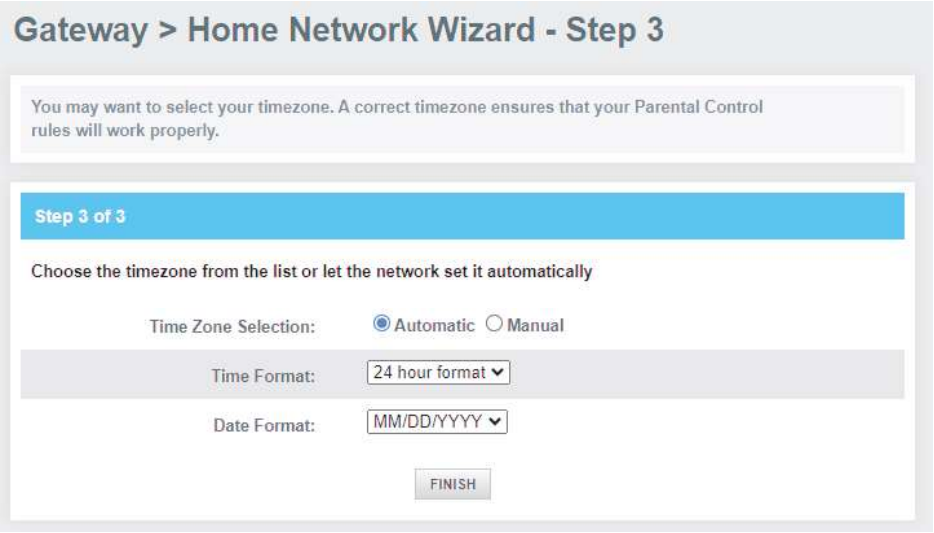
4. Enter your password again in the **Re-enter New Password** field.
5. Click **SHOW** to confirm that both passwords match.

   Please note that this password is required to log in to the Web Manager. Write it down and place it in a secure place for future reference and availability, if needed.
6. Enter the CAPTCHA code in the CAPTCHA entry box and then click **SAVE SETTINGS** .

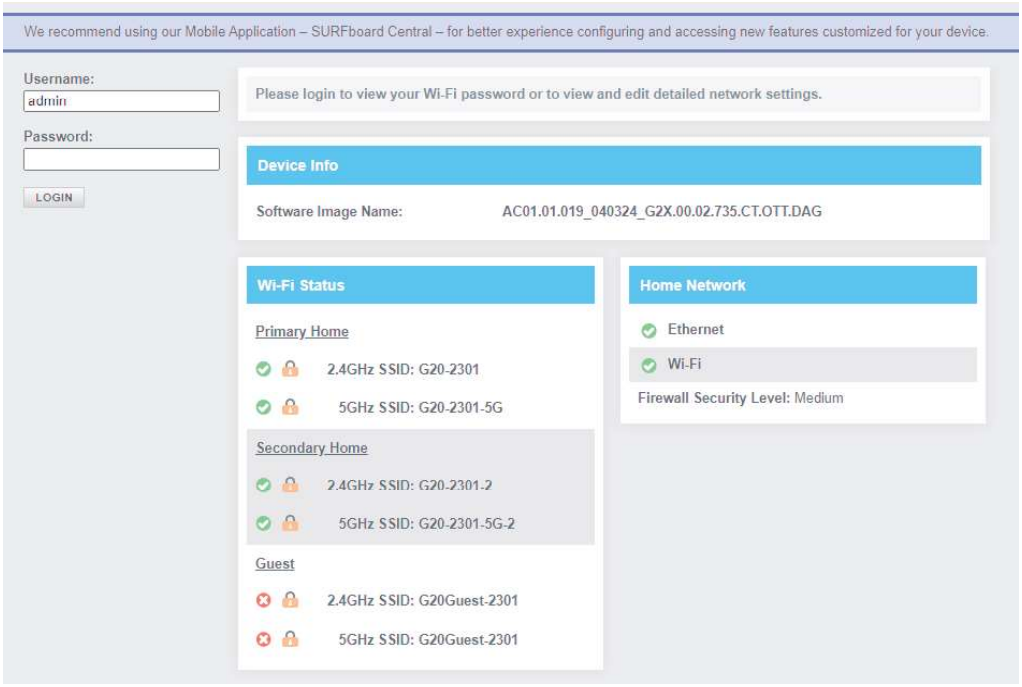
   The Home Network Wizard – Step 2 screen displays.



7. Click **NEXT** to continue.



8. From the **Time Zone** drop-down list, select to set up your time zone.
9. From the **Time Format** drop-down list, select your preferred time format.
10. From the **Date Format** drop-down list, select your preferred date format.
11. Click **FINISH** and the Web Manager Login screen appears.



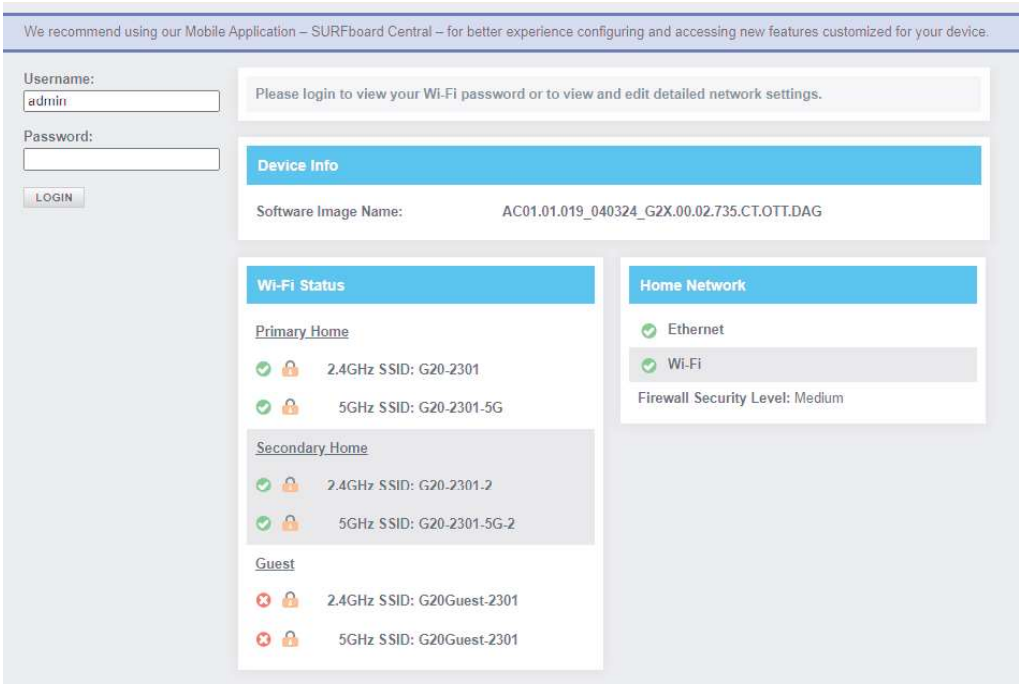
12. Type your new custom password in the **Password** field and then click **LOGIN** to access your G20/G18 Web Manager.

Starting your G20/G18 Web Manager

When you start your G20/G18 Web Manager, you should be able to see the summary page of your network and connected devices.

To start your G20/G18 Web Manager:

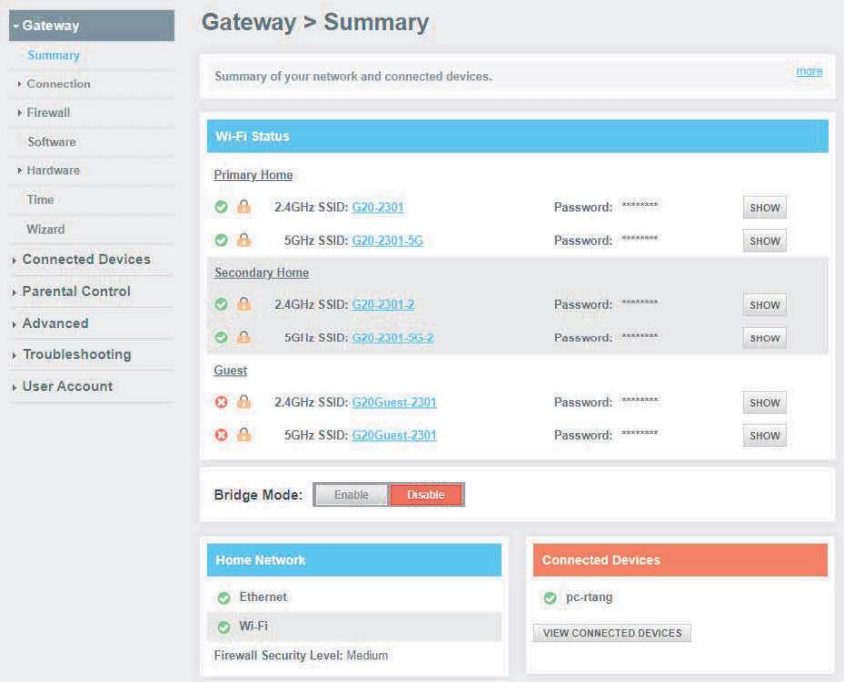
1. Open a web browser (such as Microsoft Edge, Google Chrome, Firefox, or Safari) on the computer or laptop connected to your G20/G18.
2. Type the default LAN IP address, `192.168.0.1`, in the Address bar and then press **Enter** to log into your G20/G18 Web Manager Login screen.



3. Type `admin` (case-sensitive) in the **Username** field.
4. Type your new custom password in the **Password** field.
5. Click **LOGIN** to open the Web Manager page.
   The Product Registration screen appears.

The Product Registration screen

6. Click **Register**, **Ask me later**, or **Stop asking** to proceed.
   Your G20/G18 Summary page appears.



7. To enable Bridge mode option, click **Enable** under the **Bridge Mode** field. We recommend NOT to enable bridge mode.

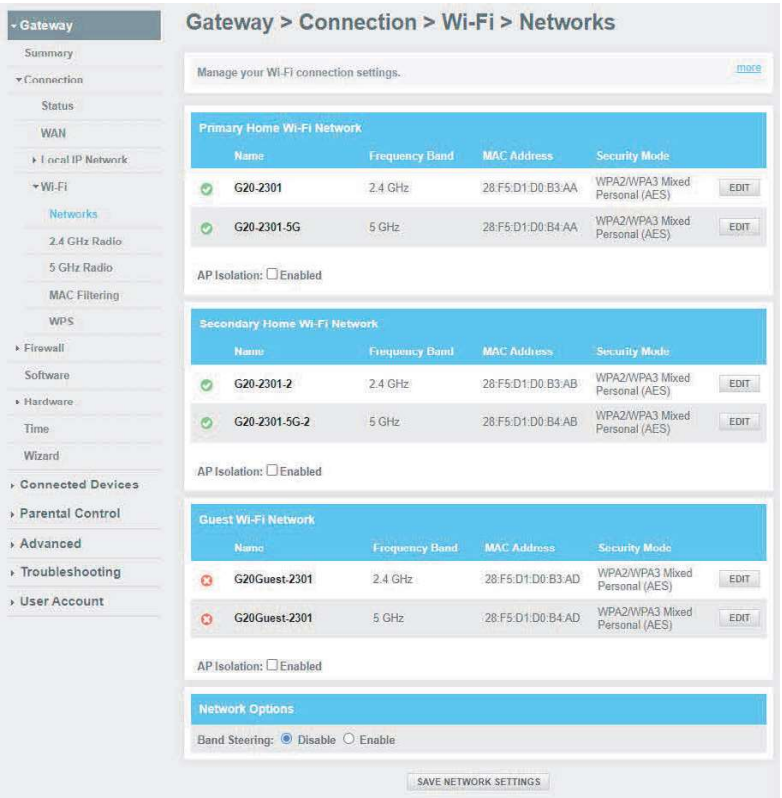
   Note: Enabling Bridge mode will disable the router functionality and then turn off your Wi-Fi network. However, You can still access WEB GUI when you enable the Bridge mode and you can disable the Bridge mode setting by clicking **Disable** under the **Bridge Mode** field .

Configuring your Wi-Fi network

You have the option to either use the default network settings which are unique to your G20/G18 for security purposes or you can configure different network settings. It also supports a secure method for setting up multiple Wi-Fi networks.

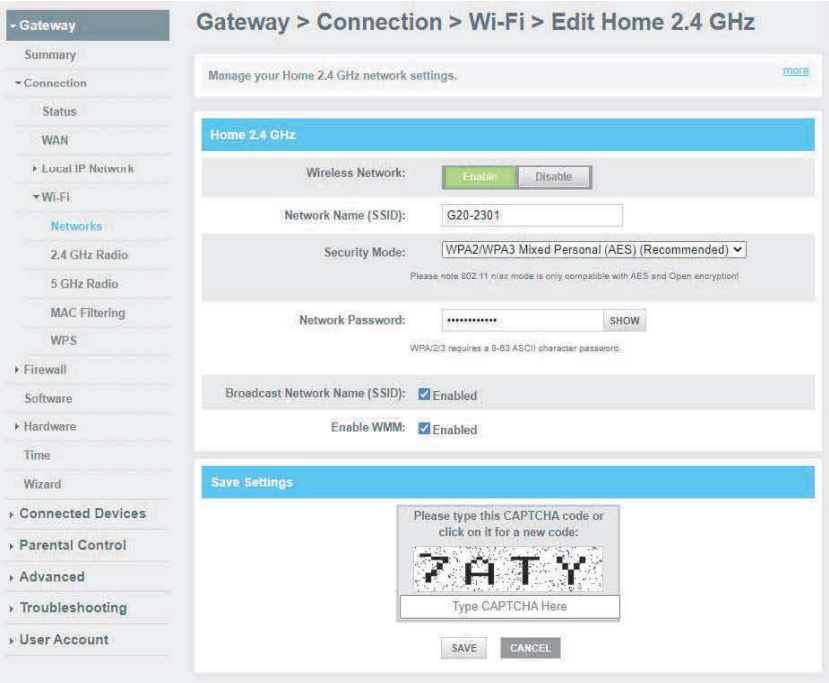
Changing your Wi-Fi network name and configuration details

1. Open a web browser and log on to open your G20/G18 Web Manager screen.
   For information about starting your G20/G18 Web Manager, see *Starting your G20/G18 Web Manager* (page 25).
2. Click the menu links **Gateway** > **Connection** > **Wi-Fi** > **Networks**.
   The Gateway Connection Wi-Fi screen appears.



3. To set up the Network Security mode on your primary Home Wi-Fi network, on the Primary Home Wi-Fi Network tab, click **EDIT** respective to the Frequency Band.

The Manage Home Networks Settings screen appears.



4. You can choose to retain the default network name SSID (Service Set Identifier) for your Wi-Fi home network. If you prefer to choose a new network name then in the **Network Name (SSID)** field, enter a new network name of your choice.

   Note: The Wi-Fi network name cannot be the same name as any other SSID on your home network. You can use any combination of lowercase and uppercase letters, numbers, and/or special characters (symbols) up to a maximum of 32 characters.

5. Select one of the following Wi-Fi network security options for your G20/G18 from the **Security Mode** drop-down list:

   - **WPA2/WPA3 Mixed Personal (AES/SAE) (Recommended)**: Combination Wi-Fi Protected Access version 2 and Wi-Fi Protected Access version 3 and provides additional network security.
   - **None** (not secure and not recommended): This network security option does not provide any level of network security for your Wi-Fi network. It allows outside users to connect to your Wi-Fi network without having to use a Wi-Fi Security Key (network password).
   - **WPA3 Personal (SAE)**: Wi-Fi Protected Access version 3 with Pre-Shared Key.
   - **WPA2-PSK (AES)**: It is an advanced encryption mechanism which safeguard network access and data transfer.

6. Enter your Wi-Fi network password in the **Network Password** field.

   Note: Keep in mind that network passwords are case-sensitive. You can use any combination of uppercase and lowercase letters, special characters, and numbers. Spaces are not acceptable.

7. Select the **Show Network Password** checkbox to view and confirm your network password.

8. If you prefer to display your SSID as an available Wi-Fi network to other users, select the **Broadcast Network Name (SSID) Enabled** checkbox.
9. To enable multi-media functionality, select the **Enable WMM** checkbox.

   Enabling WMM can help control latency and jitter when transmitting multi-media content over a Wi-Fi connection. This quality of service mechanism uses four access categories:

   - Voice
   - Video
   - Best effort
   - Background

     WMM ensures that applications with low tolerance for latency and jitter are treated with higher priority than less sensitive data applications. WMM sets different wait times for the above four categories to provide priority network access for applications that are less tolerant of packet delays.
10. Enter the CAPTCHA code located in the **Type CAPTCHA Here** entry box.
11. Click **SAVE** to save the settings.
12. To set up the Network Security mode on your Guest Wi-Fi network, on the Guest Wi-Fi Network tab, click **EDIT** and then perform steps 4 through 11.
13. If you do not want your devices connected to this network to communicate with each other, then select the **AP Isolation** checkbox.
14. Under the **Network Options** tab, you can choose to enable or disable the **Band Steering** checkbox. Enabling this feature helps to do periodic checking of your devices that are connected on 2.4GHz bands and steer them to faster available 5GHz bands.
15. Click **SAVE NETWORK SETTINGS**.

Changing the Wi-Fi Radio configuration settings

You can manage your Wi-Fi connection settings such mode selection, channel selection, dynamic channel selection, and setting the DCS scan interval.

To change the Wi-Fi Radio configuration settings for 2.4GHz and 5GHz

1. Open a web browser and log on to open your G20/G18 Web Manager page.

   For more information, see *Starting your G20/G18 Web Manager* (page 25).
2. From any of the G20/G18 Web Manager screen, click the **Gateway** menu link and then click the **Connection** submenu options link.
3. Click **Wi-Fi** > **2.4GHz Radio** on the left pane.

Wi-Fi Network 2.4GHz Radio Connection screen

4. To turn on the 2.4GHz Wi-Fi frequency range for your Wi-Fi home network, click the **2.4GHz Radio** submenu on the left pane and then click the **Enable** button.
5. To specify the Wi-Fi standards that your G20/G18 should use to communicate with your client devices, choose from the **Mode** drop-down list.
6. Select the Tx (Transmit) Power level of the Wi-Fi radio from the **Tx Power** drop-down list.
7. Select a channel number (Auto, 1 through 11) from the **Channel** drop-down list to determine how the channel in your Wi-Fi network is selected.

   Note: In Automatic mode, which is the default selection, your G20/G18 shall select the channel with the least amount of Wi-Fi interference. But in Manual mode, you can specify the channel to be used.

   Note: For 2.4 GHz Wi-Fi networks, it is recommended to use Channel 1, 6, or 11, if it is not listed as the Current Channel. In the Wi-Fi spectrum, there are multiple channels that overlap and thus degrade Wi-Fi network performance. Channels 1, 6, and 11 are used for better network performance and stability because they do not overlap.
8. Set the channel bandwidth for your G20 modem from the **Channel Bandwidth** box.
9. Click **Enable** under the **Dynamic Channel Selection** option if you want your G20/G18 modem to periodically scan other Wi-Fi channels and switch to a channel with least amount of interference.

   Note: During scanning of the Wi-Fi channels, your Wi-Fi clients may get temporarily disconnected. This option is available if you have set Channel selection to **Automatic**.
10. To determine the time period between Dynamic Channel Selection scans, set the DCS scan interval from the **DCS Scan Interval** drop-down list.
11. Click **SAVE SETTINGS**.

12. You can change the Wi-Fi connection settings for 5GHz Radio as well.

    To change the 5GHz Radio Configuration settings:

    a) Click **Wi-Fi** > **5GHz Radio** on the left pane of the Wi-Fi Connection screen.

    b) Perform previous steps 5 through 11.

    c) To enable 5GHz supported devices on DFS channels, select **Enable** under the **DFS** option. During this time your system shall scan for DFS channels and disconnects your 5GHz clients that do not support DFS functionality. These clients shall reconnect to your Wi-Fi network using 2.4GHz.

    d) Click **SAVE SETTINGS**.

Changing MAC filtering settings

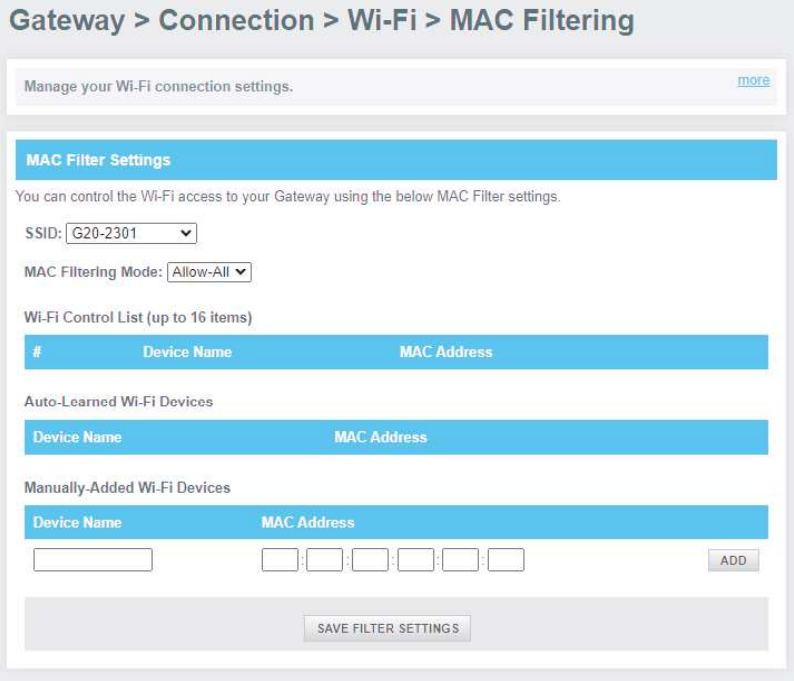
You can control the Wi-Fi access to your G20/G18 using the MAC filtering settings. These settings are specific to each Network name (SSID).

To change the MAC filtering mode:

1. Open a web browser and log on to open the G20/G18 Web Manager.

   For more information, see *Starting your G20/G18 Web Manager* (page 25).

2. Click the **Gateway** menu link and then click the **Connection** submenu options link.
3. Click **Wi-Fi** > **MAC Filtering** to open the MAC Filtering settings screen.



MAC Filtering settings screen

4. Select the SSID to which you prefer to apply the MAC filtering mode.
5. From the **MAC Filtering Mode** drop-down list, select one of the following:
   - **Allow-All**: No Mac filtering rules are applied. All wireless clients can connect to your G20/G18.

- **Allow**: On the devices in the "Wi-Fi Control list" are allowed to connect to your G20/G18.
- **Deny**: Wireless devices in the "Wi-Fi Control list" are not allowed to connect to your G20/G18.

Under the **Wi-Fi Control List**, you can view all the wireless devices (by Network name and MAC address) that are added manually or auto-learned.

Under the **Auto-Learned Wi-Fi Devices** tab, it displays all the wireless devices that are auto-learned by your G20/G18.

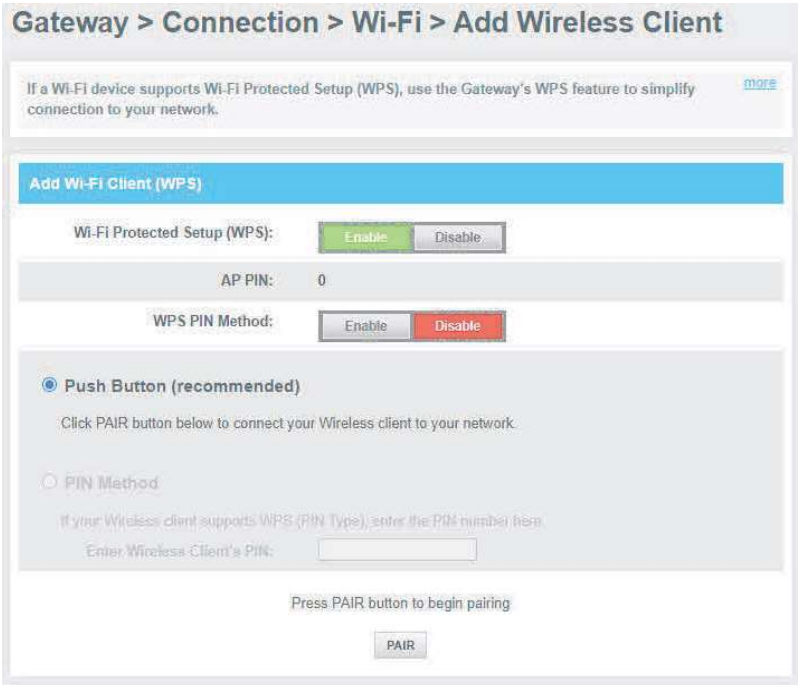
6. Under the **Manually-Added Wi-Fi Devices** tab, type a unique name and MAC address for the wireless device that you want to manually add and then click **ADD**.
7. Click **SAVE**.

Setting up WPS on your G20 Wi-Fi network

You can set up the Wi-Fi Protected Setup (WPS) PIN option on your G20/G18 to connect WPS-enabled devices on your Wi-Fi home network.

1. Open a web browser and log on to open the G20/G18 Web Manager.

   For more information, see *Starting your G20/G18 Web Manager* (page 25).
2. Click the **Gateway** menu link and then click the **Connection** submenu options link.
3. Click **Wi-Fi** > **WPS** to open the Gateway Connection Wi-Fi screen.



4. Do one of the following:
   - Click the Wi-Fi Protected Setup (WPS) **Enable** button to turn ON WPS Wi-Fi networking on your home network using the provided AP PIN number.

- Click the Wi-Fi Protected Setup (WPS) **Disable** button to turn OFF WPS Wi-Fi networking on your home network.

5. Do one of the following:
   - Click the WPS Pin Method **Enable** button to turn ON WPS Wi-Fi networking.
   - Click the WPS Pin Method **Disable** button to turn OFF WPS Pin connections.
6. To proceed with the PIN method, click the **PIN Method** option and then Enter the WPS Pin number listed in the **AP PIN** field when you are prompted on your WPS device screen.
7. Click **PAIR** to connect your WPS-enabled device.
8. Repeat steps 6 through 8 for each additional WPS-enabled device that you want to connect to your Wi-Fi home network.
9. To proceed with the Push button option, click the **Push Button (recommended)** option to connect your wireless client to your network.
10. Click **PAIR** to connect your WPS-enabled device.

Protecting and monitoring your Wi-Fi network

After you have successfully connected your G20/G18 and your Wi-Fi devices, you should configure your G20/G18 to protect your Wi-Fi network from unwanted and unauthorized access by any Wi-Fi devices that are within range of your Wi-Fi network. Although you have configured the network security for your G20/G18, you can use your G20/G18 Web Manager to set the level of security and network access that you want to allow on your Wi-Fi network.

Setting up firewall protection

You can set up firewall filters to protect your computer(s) and other connected network devices on your Wi-Fi home network. You can also block Java Applets, Proxies, and website access to protect the network devices on your home network from hackers, viruses, and other attacks from the Internet.

To set the firewall protection level on your Wi-Fi network:

1. From the G20/G18 Web Manager screen, click the **Gateway** menu link.
2. Click the **Firewall** submenu link and then click *IPv4* or *IPv6* to display the Gateway Firewall Security Level screens.
3. Select the security level that you want to set for your G20/G18 firewall. You may select a security level from these preset values or customize your own setting:
   - **Maximum Security (High)** - Block all applications, including voice applications and P2P applications, but allow Internet, email, VPN, DNS, and iTunes services.
   - **Typical Security (Medium)** - Block P2P applications and pings to the Gateway, but allow all other traffic.
   - **Minimum Security (Low)** - Block no applications or traffic. (Default Setting).
4. Enter the CAPTCHA details and then click **SAVE SETTINGS** to save your changes.

Setting up Parental Control

The Parental Control feature provides the ability to block specific websites or restricts Internet access, which can keep your family members (especially minors) healthy and safe. This allows you to manage and limit the usage and activity for specific users and client devices on your home network.

Following are the main features available under Parental Control:

- Managed Sites: Blocks specific websites based on URLs or keywords.
- Managed Groups: Blocks specific websites or restricts Internet for a group of devices.
- Managed Devices: Trusts devices to bypass the Parental Control feature.

Note: The Parental Control features may vary based on your product type and the firmware version.

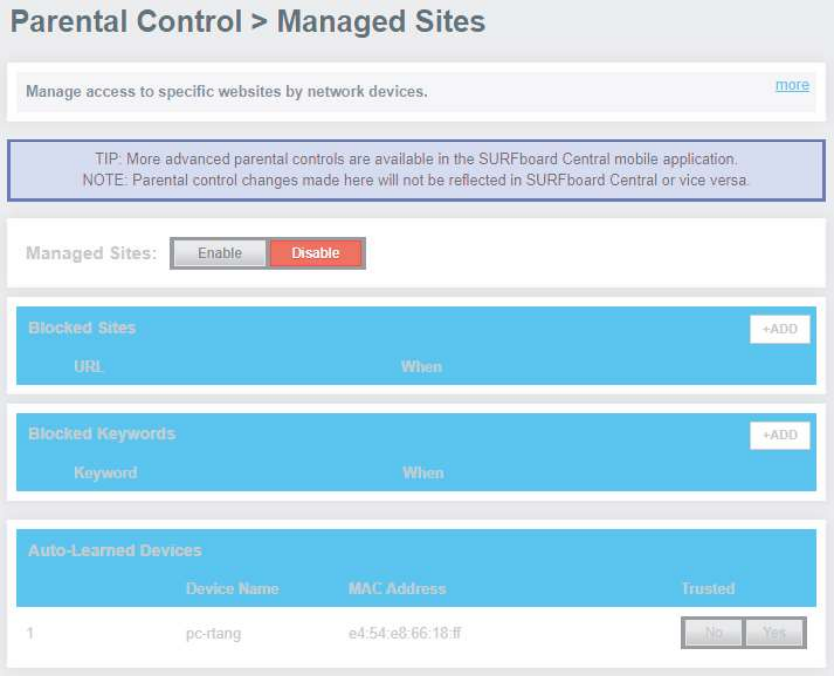
Note: Ensure to enable the Parental Control feature before you set up Managed Sites/Managed Groups/Managed Devices.

To set up Parental Control on your home network:

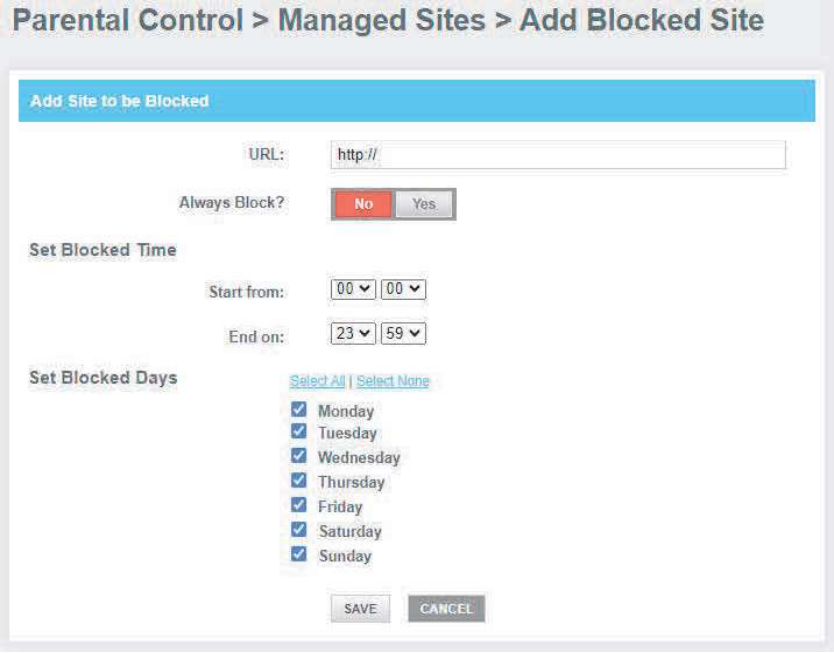
1. From the Web Manager screen, click the **Parental Control** menu link and then click **Enable** button to enable the features for Managing Sites, Managing Devices, and Managing Groups.

   Managing Sites:

2. Click **Managed Sites** from the Parental Control submenu options list to display the Parental Control Managed Sites screen.

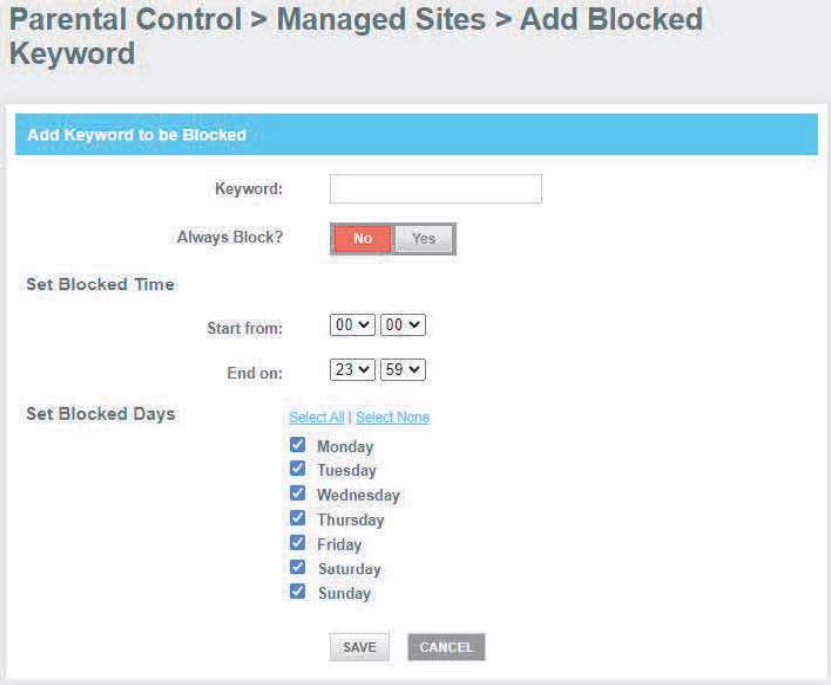


3. Click **+ADD** button under the **Blocked Sites** section. The screen to manually add the URL appears.



4. Enter the website address in the **URL** field (for example: www.surfboard.com).
5. If you prefer to block by specific days in a week, then select the days of the week in the **Date** field.
6. If you prefer to block by specific time, then select the **Start from** and **End on** times of the day in the **Time** field (for example: "18:00" to "23:00").
7. Click **SAVE.**
8. Repeat steps 4 through 7 for each website that you want to block.

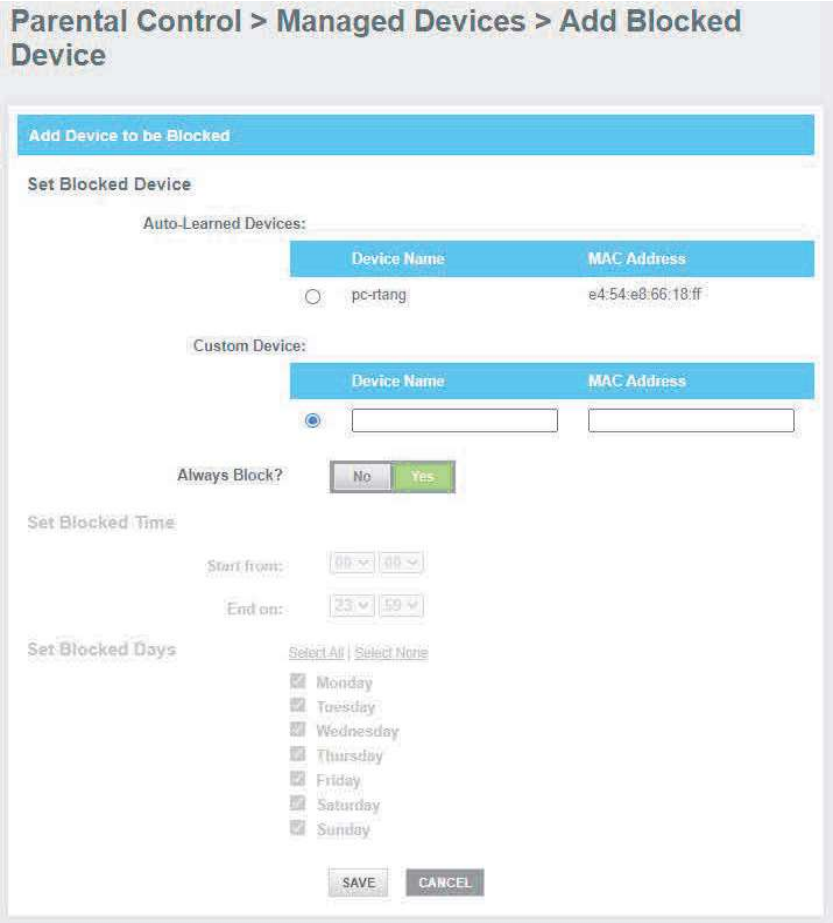
   Managing Keywords:
9. Under the **Managed Sites** from the Parental Control submenu options, click **+ADD+** under the **Blocked Keywords** section.



10. Enter the keyword in the **KEYWORD** field (for example, type "surfboard").
11. If you prefer to block by specific days in a week, then select the days in the **DATE** field (for example, select Mon, Tue, Wed, Thu, Fri).
12. If you prefer to block by specific time, then add the time in the **TIME** field (for example, specify 00:00- 23:59).
13. Select **Enable** and then click **SAVE**.

    Managing Devices:

14. Under Parental Control Managed Devices submenu, click **+ADD TRUSTED DEVICE** to add only the device you want to restrict.
15. To manually trust a device, type the **Name** of your device (for example "MyPhone" and enter the MAC address if your device in the **MAC** field (for example: 11:11:11:11:11:11).



16. Click **SAVE** to save the changes.

Setting up Port Forwarding

Your G20/G18 firewall may be set up to block all device or application connections from the Internet to the devices on your Wi-Fi home network. Port Forwarding allows you to open specific ports or IP addresses on the Internet behind the firewall on your home or small business network. It also allows for remote access to your wireless computer or other client devices. The inbound traffic from the Internet, such as specific websites or online gaming applications, is forwarded to the designated open ports that you set up.

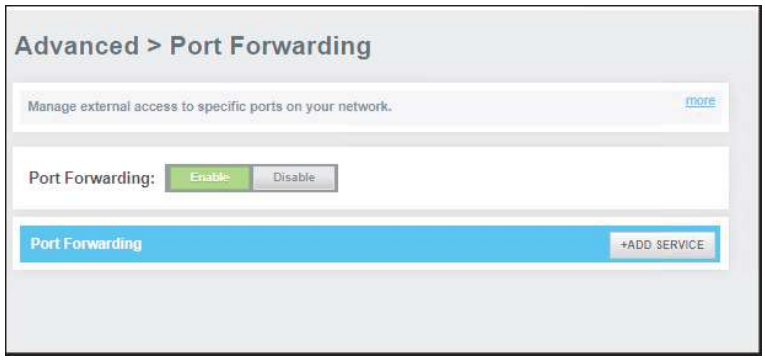
Note:

ARRIS recommends that you manually configure the TCP/IP settings listed below on the client device you are setting up for remote access. Otherwise, remote access to your client device will not be available on the Internet.

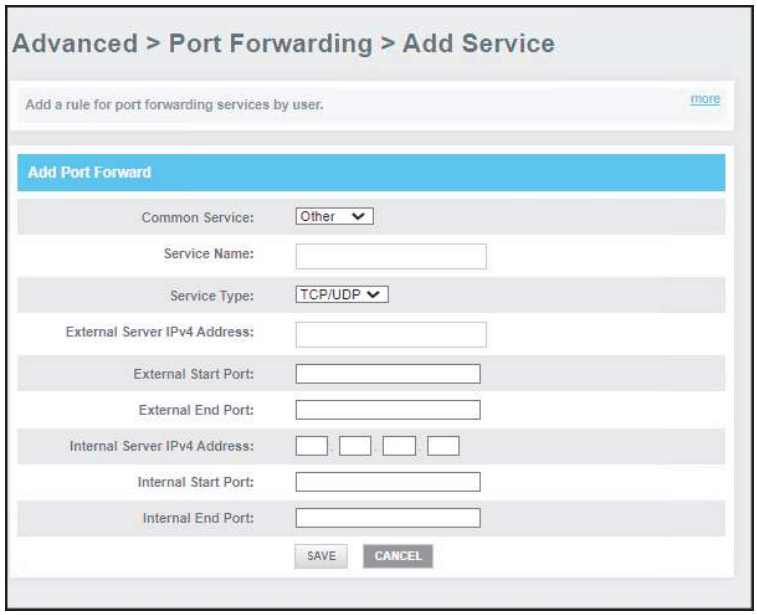
- IP address
- Subnet mask
- Default gateway
- DNS address (at least one)

To set up Port Forwarding:

1. From the G20/G18 Web Manager screen, click the **Advanced** menu link.
2. Click **Port Forwarding** from the Advanced submenu options list to display the Port Forwarding Configuration screen.



3. Click the Port Forwarding **Enable** button.
4. Click the **+ADD SERVICE** button to open the Add Port Forward screen.



Add Port Forward screen

5. Select **FTP**, **AIM**, **HTTP**, **PPTP**, **HTTPs**, **Telnet**, **SSH**, or **Other** for the Internet data transfer protocol from the **Common Service** drop-down list.

   Note: When **Other** is selected, the **Service Name** field will display. Enter a name for the service type you will be using.

6. Select **TCP/UDP**, **TCP**, or **UDP** for the Internet data transmission protocol from the **Service Type** drop-down list.
7. Enter the IP address of your local computer that you are setting up for port forwarding in the **Internal Server IPv4 Address** field.
8. Enter the external the starting port number and end port number of the external hosts in the **External Start Port** and **External End Port** fields.
9. Enter the Enter the starting port number and end port number of the internal services in the **Internal Start Port** and **Internal End Port** field.

10. Click **SAVE** to save the changes.

Setting up Port Triggering

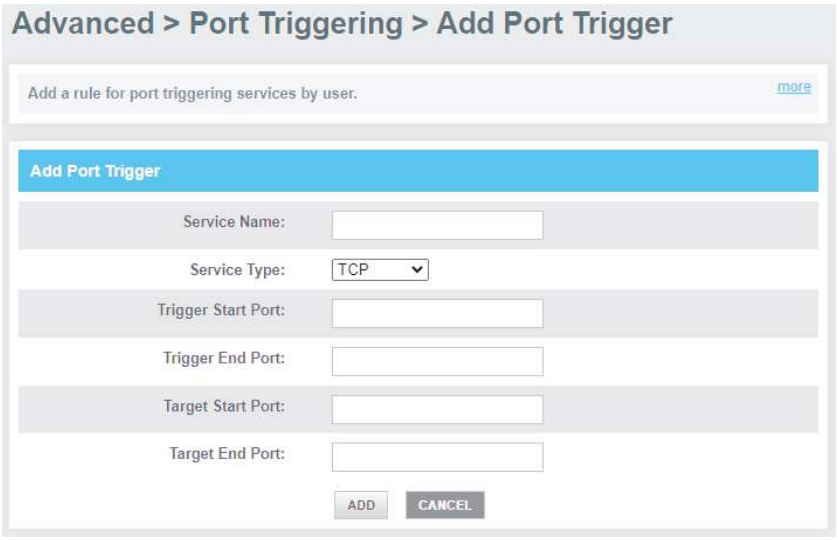
You can use Port Triggering option to set up your G20/G18 to monitor outgoing traffic on specific ports on your home network. Port Triggering can be useful for some applications such as video conferencing, online chatting, and online gaming that may require specific port numbers with bi-directional traffic to function properly.

Note: If your G20/G18 firewall is enabled and custom port triggers are set up, then you must configure the firewall to allow traffic through those custom ports. For more information see *Setting up firewall protection* (page 35).

To configure Port Triggering:

1. From the G20/G18 Web Manager screen, click the **Advanced** menu link.
2. Click **Port Triggering** from the Advanced submenu options list to display the Port Triggering Configuration screen.

3. Click the Port Triggering **Enable** button.
4. Click the **+ADD PORT TRIGGER** button to open the Add Port Trigger screen.



Add Port Trigger screen

5. Enter a name or description for the Port Trigger in the **Service Name** field.
6. Select **TCP/UDP**, **TCP**, or **UDP** from the **Service Type** drop-down list.

7. Enter the starting port number in the **Trigger Port From** field.
8. Enter the ending port number in the **Trigger Port To** field.
9. Enter the starting port number in the **Target Port From** field.
10. Enter the ending port number in the **Target Port To** field.
11. Click **ADD** to create the port trigger.
12. Repeat steps 4 through 11 to create additional port triggers.

Setting up the DMZ host

Warning: The gaming DMZ host is not protected by the G20/G18 firewall. It is exposed to the Internet which makes it vulnerable to attacks or hacking from any client device (e.g., computer or laptop) on the Internet. Consider carefully before configuring a device to be in the DMZ.

You can configure one client device on your home network to be the DMZ Host. That client device will operate outside of the G20/G18 firewall and allow remote access from the Internet to your client device, gaming device, or other IP-enabled device. The DMZ Host feature will only allow outside users to have direct access to the designated DMZ Host device and not your home network.

To create the DMZ host:

1. From the G20/G18 Web Manager screen, click the **Advanced** menu link.
2. Click **DMZ** to display the Advanced DMZ screen.

3. Click the **DMZ Enable** button to set up the DMZ Host on your home network.
4. Enter the last one to three digits (from 2 to 254) of the IP address of the computer or gaming device that you are setting up as the DMZ host
5. Click **SAVE** when you are finished.

Note: To disable the DMZ Host, click the **DMZ Disable** button and then click **SAVE**.

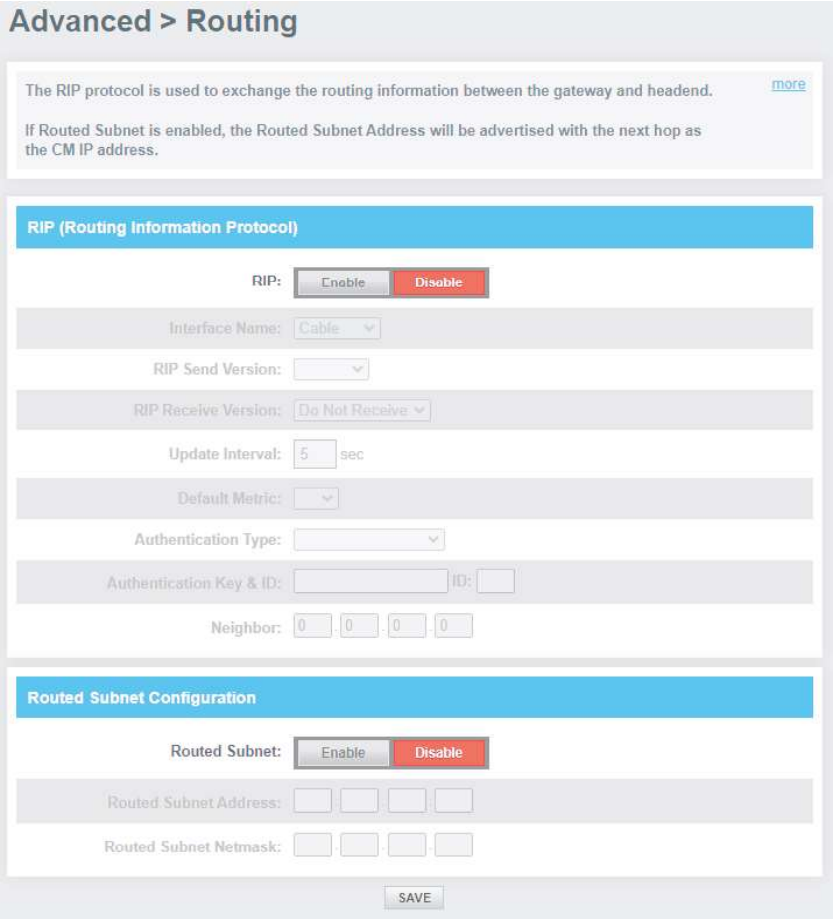
Note: Remember to reset the IP address back to **0** (zero) to close all the ports when you are finished with the needed application. If you do not reset the IP address, that computer will be exposed to the public Internet.

Exchanging the Routing information

The RIP protocol is used to exchange the routing information between the gateway and the headend.

To enable routing information:

1. From the Web Manager screen, click the **Advanced** menu link.
2. Click **Routing** to display the Routing screen.



3. Under **RIP (Routing Information Protocol)** submenu, click **Enable** button and enter the details to set up the routing information.
4. Under **Routed Subnet Configuration** submenu, click **Enable** button to set up the subnet information.
5. Click **SAVE** to save the changes.

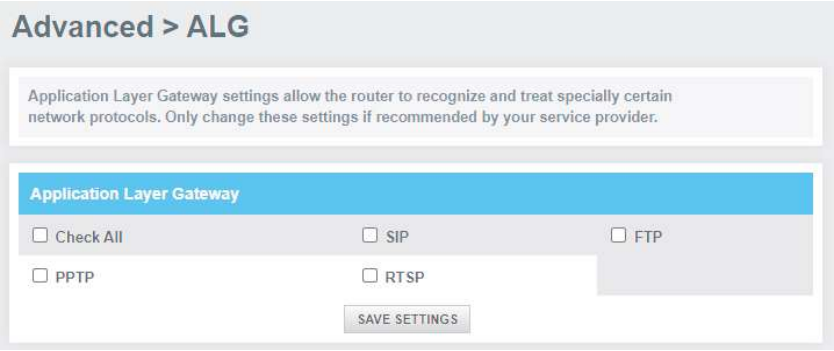
Setting up the ALG

Application Layer Gateway (ALG) allows your router to recognize and treats certain network protocols.

Note: Please change these settings if recommended by your service provider.

To set up the ALG:

1. From the G20/G18 Web Manager screen, click the **Advanced** menu link.
2. Click **ALG** to display the ALG screen.



3. Click the required check boxes and then click **SAVE SETTINGS**.

Setting up Dynamic DNS client

You can configure your Gateway's router functionality as a Dynamic DNS client.

To create as DNS client:

1. From the G20/G18 Web Manager screen, click the **Advanced** menu link.
2. Click **Dynamic DNS** to display the Dynamic DNS client screen.

3. Click the **Enable** button to configure your Gateway's router functionality as DNS client.
4. Click **+ADD DDNS** to configure new DDNS.
5. Click **SAVE** to save the changes.

Note: To disable configuring the DNS client, click the **Disable** button and then click **SAVE**.

Managing the UPnP network

The UPnP enabled gateway discovers all UPnP devices such as printers and computers. Using UPnP, the ports are automatically open for appropriate services and applications.

1. From the G20/G18 Web Manager screen, click the **Advanced** menu link.
2. Click **Device Discovery** to manage UPnP screen.

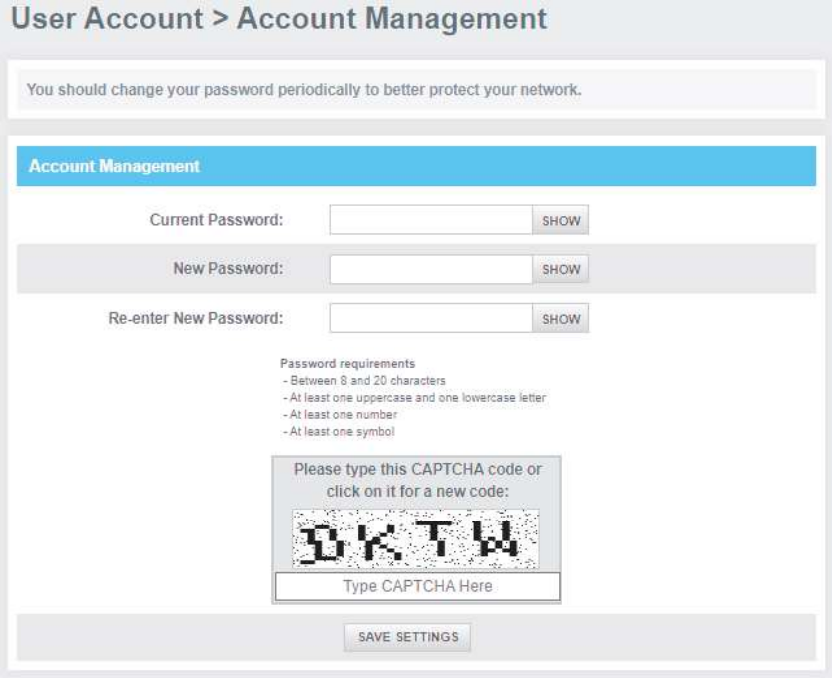
3. Click the **Enable** button for the managing UPnP.
4. Enter the time in the **Advertisement Period** field to allow your gateway to advertise the UPnP information.
5. Enter the number of steps each UPnP advertisement is allowed to propagate before disappearing in the **Time To Live** field.
6. Click the **Enable** button to allow devices such as printers and computers to connect to a network automatically.
7. Click **SAVE**.

Changing your login password

When logging in to the G20/G18 Web Manager for the first time, you will be prompted to enter a new password. However, you can also change your login password again if you want to based on your requirement.

1. Open a web browser and log on to open the G20/G18 Web Manager.

   For more information, see *Starting your G20/G18 Web Manager* (page 25).
2. Click the **Gateway** menu link and then click the **User Account** submenu option.
3. Click **Account Management** and the Account Management page appears.



4. Enter the current admin password in the **Current Password** field.
5. Enter your new admin password in the **New Password** field.

   Note: Remember passwords are case-sensitive and that you can use any combination of the following letters, numbers, and special characters:

   - Letters: **A** through **Z** (uppercase and lowercase)
   - Numbers: **0** to **9**
   - Special characters: **! @ # $ % & ***

6. Enter your new admin password in the **Re-enter New Password** field.
7. Select the **Show Typed Password** checkbox to view the new passwords and confirm that both passwords match.
8. Enter the CAPTCHA code located in the **Type CAPTCHA Here** entry box.
9. Click **SAVE** to update your admin password.
10. Find a secure place to write down and keep your new password for future reference.

Managing your Wi-Fi cable modem and connected networks

You can also use the Web Manager to view and monitor the network configuration settings and operational status of your G20/G18.

Coordinating the Web Interface and Mobile Application

Example:

There are two methods to install and manage your SURFboard device: through the SURFboard Central mobile application OR the device's Web Manager. Both installation processes are simple, but care must be taken to understand the relationship between the different login credentials if you use both methods to manage your device.

First time installation

Installing your device using the SURFboard Central mobile application:

Using the mobile application to install your device requires you to create a SURFboard account. The account login credentials are based on your email address - the mobile application will request and verify an email address as part of the process. The password is generated by the mobile application.

Once your SURFboard account is set up, the mobile application will synchronize your new SURFboard account credentials with the device's Web Manager login credentials. Therefore, the login credentials for your device's Web Manager will be your email address and a password generated by the mobile application. You cannot change this password.

Installing your device using the device's Web Manager

If you install your device using the Web Manager, you do not need to set up a SURFboard account. You use the device's default "admin" username and choose your own password. You may change this password at any time using the Web Manager account management page. The Web Manager will require a login on each use, so you will need to remember your password.

Managing your device after first install

If you use the Web Manager **OR** mobile application exclusively, there are no issues with credential synchronization - you will use the credentials you set up during the installation.

However, if you use both the mobile app **AND** the Web Manager, it is important to understand how the usernames and passwords used by each method are coordinated.

If you installed the device using the Web Manager, and *then* use the mobile application, a SURFboard account using an email address will be created. The mobile application will ask for your password used in the Web Manager. This combination of email address and password will become the new login credentials for the Web Manager. In other words, “admin” will be replaced by your email address.

If you installed the device using the mobile application, and then want to log into the Web Manager, you need to use your SURFboard account credentials. The mobile application can provide the new username and password using the "Access Web Interface" menu option.

Important notes

If you want to continue to use the mobile application, it is important to **NOT** change the username or password using the web interface. This will prevent the mobile application from connecting to the device. The only recovery for this is to factory reset and re-install the device.

The mobile application and web interface are **NOT** designed for simultaneous use. Each may be used at any time, but not at the *same* time.

Viewing the G20/G18 system hardware information

The Gateway Hardware screen displays system hardware information for your G20/G18. This information may be helpful if you contact ARRIS, Comcast, or Cox for technical assistance.

To open the G20/G18 Hardware information screen:

1. From the G20/G18 Web Manager screen, click the **Gateway** menu link.
2. Click **Hardware** from the Gateway submenu links and then click **System Hardware** from the Hardware submenu options.

The Gateway System Hardware screen appears.

Viewing the G20/G18 software version

The Gateway Software Version screen displays device software related information for your G20/G18. This information may be helpful if you have to contact ARRIS or Comcast for technical support.

To open the Software screen of your G20/G18:

1. From the G20/G18 Web Manager screen, click the **Gateway** menu link.
2. Click **Software** from the Gateway submenu links.
   The Gateway Software screen appears.

Viewing the wireless information

You can view your G20/G18 wireless components.

To view the wireless information screen:

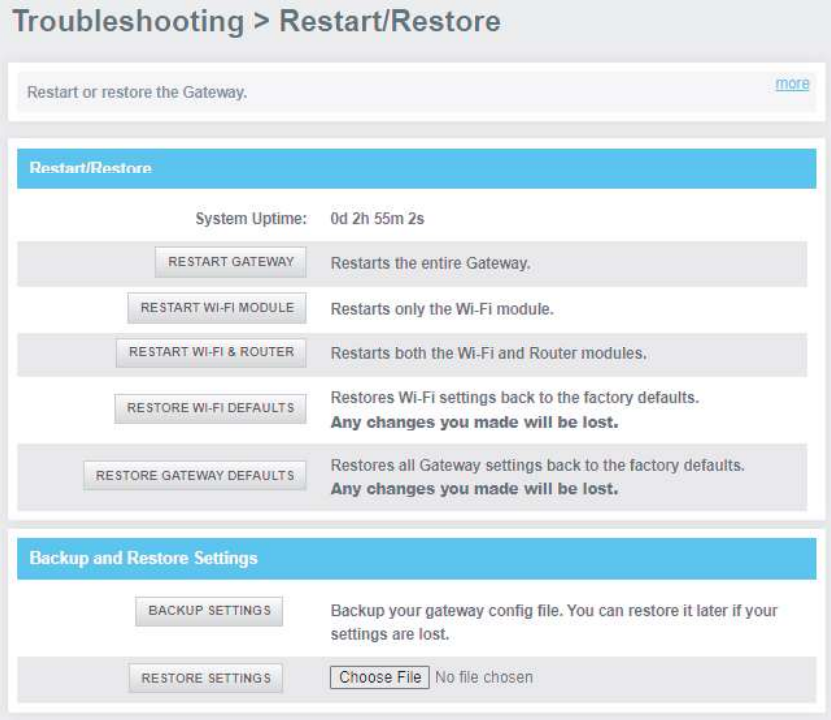
1. From the G20/G18 Web Manager screen, click the **Gateway** menu link.
2. Click **Hardware** from the Gateway submenu links and then click **Wireless** from the Hardware submenu options to display your wireless information screen.

Backup and restore

You can download the current configuration files and then restore those configuration files as required. Your G20/G18 stores the configuration files on your computer for later retrieval. These configuration files are helpful if you want to make temporary changes to your G20/G18 configuration.

To open the G20/G18 Restart/Restore page:

1. From the G20 Web Manager screen, click the **Troubleshooting** menu link.
2. Click **Restart/Restore** from the Troubleshooting submenu options list to display the Restart/Restore screen



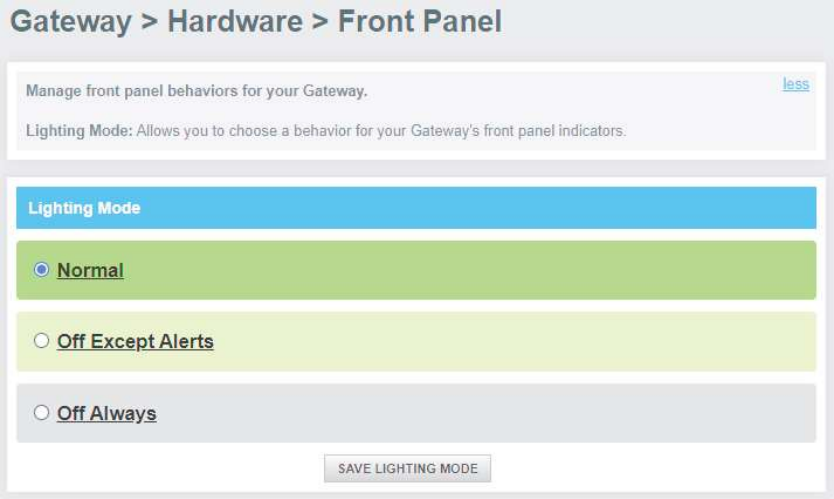
3. Under the **Backup and Restore Settings** tab, click **Backup Settings** to download a set of current configuration files.
4. Under the **Restore Settings** tab, click **Choose File** to select and restore your previously generated backup archive configuration files.

Managing the front panel LED behavior

You can manage the front panel LED behavior of your G20/G18.

To manage the front panel LED behavior:

1. From the G20/G18 Web Manager screen, click the **Gateway** menu link.
2. Click **Hardware** from the Gateway submenu links and then click **Front Panel** from the Hardware submenu options to display the Gateway Front Panel LED screen.



3. You can choose the following settings to manage your front panel LED behavior:
   - **Normal**
   - **Off Except Alerts**
   - **Off Always**
4. Click **SAVE LIGHTING MODE** to save your changes.

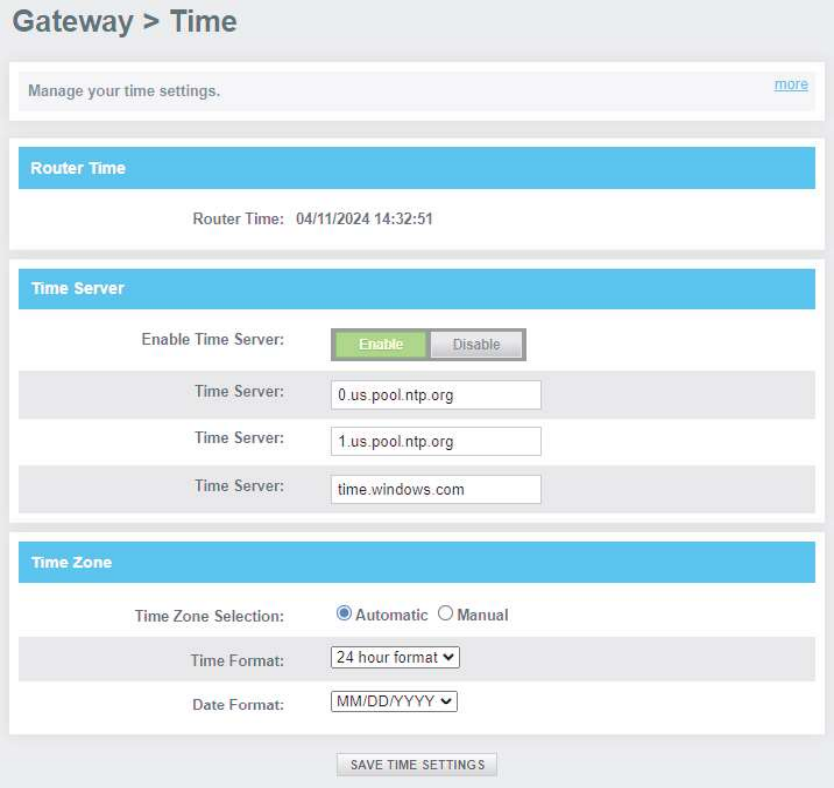
Managing time servers

You can use this feature to provision accurate time on your G20/G18. The time is retrieved from the servers listed in the order. If the first server is not accessible, then the next server shall be used. You can also choose your preferred timezone for accurate local time.

To provision accurate time and to modify the time zone selection:

1. From the G20/G18 Web Manager screen, click the **Gateway** menu link and then click **Time**.

   The Time screen appears.



2. Under the **Time Server** tab, if you prefer to retrieve time from the servers, then click the **Enable** button under **Enable NTP function**.
3. Under the **Time Zone** tab, you can choose to select **Automatic** or **Manual** time zone selection and also specify the **Time Format** and **Date Format**.
4. Click **SAVE TIME SETTINGS**.

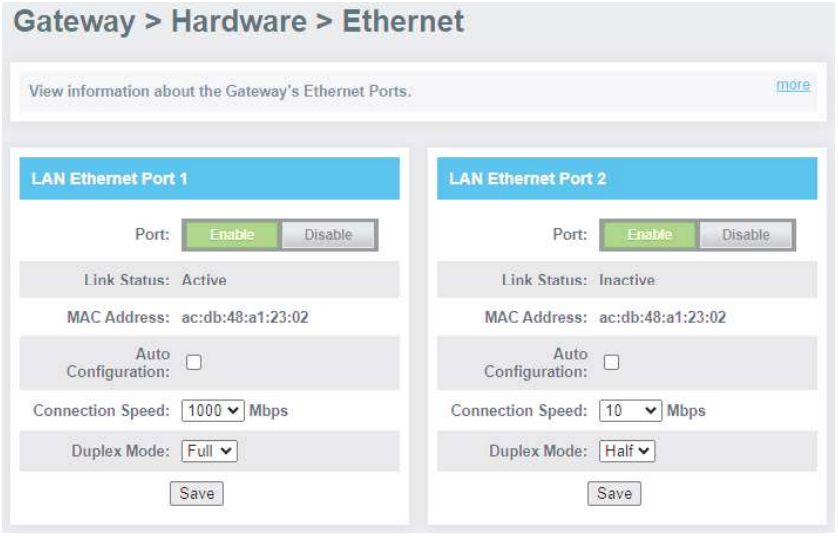
Managing Ethernet ports

You can view and manage your modem's Ethernet ports information

From the G20/G18 Web manager screen, click the **Gateway** menu link.

1. Click **Hardware** from the Gateway submenu links to display the Gateway Software screen.
2. Click **Ethernet** from the Hardware submenu links.

   The Gateway Hardware Ethernet screen appears.



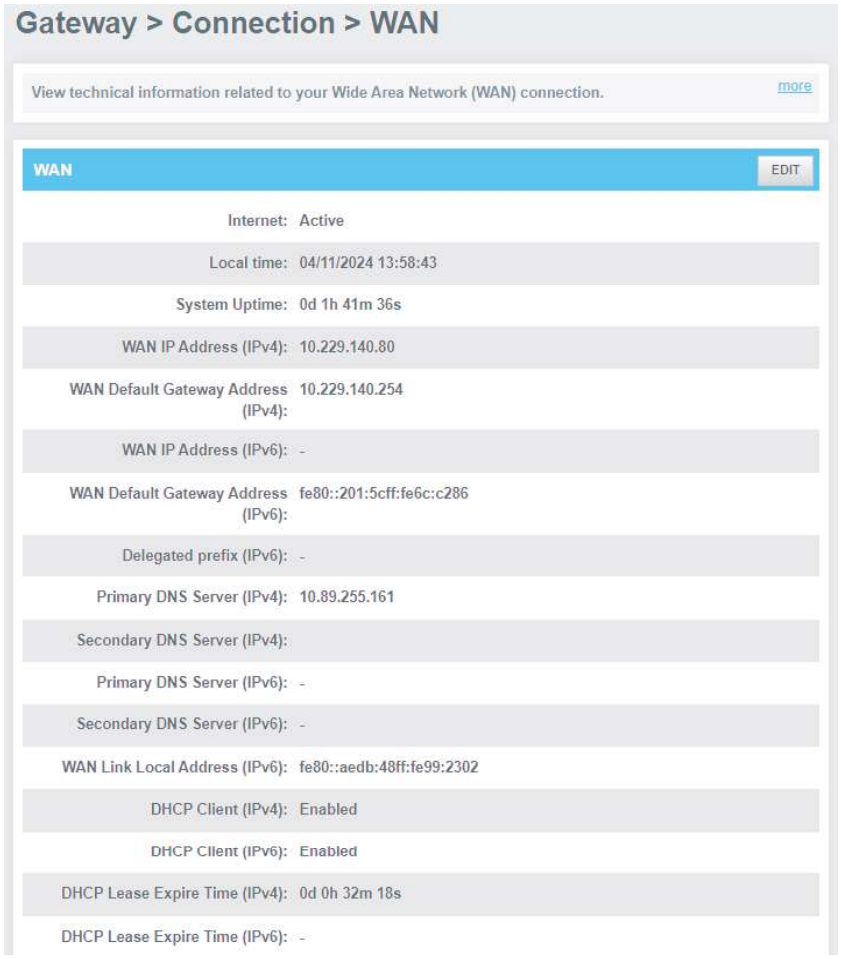
3. Click the **Enable** button in the **LAN Ethernet Port 1** box.
4. Similarly you can click **Enable** button for **LAN Ethernet Port 2**.

Managing WAN configuration settings

If you have installed your G20/G18 using an Ethernet port for your data input, perform the following to activate the Ethernet port.

To open the Gateway hardware Ethernet screen:

1. From the G20/G18 Web manager screen, click the **Connection** menu link to display the **Status** and **WAN** submenu links.
2. Click the **WAN** submenu link to open the Gateway Connection WAN screen.

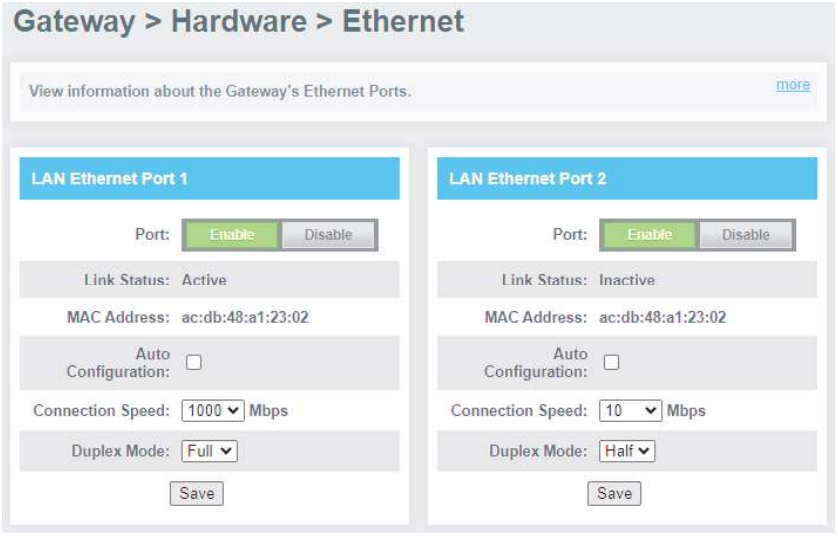


3. Click **EDIT** on the WAN screen.
4. Click **Interface CHANGE** to select either **DOCSIS** (for a regular cable connection) or Ethernet (for an input signal from a different modem device) with an Ethernet connection from the modem device to your G20/G18 top-most 1Gbps Ethernet port.

From the G20/G18 Web manager screen, click the **Gateway** menu link.

1. Click **Hardware** from the Gateway submenu links to display the Gateway Hardware screen.
2. Click **Ethernet** from the Hardware submenu links.

   The Gateway Hardware Ethernet screen appears.



3. Click the **Enable** button in the **LAN Ethernet Port 1** box.

Rebooting your G20/G18

Choose one of the following options to reboot (or restart) your G20/G18:

- Using the Reboot/restore option available on your G20/G18 Web Manager screen: *Rebooting your G20/G18 using the Web Manager* (page 56)

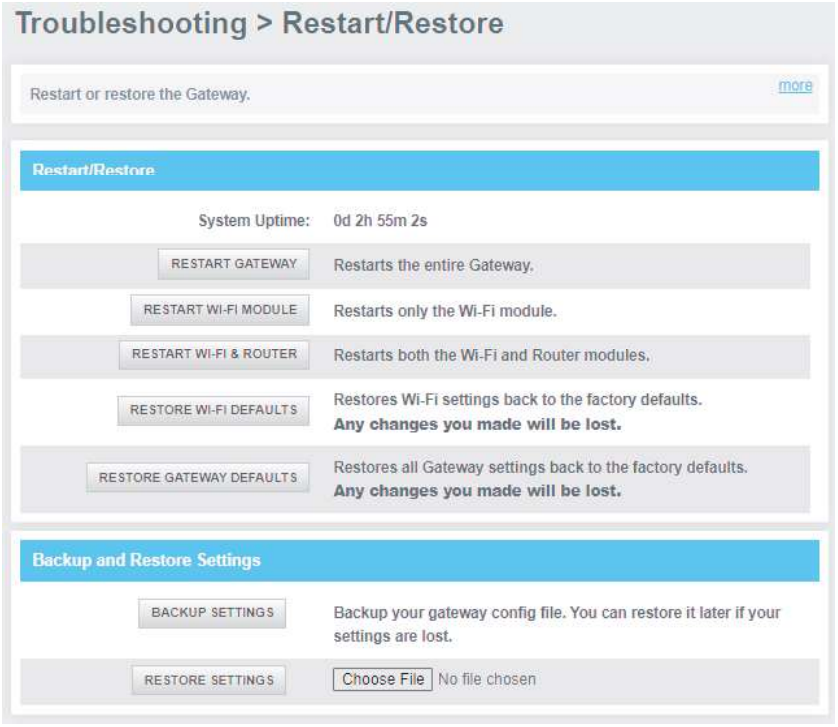
  OR

- Using the Reset button on the rear panel of your G20/G18: *Rebooting your G20/G18 using the Reset button* (page 57)

Rebooting your G20/G18 using the Web Manager

To reboot (or restart) your G20/G18 modem using the Web Manager:

1. From any of the G20/G18 Web Manager screen, click the **Troubleshooting** menu link.
2. Click **Restart/Restore** from the Troubleshooting submenu links.



3. Click **RESTART GATEWAY** located in the Reset/Restore table.

   The following Reset your Gateway message appears.

4. Click **OK** to reboot your G20/G18 modem and then log back in.

Rebooting your G20/G18 using the Reset button

To reboot (or restart) your G20/G18 using the **Reset** button:

1. Insert the end of a paper clip (or other small object with a narrow tip) into the indented **Reset** button opening on the rear panel of your G20/G18.
2. Press and release the small object that you inserted immediately.

   Warning: Do not press the **Reset** button for a few seconds (do not hold the reset button for more than 10 seconds). If you do, your G20/G18 modem shall reset automatically and your custom gateway configuration settings (e.g., admin password, network name (SSID) and password) shall be deleted and replaced with the factory default configuration.

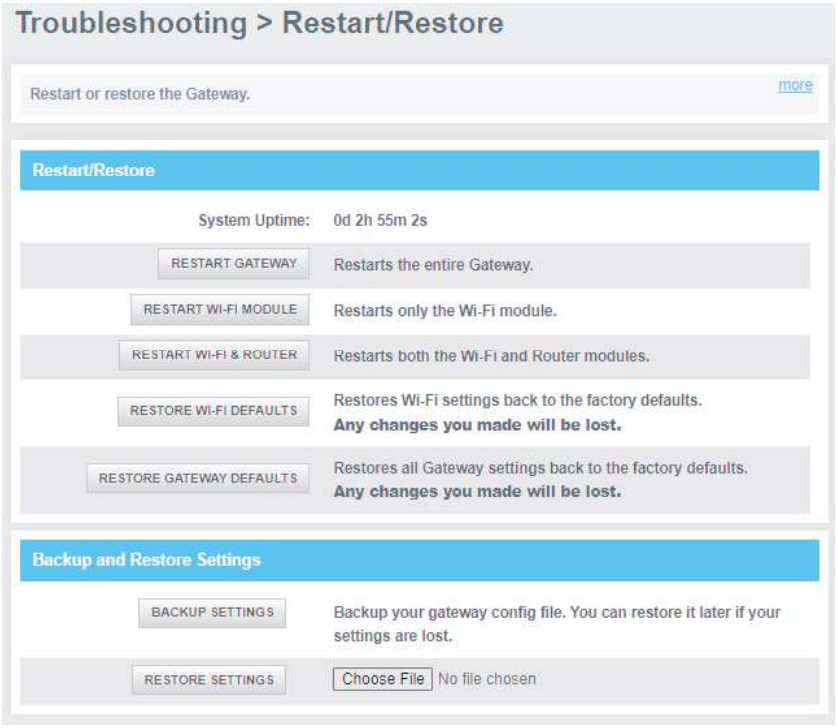
Restoring the default configuration settings using your G20/G18 Web Manager

Warning: This action will delete your current G20/G18 configuration settings and allow you to restore the default (original) G20/G18 configuration.

Note: After the configuration settings are restored, the G20/G18 automatically reboots and you will have to log in using the default username (**admin**) and your current admin password.

To open the Restart/Restore Gateway screen:

1. From the Web Manager screen, click the **Troubleshooting** menu link.
2. Click **Restart/Restore** from the Troubleshooting submenu links to display the Troubleshooting **Restart/Restore** screen.



3. Click **RESTORE Wi-Fi SETTINGS** to reset your G20/G18 Wi-Fi settings.

Restore settings screen

4. Click **OK** to restore the Wi-Fi factory defaults.

   The `Operation in Progress` for restarting the Wi-Fi radios message displays.

Troubleshooting tips

If the solutions listed in the Troubleshooting Solutions table below do not solve your problem, please contact your service provider for assistance.

You may have to reset your G20/G18 configuration to its original factory settings if your G20/G18 is not functioning properly.

Note:

For any additional help and information related to troubleshooting, visit the ARRIS Support website at *https://arris.com/selfhelp* for assistance.

Solutions

G20/G18 Problem	Possible solution
Cannot Send or Receive Data	Check each end of the coaxial cable connection on the G20/G18 and cable wall outlet. Use your hand to tighten each connector, if necessary. Check the Ethernet cable (if connected) to make sure it is properly connected to your G20/G18 and computer. If you have cable television service, check your television to ensure your cable service is operating properly.
Cannot Access the Internet	Check that all cable and power connections on your G20/G18 and computer are properly connected. Check that the front panel LED is lit up solid. Contact your service provider for assistance.
Wi-Fi Devices Cannot Send or Receive Data	If the problem continues after checking the coaxial cable and Ethernet connections and your IP address, check the Wi-Fi **Security Mode** setting on the Gateway Wi-Fi Connection screen. If you enabled Wi-Fi security and configured a passphrase on your G20/G18, be sure each affected Wi-Fi client has the identical passphrase. If this does not solve the problem, check if the Wi-Fi client supports the selected Wi-Fi security method.

Vantiva USA LLC
4855 Peachtree Industrial Blvd., Suite 200
Norcross, GA 30093