

SURFboard™



SURFboard® SBG6950AC2, SBG7400AC2 DOCSIS 3.0 Wireless Gateways with ARRIS Secure Home Internet by McAfee®

User Guide

June 2017

Copyright 2017, ARRIS Enterprises, LLC. All rights reserved.

ARRIS Copyrights and Trademarks

© 2017 ARRIS Enterprises, LLC. All rights reserved.

No part of this publication may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from ARRIS Enterprises, LLC ("ARRIS"). ARRIS reserves the right to revise this publication and to make changes in content from time to time without obligation on the part of ARRIS to provide notification of such revision or change.

ARRIS, SURFboard, and the ARRIS logo are all trademarks of ARRIS Enterprises, LLC. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks or the names of their products. ARRIS disclaims proprietary interest in the marks and names of others.

Wi-Fi Alliance®, Wi-Fi®, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access® (WPA), the Wi-Fi Protected Setup logo, and WMM® are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance.

ARRIS provides this guide without warranty of any kind, implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. ARRIS may make improvements or changes in the product(s) described in this manual at any time.

The capabilities, system requirements and/or compatibility with third-party products described herein are subject to change without notice.

Table of Contents

1. Safety and Regulatory Information	5
Important Safety Instructions.....	5
FCC Statements.....	7
Wireless LAN Information.....	8
Caring for the Environment by Recycling Your ARRIS Equipment.....	9
2. Getting Started	10
Introduction	10
In The Box	10
System Requirements.....	11
Contact Information	12
3. Product Overview	13
Front Panel	13
Wi-Fi Protected Setup™ (WPS)	14
Rear Panel.....	15
Gateway Label	17
4. Installing the Gateway	18
Connect Your Wireless Gateway and Computer	18
Establish an Internet Connection	19
5. Setting Up a Wi-Fi Network Connection	21
Set Up a Wi-Fi Network Connection Using the ARRIS SURFboard Manager.....	21
Set Up a Wi-Fi Network Connection Using Your Client Device	23
Quick Connect Using the Windows Taskbar	24
Connect Using the Windows Control Panel.....	26
Connect Your WPS-Enabled Device	29
Test Your Wi-Fi Network Connection	29
6. Using the Gateway Web Manager	30
Start the Gateway Web Manager.....	30
Gateway Web Manager Menu Bar	33
Gateway Web Manager-Available Languages.....	34
Get Help.....	35
Exit the Gateway Web Manager.....	36
7. Configuring Your Wi-Fi Network	37
Set Up Your Wi-Fi Network.....	37

Change Your Wi-Fi Network Name (SSID)	40
8. Protecting & Monitoring Your Wi-Fi Network	43
Prevent Unauthorized Access.....	43
Change the Default User Password	43
Set Up Firewall Protection	45
Set Up Parental Controls	47
Set Up IP Filtering	47
Set Up MAC Address Filtering.....	49
Set Up Port Triggers.....	50
Set Up the DMZ Host	51
9. Managing Your Gateway and Connected Networks	53
View the Gateway Status and Network Connection	53
View the Gateway Product and Status Information.....	54
Back Up Your Gateway Configuration	55
Restore the Gateway Configuration Settings	56
Reset the Gateway Configuration Settings.....	57
Exit the Gateway Web Manager.....	58
10. Troubleshooting Tips.....	59
Solutions	59
Front Panel LED Icons and Error Conditions.....	60
11. Warranty Information	61

Safety and Regulatory Information

Important Safety Instructions

Read This Before You Begin — When using your equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock, and injury to persons, including the following:

- Read all of the instructions listed here and/or in the user manual before you operate this device. Give particular attention to all safety precautions. Retain the instructions for future reference.
- This device must be installed and used in strict accordance with manufacturer's instructions, as described in the user documentation that is included with the device.
- Comply with all warning and caution statements in the instructions. Observe all warning and caution symbols that are affixed to this device.
- To prevent fire or shock hazard, do not expose this device to rain or moisture. The device must not be exposed to dripping or splashing. Do not place objects filled with liquids, such as vases, on the device.
- This device was qualified under test conditions that included the use of the supplied cables between system components. To ensure regulatory and safety compliance, use only the provided power and interface cables and install them properly.
- Different types of cord sets may be used for connections to the main POWER supply circuit. Use only a main line cord that complies with all applicable device safety requirements of the country of use.
- Installation of this device must be in accordance with national wiring codes and conform to local regulations.
- Operate this device only from the type of power source indicated on the device's marking label. If you are not sure of the type of power supplied to your home, consult your dealer or local power company.
- Do not overload outlets or extension cords, as this can result in a risk of fire or electric shock. Overloaded AC outlets, extension cords, frayed power cords, damaged or cracked wire insulation, and broken plugs are dangerous. They may result in a shock or fire hazard.
- Route power supply cords so that they are not likely to be walked on or pinched by items placed upon or against them. Pay particular attention to cords where they are attached to plugs and convenience receptacles, and examine the point where they exit from the device.

- Place this device in a location that is close enough to an electrical outlet to accommodate the length of the power cord.
- Place the device to allow for easy access when disconnecting the power cord of the device from the AC wall outlet.
- Do not connect the plug into an extension cord, receptacle, or other outlet unless the plug can be fully inserted with no part of the blades exposed.
- Place this device on a stable surface.
- Avoid damaging the device with static by touching the coaxial cable when it is attached to the earth-grounded coaxial cable-TV wall outlet.
- Always first touch the coaxial cable connector on the device when disconnecting or reconnecting the Ethernet cable from the device or user's PC.
- Installation of an AC surge protector in the AC outlet to which this device is connected is recommended. This is to avoid damaging the device by local lightning strikes and other electrical surges.
- Postpone installation until there is no risk of thunderstorm or lightning activity in the area.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There is a remote risk of electric shock from lightning. For added protection, unplug the device from the wall outlet and disconnect the cables to avoid damage to this device from lightning and power surges.
- Do not use this product near water. For example, near a bathtub, washbowl, kitchen sink, laundry tub, swimming pool, or in a wet basement.
- Do not use the telephone to report a gas leak in the vicinity of the leak.
- Do not cover the device or block the airflow to the device with any other objects. Keep the device away from excessive heat and humidity and keep the device free from vibration and dust.
- Wipe the device with a clean, dry cloth. Never use cleaning fluid or similar chemicals. Do not spray cleaners directly on the device or use forced air to remove dust.
- For added protection, unplug the device from the wall outlet and disconnect the cables to avoid damage to this device during lightning activity or power surges.



Caution: To reduce the risk of fire, use only No. 26 AWG or larger (e.g., 24 AWG) UL Listed or CSA Certified Telecommunication Line Cord, or national equivalent.

- Upon completion of any service or repairs to this device, ask the service technician to perform safety checks to determine that the device is in safe operating condition.
- Do not open the device. Do not perform any servicing other than that contained in the installation and troubleshooting instructions. Refer all servicing to qualified service personnel.
- This device should not be used in an environment that exceeds 104° F (40° C).

SAVE THESE INSTRUCTIONS



Note to CATV System Installer — This reminder is provided to call the CATV system installer’s attention to Section 820.93 of the National Electric Code, which provides guidelines for proper grounding and, in particular, specifies that the Coaxial cable shield must be connected to the grounding system of the building, as close to the point of cable entry as practical.

FCC 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 harmful interference in a residential environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the device 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 device and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

FCC Caution: Any changes or modifications not expressly approved by ARRIS could void the user’s authority to operate the equipment.

FCC Declaration of Conformity

ARRIS Enterprises, LLC, 3871 Lakefield Drive, Suwanee, GA 30024, declares that the SURFboard DOCSIS 3.0 Wireless Gateway-SBG6950AC2 and SBG7400AC2 comply with 47 CFR Parts 2 and 15 of the FCC rules as a Class B digital device.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. To comply with the FCC RF exposure compliance requirements, the separation distance between the antenna and any person’s body (including hands, wrists, feet and ankles) must be at least 8 inches (20 centimeters).

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter except those already approved in this filing.

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 destinations. The firmware setting is not accessible by the end user.

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, and Revision N), 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).



Restrictions on the Use of Wireless Devices

In some situations or environments, the use of wireless devices may be restricted by the proprietor of the building or responsible representatives of the organization. For example, using wireless equipment in any environment where the risk of interference to other devices or services is perceived or identified as harmful.

If you are uncertain of the applicable policy for the use of wireless equipment in a specific organization or environment, you are encouraged to ask for authorization to use the device prior to turning on the equipment.

The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of the devices included with this product, or the substitution or attachment of connecting cables and equipment other than specified by the manufacturer. Correction of the interference caused by such unauthorized modification, substitution, or attachment is the responsibility of the user.

The manufacturer and its authorized resellers or distributors are not liable for any damage or violation of government regulations that may arise from failing to comply with these guidelines.



Note: The use of the 5150-5250 MHz frequency band is restricted to Indoor Use Only.

Security Warning: This device allows you to create a wireless network. Wireless network connections may be accessible by unauthorized users. For more information on how to protect your network, see [Protecting & Monitoring Your Wi-Fi Network](#) (page 44) in this guide for more information or visit the ARRIS Support website at www.arris.com/selfhelp.

Caring for the Environment by Recycling Your ARRIS Equipment



Please do not dispose of this product or any included electronic accessories, i.e., power supply or battery, with your residential or commercial waste. ARRIS devices may be disposed of through the ARRIS Product Recycling program, further described at corporateresponsibility.arrisi.com/phoenix.zhtml. You may also contact your local community authorities for information regarding where you may dispose of your ARRIS devices.

Getting Started

Introduction

Welcome to the next generation of the ultra-high-speed DOCSIS 3.0 ARRIS SURFboard® wireless gateways, SBG6950AC2 and SBG7400AC2, with the new ARRIS Secure Home Internet by McAfee App. This app provides security, Internet access, and Parental Control management for all of the connected devices (e.g., smartphones, tablets, computers, Smart TVs, gaming consoles, etc.) on your home network. It is available online as a free download for your mobile devices using Google Play (for Android devices) or the App store (for Apple devices). For more information on downloading and using the ARRIS Secure Home Internet by McAfee App, refer to the **ARRIS Secure Home Internet User Guide** available online at www.arris.com/selfhelp.

Your SURFboard wireless gateway is a combination DOCSIS 3.0 cable modem and four-port Ethernet router with Wi-Fi. It uses DOCSIS 3.0 technology to provide ultra high-speed Internet access on your home or small business network. Using the connection capabilities of the gateway, you can connect your computer and other network-enabled devices via the four Ethernet ports or the 2.4 GHz and 5 GHz Wireless connections. Your wireless gateway will connect to the existing coaxial cable connection in your home. It also includes a Wi-Fi® Pairing (WPS) button option for quick and easy connections for your WPS-enabled devices.

This guide provides instructions for installing and configuring your wireless gateway, setting up secure Wi-Fi network connections, and managing your gateway and network configurations.

In The Box

Before installing your wireless gateway, check that the following items are also included in the box. If any items are missing, please call ARRIS Technical Support at **1-877-466-8646** for assistance.

Table 1. Wireless Gateway Package Contents

Item	Image	Description
Wireless Gateway SBG6950AC2 SBG7400AC2		High-speed DOCSIS 3.0 cable modem, wireless access point, and four-port Ethernet router

Item		Description
Power Adapter		Power adapter for an electrical wall outlet connection
Ethernet Cable		Standard Category 5e (CAT5e) or higher network cable
Software License & Warranty Card		Contains safety and regulatory information, software license, and warranty for your wireless gateway.
Support Information Card		Provides contact information for obtaining technical support assistance with any issues you may have with your wireless gateway.
Wireless Gateway Quick Start Guide		Provides information for installing your wireless gateway and setting up a secure Wi-Fi connection on your home network.

Additional Items Needed (Not Included)

The following items are not included in the box and must be purchased separately, if required:

- Coaxial (coax) cable, if one is not already connected to a cable wall outlet
- RF splitter (for additional coaxial cable connections, such as a set-top box or Smart TV)
- Ethernet cable for each additional Ethernet-enabled device

System Requirements

- High-speed Internet access account
- Web browser access – Internet Explorer, Google Chrome, Firefox, or Safari
- Compatible operating systems:
 - 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 this model.

- Mac® 10.4 or higher
- UNIX®
- Linux®

Contact Information

For technical support and additional ARRIS product information:

- Visit the ARRIS Support website: www.arris.com/selfhelp
- Call ARRIS Technical Support: **1-877-466-8646**

Product Overview

Front Panel



Figure 1: SBG6950AC2 & SBG7400AC2 Front Views

Table 2. Wireless Gateway Front Panel LED Icons

LED Icon	Blinking	On (Solid)
 POWER	Not applicable – icon does not blink.	Power is properly connected.
 SEND RECEIVE	Scanning for upstream (send) and downstream (receive) channel connections.	Upstream (Send) and Downstream (Receive) channels are connected.
 ONLINE	Scanning for an Internet connection.	Gateway is connected to the network.

LED Icon	Blinking	On (Solid)
 WIRELESS	Wi-Fi enabled with encrypted or unencrypted wireless data activity.	Any of the following applies: 2.4 GHz wireless connection is made between your wireless gateway and a Wi-Fi enabled device on your home network; for example, Wi-Fi telephone, tablet, or laptop. The WPS Pairing process between your wireless gateway and the WPS-enabled device was successful. The WPS Pairing process either failed or did not complete after two minutes.
 WIRELESS	Wi-Fi enabled with encrypted or unencrypted wireless data activity.	Any of the following applies: 5 GHz wireless connection is made between your wireless gateway and a Wi-Fi enabled device on your home network; for example, Wi-Fi telephone, tablet, or laptop. The WPS Pairing process between your wireless gateway and the WPS-enabled device was successful. The WPS Pairing process either failed or did not complete after two minutes.
WPS	WPS Pairing process is underway between your wireless gateway and a WPS-enabled device.	WPS-enabled device is connected.
 USB	Not applicable – no LED on port.	Not applicable – no LED on port.

Wi-Fi Protected Setup™ (WPS)

Wi-Fi Protected Setup (WPS) is a Wi-Fi network setup option that provides a quick and easy solution for setting up a secure Wi-Fi network connection for any WPS-enabled device; such as a computer, tablet, gaming device, or printer. WPS automatically configures your Wi-Fi network connections and sets up Wi-Fi security. See [Connect Your WPS-Enabled Device](#) (page 29) for more information.

Rear Panel

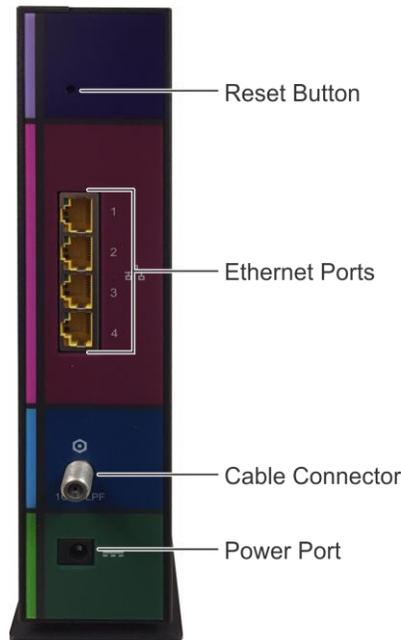


Figure 2: Wireless Gateway Rear View

Table 3. Wireless Gateway Rear Panel Ports & Connectors

Port Name	Description
Reset Button	<p>Recessed button located on the rear panel of your wireless gateway can be used to either reboot your gateway or reset your gateway configuration settings.</p> <p>To reboot (or restart) your wireless gateway:</p> <ol style="list-style-type: none"> 1. Insert the end of a paper clip or other small object with a narrow tip into the Reset opening on the rear panel of your wireless gateway. 2. Press and hold the indented Reset button for three to four seconds only. 3. Remove the paper clip or small object from the Reset opening. <p>To reset your wireless gateway configuration back to the factory default settings:</p> <ol style="list-style-type: none"> 1. Insert the end of a paper clip or other small object with a narrow tip into the Reset opening on the rear panel of your wireless gateway. 2. Press and hold the Reset button for 10 seconds. 3. Remove the paper clip or small object from the Reset opening. <p>See Reset the Gateway Configuration Settings (page 57) for more information on resetting your gateway configuration settings using the wireless gateway Web Manager.</p>

Port Name	Description
Reset Button (Continued)	 WARNING! Resetting the gateway configuration settings to the factory defaults will also delete your custom gateway configuration, including your user password, Wi-Fi network name (SSID), and other configuration settings. You should first back up your gateway configuration files before resetting your wireless gateway. See Back Up Your Gateway Configuration (page 55) for more information.
 ETHERNET 10/100/1000	<p>Four one-gigabit Ethernet ports for RJ-45 network cable connections:</p> <ul style="list-style-type: none"> ■ Green: LED is ON - Indicates a data transfer rate of one gigabit per second ■ Green: LED is Blinking - Indicates data traffic is in progress ■ Amber: LED is ON - Indicates a data transfer rate of less than one gigabit per second ■ Amber: LED is Blinking - Indicates data traffic is in progress
 CABLE	Coaxial cable connector
Power Port	<p>100 - 240 VAC Power connector</p>  WARNING! To avoid any damage to your wireless gateway, only use the power cord provided in the box.

Gateway Label



Figure 3: Sample SBG6950AC2 & SBG7400AC2 Labels

The gateway label is located on the bottom of your wireless gateway. It contains the gateway information that you may need when contacting your service provider or [ARRIS Technical Support](#) (page 12).

To receive Internet service, contact your service provider for assistance. You may have to provide the following information listed on the gateway label:

- Gateway Model name (**SBG6950AC2** or **SBG7400AC2**)
- Gateway MAC address (**HFC MAC**)
- Gateway Serial number (**SN**)

Installing the Gateway



Caution: 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.

Connect Your Wireless Gateway and Computer

Before installing your wireless gateway:

- Check with your service provider (or local cable company) to ensure broadband cable service is available in your area.

To set up a wireless network, you will need a high-speed Internet connection provided by an Internet service provider.



Note: When contacting your service provider, you may need your gateway information listed on the gateway label on the bottom of your wireless gateway (see [Gateway Label page 17](#)).

- Choose a location in your home where your computer and wireless gateway are preferably near existing cable and electrical wall outlets.

For the best Wi-Fi coverage, a central location in your home or building is recommended.



Note: The following installation procedure covers the wired Ethernet connection process so that you can confirm that your wireless gateway was properly installed and can connect to the Internet.

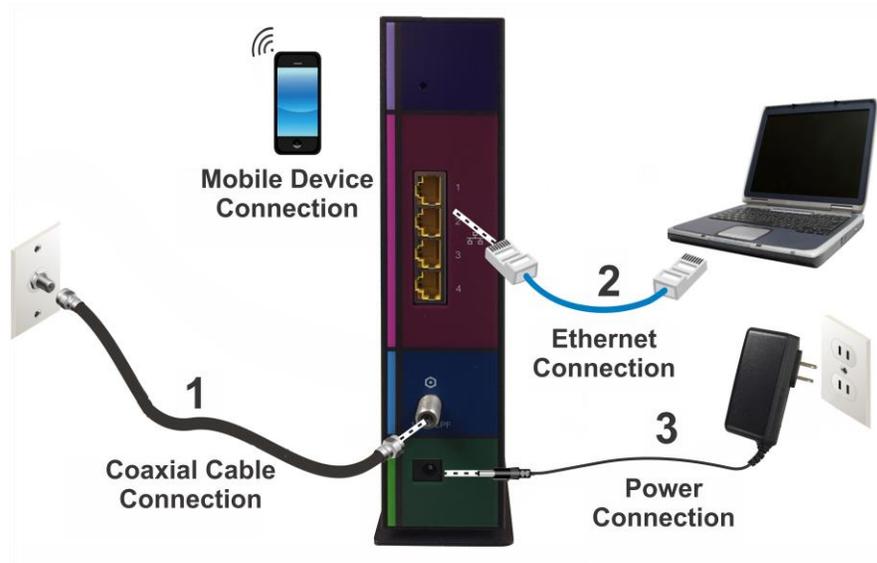


Figure 4: Wireless Gateway Connection Diagram

1. Check that a coaxial cable is already connected to a cable wall outlet or RF splitter (not included).
2. Connect the other end of the coaxial cable to the **Cable** connector on the rear of your wireless gateway.
Use your hand to tighten the connectors to avoid damaging them.
3. Connect the Ethernet cable to an available **Ethernet** port on the rear of your wireless gateway.
4. Connect the other end of the Ethernet cable to the **Ethernet** port on your computer.
Optional: Repeat steps 3 and 4 for an additional computer or other network device that you want to install as a wired connection on your home network.
5. Connect the power cord to the **Power** port on the rear of your wireless gateway.
6. Plug the other end of the power cord into an electrical wall outlet that is not controlled by a wall switch.



Note: This automatically powers **ON** your wireless gateway. There may be up to a 15 second delay for the **Power** LED on the gateway front panel to light up after the power is connected.

Establish an Internet Connection

Although your computer may already be configured to automatically access the Internet, you should still perform the following gateway connectivity test to verify that the devices were connected properly.

1. Power **ON** the computer connected to your wireless gateway if it is turned off, and then log in.

2. Contact your service provider to activate (provision) your wireless gateway. You may have to provide the **HFC MAC** ID listed on the gateway label.



Note: *Your service provider may allow for automatic activation, which will automatically launch their own special website on your computer when you open a web browser.*

3. After your wireless gateway is provisioned (or activated), open a web browser (such as Internet Explorer, Google Chrome, Firefox, or Safari) on your computer.
4. Type a valid URL (such as www.surfboard.com) in the address bar and then press **Enter**. The ARRIS website should open. If the website fails to open, please contact your service provider for assistance.
5. Check that the **Power**, **Upstream/Downstream**, and **Online** front panel LEDs on your wireless gateway light up in sequential order. See [Front Panel](#) (page 13) for additional LED status information.
 - If all four LEDs did not light up solid and you also do not have an Internet connection, you may have to contact your service provider to reactivate your wireless gateway or check for signal issues.
 - If you still cannot connect to the Internet, please call ARRIS Technical Support at **1-877-466-8646** for assistance.

Setting Up a Wi-Fi Network Connection

ARRIS recommends that you first verify that your computer (or laptop) can access the Internet using a wired Ethernet connection before configuring your Wi-Fi network.

You must currently have access to an Internet service in your home before you can set up a Wi-Fi network connection. If you do not have Internet service already set up in your home, contact a broadband service provider of your choice for assistance. Before proceeding, check that your connected client device (e.g., laptop or personal computer) and your wireless gateway can connect to the Internet.

There are four methods available to set up your Wi-Fi network connection on your home network. Choose one of the following connection options:

- [Set Up a Wi-Fi Network Connection Using the ARRIS SURFboard Manager](#)
- [Set Up a Wi-Fi Network Connection Using Your Client Device](#)
- [Quick Connect Using the Windows Taskbar](#)
- [Connect Using the Windows Control Panel](#)

Set Up a Wi-Fi Network Connection Using the ARRIS SURFboard Manager

1. Check that your wireless gateway is powered ON and connected to the Internet.
2. Click either the **Google Play** or **App Store** link to download the ARRIS SURFboard Manager app for your Android or iOS mobile device:

- **Google Play:**

play.google.com/store/apps/details?id=com.arris.SURFboardManager&hl=en

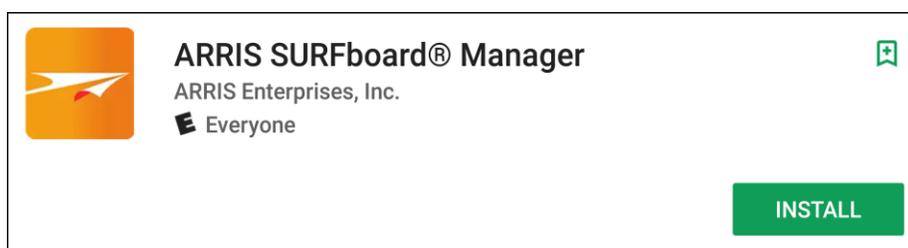


Figure 5: ARRIS SURFboard Manager Installation for Android Devices

- **App Store:**

itunes.apple.com/us/app/arris-surfboardmanager/id1061716447?mt=8

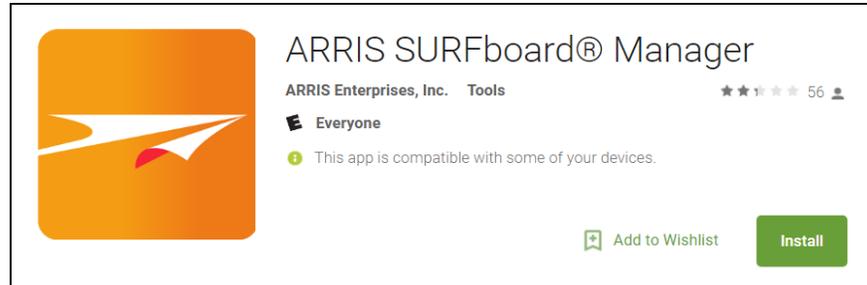


Figure 6: ARRIS SURFboard Manager Installation for Apple (iOS) Devices

3. Click **Install**.



Note: After the installation is finished, the application icon will appear on your mobile device Apps or home screen.

4. Tap **Open** and then tap **OK**.

The Thank You screen will display.

5. Tap **CONTINUE** and then choose one of the following:

- Tap **Please Scan the QR Label** to scan the QR code on your gateway label.
- Tap **SKIP** to search for available Wi-Fi networks.
The Device Connection screen will display.

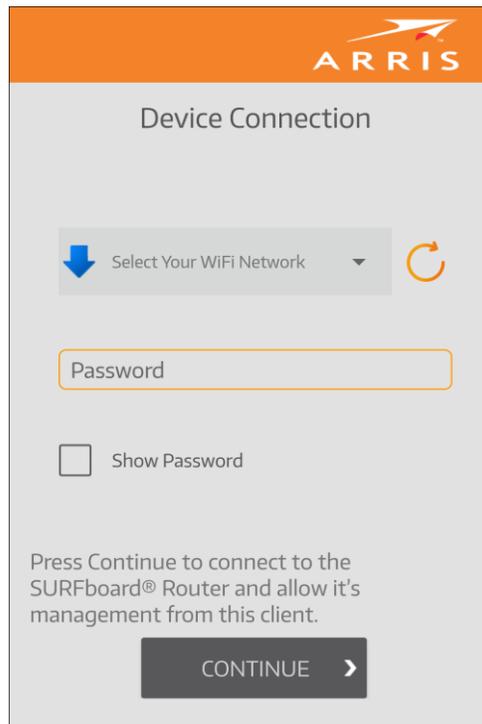


Figure 7: Device Connection Screen

6. Tap  to display the list of available Wi-Fi networks.
7. Tap the Wi-Fi network name to select the Wi-Fi network that you want to connect to.

8. Enter the network password to log on.
Tap the **Show Password** selection box to display your password to confirm that you entered it correctly.
9. Tap **CONTINUE** to connect to your Wi-Fi network.

Set Up a Wi-Fi Network Connection Using Your Client Device



Note: You will need the **Wi-Fi Network Name (SSID)** and **Wi-Fi Security Key (Network Password)** to connect your client devices to your home network. The default network name and network password are listed on the gateway label.

Choose one of the options listed below for the client device you are using to set up a Wi-Fi network connection on your home network. Repeat for each additional device:

- **Personal Computer (PC)** – Select one of the following:
 - [Quick Connect Using the Windows Taskbar](#)
 - [Connect Using the Windows Control Panel](#)

The steps for setting up your Wi-Fi network connection may differ slightly depending on the version of Microsoft Windows running on your client device. The steps used in this section apply to Windows 7.

- **Android Device**

From any screen on your client device:

- a. Select to open the Settings screen.
- b. Select **Wi-Fi** to turn it ON.

Your device will automatically start searching and then display a list of available Wi-Fi networks.

- c. Select your Wi-Fi network name (SSID) from the list.
- d. If prompted, type your Wi-Fi Security Key (network password).
Please note that your network password may be case-sensitive.
- e. Select **Connect**.

If your Wi-Fi network connection is successful, “Connected” will display under your network name.

Apple Computer

From any screen on your client device:

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



Note: Checkmark **Remember this network** if you want your Mac computer/client device to automatically connect to your home network when you log on. Your computer must be within range of your Wi-Fi network to connect to it.

- d. Click **OK**.

Apple Mobile Device

From the Home screen on your client device:

- a. Select **Settings** to open the Wi-Fi screen.
- b. Select **Wi-Fi** to turn it ON.

Your device will automatically start searching and then list the available Wi-Fi networks.

- c. Select the Wi-Fi network name (SSID) for your home network from the list to connect it.

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 Taskbar

1. From the Windows taskbar on your computer, click the **Wi-Fi Link** icon (see Figure 8) to open the list of available Wi-Fi networks (see Figure 9).



Figure 8: Sample 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.



Figure 9: Sample Available Wi-Fi Networks Window

2. Locate and left-click on the wireless gateway Wi-Fi network name or SSID (for example, **ARRIS-####**) for your wireless gateway from the list of available Wi-Fi networks. The default SSID is located on the gateway label on the bottom of your wireless gateway.



Note: You must use the default SSID listed on the gateway label when installing the gateway and setting up your first Wi-Fi network connection. You can change the SSID after your network connections are up and running. See [Change Your Wi-Fi Network Name \(SSID\)](#) (page 41) for more information.



Figure 10: 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.



Figure 11: Network Connection Window

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 Gateway label or enter your own personal Wi-Fi network password. See [Prevent Unauthorized Access](#) (page 44) for more information on creating user passwords.

If you have already changed your Wi-Fi network password using the gateway Web Manager, enter that password in the **Security key** field.



Figure 12: Network Connection-Create Network Password Window

6. Select **Hide characters** and then click **OK** to encrypt your network password.

Connect 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.

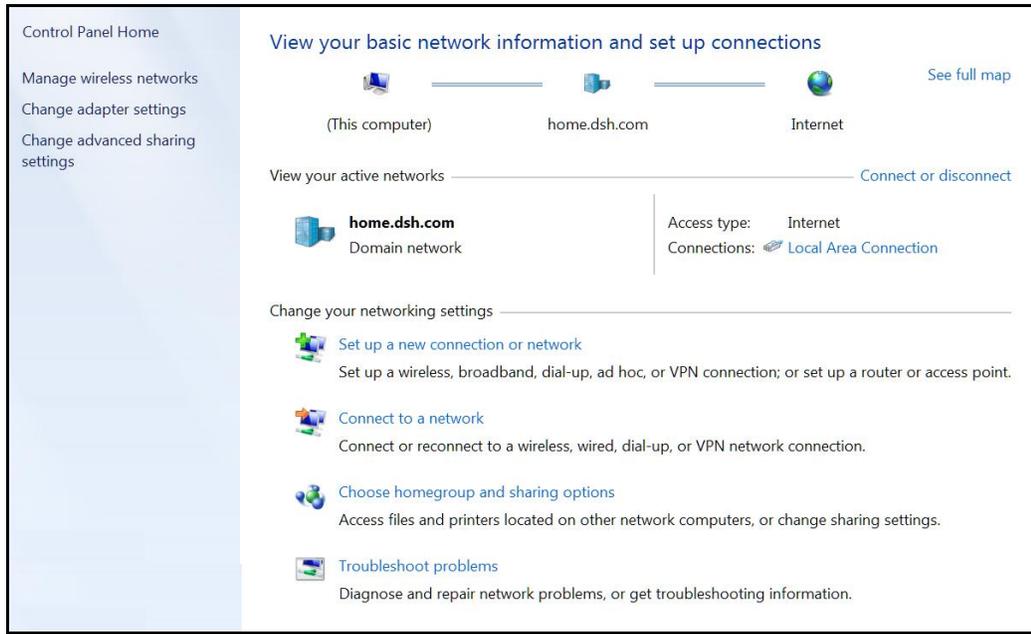


Figure 13: Control Panel-Network and Sharing Center Window

3. Click **Manage wireless networks** under Control Panel Home side panel to open the Manage Wireless Networks window.
4. Click **Add** to open the Manually Connect to a Wireless Network window.

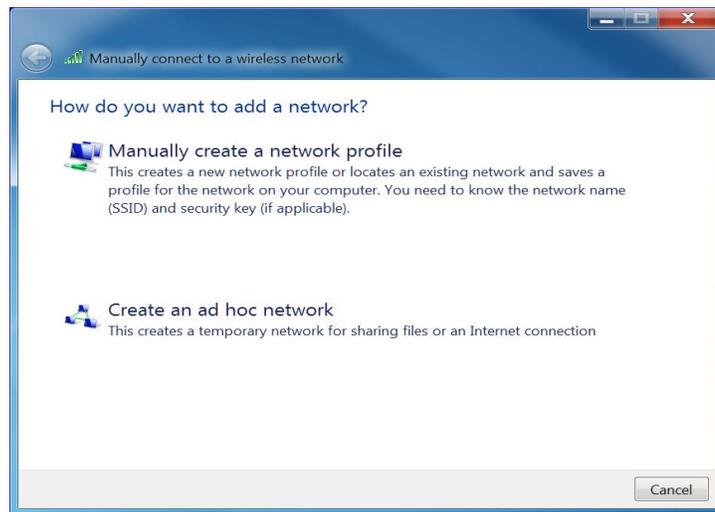


Figure 14: Manually Connect to a Wireless Network Window

5. Click **Manually create a network profile** to open another Manually Connect to a Wireless Network window.



Figure 15: Manually Connect to a Wireless Network Window

6. Enter the gateway Wi-Fi network name or SSID (**ARRIS-####**) for your wireless gateway in the **Network name** field.

The default SSID is listed on the gateway label on the bottom of your wireless gateway.



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 gateway label after installing your gateway. See [Change Your Wi-Fi Network Name \(SSID\)](#) (page 41) for more information.

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



Note: **WPA2-Personal** is the recommended wireless security level for your home network. It is the default security level for your wireless gateway and also the highest security level available.

8. 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 wireless gateway.

9. 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 gateway 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. See [Prevent Unauthorized Access](#) (page 44) for more information.

10. Select **Hide characters** checkbox to prevent your Security Key (network password) from displaying in the field.
11. Select **Start this connection automatically** so that your Wi-Fi devices will automatically connect to your Wi-Fi network when they are powered on.
12. Click **Next** to complete the Wi-Fi network setup.
The **Successfully added <Network name>** message for your new Wi-Fi network should appear.
13. Click **Close** to exit.

Connect Your WPS-Enabled Device

You can use the Wi-Fi Protected Setup (WPS) Pairing button on your wireless gateway to connect your WPS-enabled devices. WPS automatically assigns a random Wi-Fi network name (SSID) and Wi-Fi Security Key (network password) to your wireless gateway and your other WPS-enabled devices to connect them to your Wi-Fi network.



Note: To use the WPS Pairing button option, your computer hardware must support WPS and also have WPA security compatibility.

1. Power ON your wireless gateway and your other WPS-enabled devices that you want to connect to your Wi-Fi network.
2. Press and hold the **WPS** button located on your gateway front panel for five to 10 seconds and then release (see [Front Panel](#) (page 13) for the wireless gateway front view).
3. If applicable, press the **WPS** button on your WPS-enabled computer or other WPS-enabled device.
4. Repeat step 3 for each additional WPS-enabled device that you want to connect to your Wi-Fi network.

Test Your Wi-Fi Network Connection

Perform the following connectivity test to check that Wi-Fi connections were established for your wireless gateway and the other Wi-Fi devices on your home network:

1. Check if your Wi-Fi devices successfully connected to your Wi-Fi network, then disconnect the Ethernet cable, if connected, from your computer and wireless gateway.
2. Check that the **Wireless** LED on your wireless gateway front panel is lit SOLID green.
3. Open a web browser on your computer, such as Internet Explorer, Google Chrome, Firefox, or Safari.
4. Type a valid URL (such as www.surfboard.com) in the address bar and then press **Enter**.
If the website failed to open, please contact your service provider or call ARRIS Technical Support at **1-877-466-8646** for assistance.

Using the Gateway Web Manager

Use the gateway Web Manager to view and monitor the network configuration settings and operational status of your wireless gateway. You can also configure your network connections and Wi-Fi security settings. See [Protecting & Monitoring Your Wi-Fi Network](#) (page 43) for more information.



Note: *If you did not purchase your wireless gateway from a retail store, you may notice a few blocked configuration settings in the gateway Web Manager that cannot be modified. This may be due to some restrictions set up by your service provider to prevent unauthorized changes to certain configuration parameters.*

Start the Gateway Web Manager



Note: *You must use the default user name and password (see step 3) if you are logging on to the gateway Web Manager for the first time. For network security purposes, ARRIS recommends that you change the default user name and password after setting up your Wi-Fi network. See [Change the Default User Password](#) (page 43) for more information.*

1. Open a web browser (such as Internet Explorer, Google Chrome, Firefox, or Safari) on the computer connected to your wireless gateway.
2. Type the default LAN IP address, **192.168.0.1**, in the Address bar and then press **Enter** to log onto your wireless gateway.

The gateway Login screen displays.

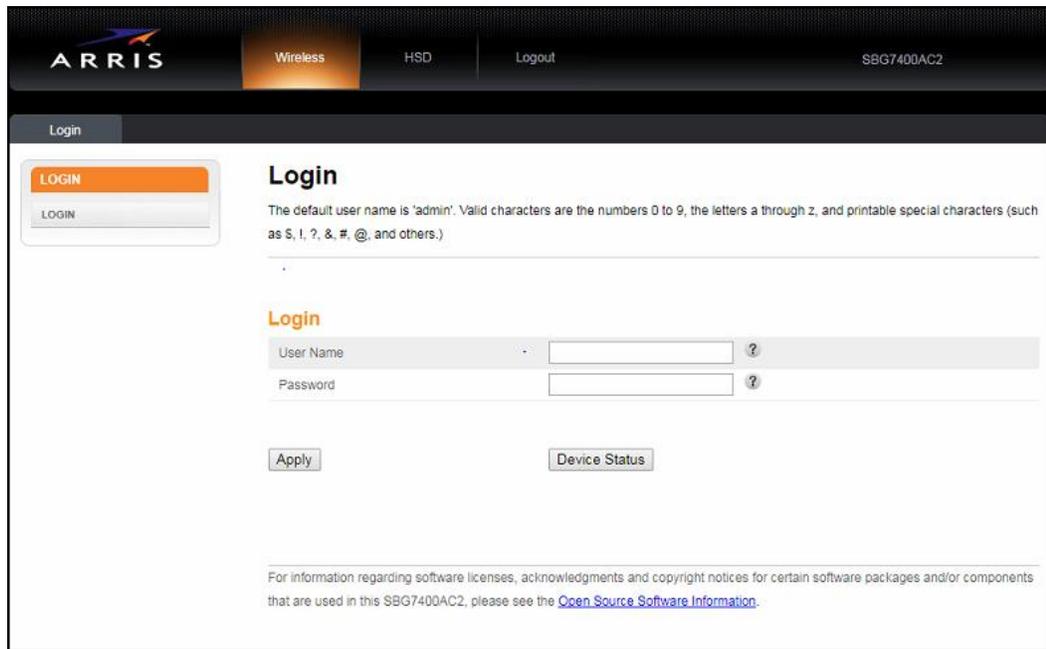


Figure 16: Wireless Gateway Login Screen

3. Type the following default user name and password. Both entries are case-sensitive.

- User Name: **admin**
- Password: **password**



Note: You must enter the default user name and password if you are logging in to the gateway Web Manager for the first time.

Figure 17: Gateway Login Screen

4. Click **Apply** to open the gateway Web Manager.
The Alerts!! Message box displays.



Figure 18: Gateway Opening Alerts Screen



Note: For Parental Control, download the **ARRIS Secure Home Internet by McAfee App** to set it up on your home network using your Apple or Android mobile device. This app is available as a free download from the App Store or Google Play.

For more information, please refer to the **ARRIS Secure Home Internet User Guide** available online at www.arris.com/selfhelp.



Note: ARRIS recommends that you change the default password for network security purposes. To change the password now, continue with step 5 below.

To change the password at a later time, see [Change the Default User Password](#) (page 43) for more information.

5. Click the **Click Here** link in the Alerts!! Message box.
A new Login Settings screen will display.

Login Settings

You can change the password for admin account. Use a password that will not be easy to guess. Passwords are case-sensitive. Valid characters are the numbers 0 to 9, the letters a through z and A through Z, and printable special characters (such as \$, !, ?, &, #, @, and others.)

Change Password

Old Password	<input type="password"/>	?
New Password	<input type="password"/>	?
Repeat New Password	<input type="password"/>	?

Other Settings

Login Timeout	<input type="text" value="900"/>	?
---------------	----------------------------------	---

Figure 19: Wireless Gateway Change Password Screen

6. Enter your current password in the Old Password field.
 7. Enter your new password in the New Password field.
-  **Note:** Remember that 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: **! @ # \$ % & ***
8. Enter your new password again in the Repeat New Password field.
 9. Click **Apply** to update your password.
 10. Find a secure place to write down and keep your new password for future reference, if needed.

Gateway Web Manager Menu Bar

The wireless gateway menu buttons are displayed along the top of the gateway Web Manager screen. To view a submenu screen (see Figure 21), click the related menu button on the menu bar.

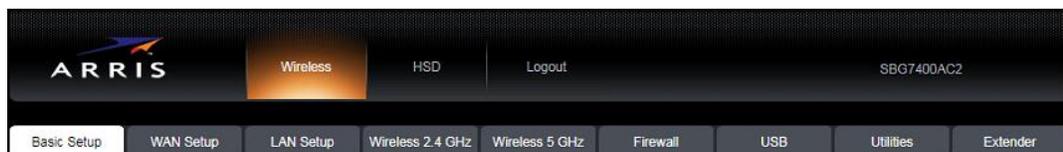


Figure 20: Gateway Web Manager Menu Bar

Table 4. Gateway Web Manager Menu Bar

Menu Option	Function
Wireless	
Basic Setup	Displays the default configuration settings for the gateway and allows you to change your user password.
WAN Setup	Displays the network configuration settings for the network connections outside your home.
LAN Setup	Displays the network configuration settings for your home network.
Wireless 2.4 GHz	Sets up your 2.4 GHz wireless network.
Wireless 5 GHz	Sets up your 5 GHz wireless network.
Firewall	Configures the gateway firewall to protect your home network from possible attacks from hackers or viruses.

Menu Option	Function
USB	Displays the current storage status of your USB device.
Utilities	Provides general information to help you set up your home network.
Extender	Configures your wireless SURFboard network extenders.
HSD	Displays the gateway product information including network connection status, hardware and software versions, and event log.
Logout	Closes the gateway Web Manager

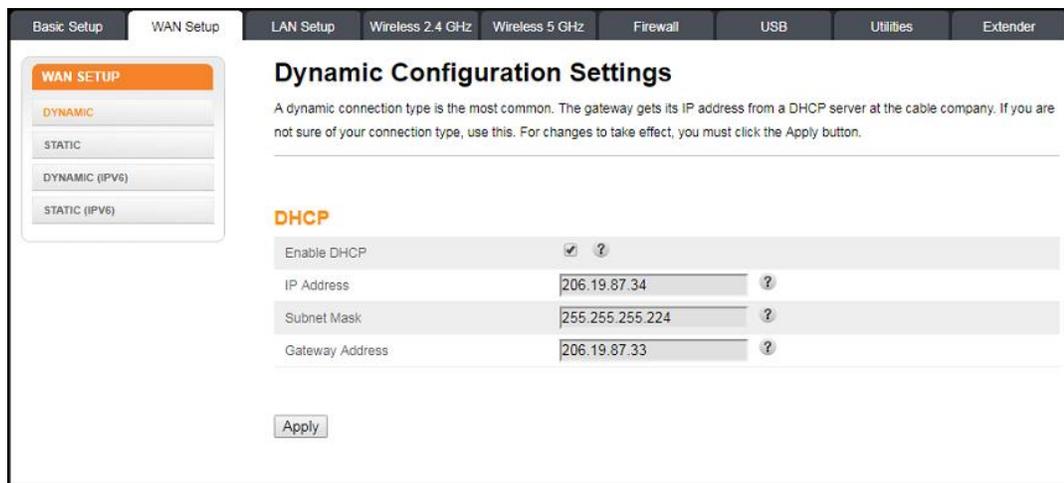


Figure 21: Sample Submenu Options

Gateway Web Manager-Available Languages

The gateway Web Manager is available in the following languages:

- English
- Spanish
- French
- Dutch
- Brazilian Portuguese

Do the following to change the language:

1. Open a web browser (such as Internet Explorer, Google Chrome, Firefox, or Safari) on the computer connected to your wireless gateway.
2. Type the default LAN IP address, **192.168.0.1**, in the Address bar and then press **Enter** to log onto your wireless gateway.

The Gateway Login screen displays.

3. Type the following default user name and password or your new password. Both entries are case-sensitive.
 - User Name: **admin**
 - Password: **password**
4. Click **Apply** to open the gateway Web Manager.
5. Click the **Utilities** menu button on the gateway Web Manager menu bar.
6. Click **Language** from the Utilities submenu options.

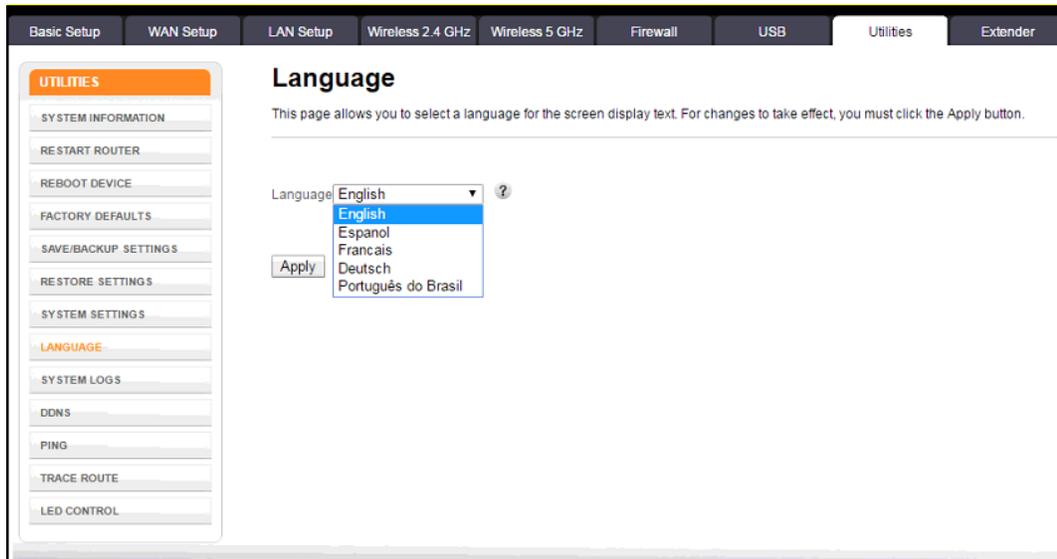


Figure 22: Gateway Language Screen

7. Select the language from the Language drop-down list.
8. Click **Apply**.

Get Help

Field-level help is available for all screen entries in the gateway Web Manager.

- Click on or move the cursor over the  icon located to the right of the applicable field.

Basic Setup

Language: English ?

Host Name: ARRISGW ?

Routing Enabled: ?

[More LAN Settings...](#)

Wireless 2.4 GHz

Enable Wireless: ?

Wireless Network Name (SSID): ARRIS-99E5 ?

Pre-Shared Key: 332333302257 ?

[More Wireless Settings...](#)

Enter a user friendly name to identify your wireless network. This name is also referred to as the Service Set Identifier (SSID). The name can be up to 32 characters long.

Wireless 5 GHz

Enable Wireless: ?

Wireless Network Name (SSID): ARRIS-99E5-5G ?

Pre-Shared Key: 332333302257 ?

[More Wireless Settings...](#)

2.4G/5G WPS Settings

WPS Enable: ?

Device PIN Enable: ?

Device PIN Code: 08913654 ?

WPS Mode: PBC ?

Enrollee PIN Code: ?

Start WPS Association: ?

Figure 23: Wireless Gateway Field Level Help

Exit the Gateway Web Manager

To log out and close the gateway Web Manager:

- Click **Logout** button located above the gateway Web Manager menu bar.

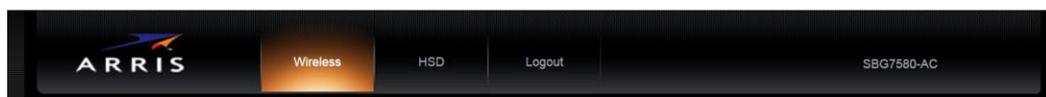


Figure 24: Gateway Web Manager Logout Button

Configuring Your Wi-Fi Network

Set Up Your Wi-Fi Network

1. Open a web browser and log onto your wireless gateway to open the gateway Web Manager.
See [Start the Gateway Web Manager](#) (page 31) for more information, if necessary.
2. Click the **Wireless 2.4 GHz** or **Wireless 5 GHz** main menu button on the gateway Web Manager menu bar.
Choose the Wi-Fi frequency range that you want to set up for your Wi-Fi network.
3. Click **BASIC** from the **Wireless** submenu option you are setting up.

System Basic Setup

While your system has many configuration options, the options on this Basic Setup page are those required by most users. Click the tabs to access the other configuration pages to set advanced options. Hover the mouse pointer over the question mark icon next to an option to view a description of that option. For changes to take effect, you must click the Apply button.

Basic Setup

Enable Wireless	<input checked="" type="checkbox"/> ?
Wireless Network Name (SSID)	<input type="text" value="ARRIS-99E5"/> ?
Broadcast Network Name (SSID)	<input checked="" type="checkbox"/> ?
Tx Power Level	<input type="text" value="High"/> ?
Channel	<input type="text" value="Auto"/> ?
AP Isolation	<input type="checkbox"/> ?
Enable WMM	<input checked="" type="checkbox"/> ?
WMM Power Save mode	<input checked="" type="checkbox"/> ?
Security Mode	<input type="text" value="WPA2-PSK (AES) (Recommended)"/> ?
Pre-Shared Key	<input type="text" value="332333302257"/> ?

Figure 25: Gateway 2.4 GHz Wireless Screen

System Basic Setup

While your system has many configuration options, the options on this Basic Setup page are those required by most users. Click the tabs to access the other configuration pages to set advanced options. Hover the mouse pointer over the question mark icon next to an option to view a description of that option. For changes to take effect, you must click the Apply button.

Basic Setup

Enable Wireless	<input checked="" type="checkbox"/> ?
Wireless Network Name (SSID)	<input type="text" value="ARRIS-99E5-5G"/> ?
Broadcast Network Name (SSID)	<input checked="" type="checkbox"/> ?
Tx Power Level	High ▾ ?
Channel	Auto ▾ ?
AP Isolation	<input type="checkbox"/> ?
Enable WMM	<input checked="" type="checkbox"/> ?
WMM Power Save mode	<input checked="" type="checkbox"/> ?
Enable 5G MU-MIMO	<input type="checkbox"/> ?
Security Mode	WPA2-PSK (AES) (Recommended) ▾ ?
Pre-Shared Key	<input type="text" value="332333302257"/> ?

Figure 26: Gateway 5 GHz Wireless Network Screen

4. Select the **Enable Wireless** checkbox to turn ON Wi-Fi networking on your home network.
- or -
Deselect the **Enable Wireless** checkbox to turn OFF Wi-Fi networking on your home network.
5. Do one of the following to set the network name or SSID (Service Set Identifier) for your Wi-Fi network in the Wi-Fi Network Name (SSID) field:
 - Keep the default network name listed in the network name field (also listed on the gateway label).
 - Enter a new network name for your Wi-Fi network.
The Wi-Fi network name cannot be the same name as any other SSID on your home network. You can use any combination of letters (lowercase and uppercase), numbers, and/or special characters (symbols) up to a maximum of 32 characters.
6. Select the **Broadcast Network Name (SSID)** checkbox to turn ON displaying your SSID as an available Wi-Fi network to outside users.
- or -
Deselect the **Broadcast Network Name (SSID)** checkbox to turn OFF displaying your SSID as an available Wi-Fi network to outside users.



Note: When **Broadcast Network Name (SSID)** is enabled, your SSID is visible and also available to unauthorized Wi-Fi clients that are within range to connect to your home network.

7. Select **High, Medium, or Low** for the Tx (Transmit) Power level of the Wi-Fi radio.
8. Select a channel number (**Auto, 1 thru 11**) from the **Channel** drop-down list to set the Communications channel for your wireless gateway.



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.

9. Select the **AP Isolation** checkbox to enable separate virtual networks for your Wi-Fi clients.

- or -

Deselect the **AP Isolation** checkbox to disable separate virtual networks for your Wi-Fi clients.



Note: When **AP Isolation** is enabled, each of your Wi-Fi clients will be in its own virtual network and will not be able to communicate with the other Wi-Fi clients. This may be useful if several guests are using your Wi-Fi network.

10. Select the **Enable WMM** checkbox to turn ON Wi-Fi Multi-media functionality.

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 in order to provide priority network access for applications that are less tolerant of packet delays.

11. Select the **WMM Power Save mode** checkbox to set the more efficient power management method.

-or-

Deselect the **WMM Power Save mode** checkbox to turn OFF the WMM Power Save mode.

12. Select one of the following Wi-Fi network security options for your wireless gateway from the **Security Mode** drop-down list:

- **Open** (not secure): Network security is not set for your Wi-Fi network. This network security option allows access to your Wi-Fi network without a Wi-Fi Security Key (network password)

- **WEP (64/128)** (poor security): Wired Equivalent Privacy
 - **WPA/WPA2-PSK (TKIP/AES)** (most compatible): Wi-Fi Protected Access version 2 with Pre-Shared Key (most compatible)
 - **WPA2-PSK (AES)** (recommended): Wi-Fi Protected Access version 2 with Pre-Shared Key
13. Enter a string of either ASCII characters or hexadecimal numbers (0 through 9, A thru F) in the Pre-Shared Key field to create your WPA Pre-Shared key.
- The Pre-Shared key is used to generate a unique password for WPS-enabled devices to connect to your Wi-Fi network.
14. Click **Apply**, when you are finished.

Change Your Wi-Fi Network Name (SSID)

The SSID (Service Set Identification) is the Wi-Fi network name assigned to your gateway Wi-Fi network. The default SSID (listed on the gateway label) is automatically populated in the network configuration screens. A list of available Wi-Fi networks (SSIDs) in close proximity of your home (for example, neighbors or local businesses) will display when you or someone else in your home attempt to establish a Wi-Fi network connection. For security purposes and quick recognition of your Wi-Fi network, ARRIS recommends that you change the default SSID.



Note: When you change the SSID, any Wi-Fi devices that are already connected to your Wi-Fi network will be disconnected from the network. The Wi-Fi devices will have to be reconnected to the Wi-Fi network using the new SSID.

Do the following to change your Wi-Fi network name (SSID):

1. Open a web browser and log onto your wireless gateway to open the gateway Web Manager.
See [Start the Gateway Web Manager](#) (page 31) for more information, if necessary.
2. Click the **Wireless 2.4 GHz** or **Wireless 5 GHz** main menu button on the gateway Web Manager menu bar.
Choose the Wi-Fi frequency range that you want to set up for your Wi-Fi network.
3. Click **BASIC** from the **Wireless** submenu option you are setting up.

Basic Setup

Enable Wireless	<input checked="" type="checkbox"/> ?
Wireless Network Name (SSID)	ARRIS-99E5 ?
Broadcast Network Name (SSID)	<input checked="" type="checkbox"/> ?
Tx Power Level	High ?
Channel	Auto ?
AP Isolation	<input type="checkbox"/> ?
Enable WMM	<input checked="" type="checkbox"/> ?
WMM Power Save mode	<input checked="" type="checkbox"/> ?
Security Mode	WPA2-PSK (AES) (Recommended) ?
Pre-Shared Key	332333302257 ?

Apply

Figure 27: Gateway 2.4 GHz Wireless Screen-Change SSID

Basic Setup

Enable Wireless	<input checked="" type="checkbox"/> ?
Wireless Network Name (SSID)	ARRIS-99E5-5G ?
Broadcast Network Name (SSID)	<input checked="" type="checkbox"/> ?
Tx Power Level	High ?
Channel	Auto ?
AP Isolation	<input type="checkbox"/> ?
Enable WMM	<input checked="" type="checkbox"/> ?
WMM Power Save mode	<input checked="" type="checkbox"/> ?
Enable 5G MU-MIMO	<input type="checkbox"/> ?
Security Mode	WPA2-PSK (AES) (Recommended) ?
Pre-Shared Key	332333302257 ?

Apply

Figure 28: Change Your 5 GHz Network Name (SSID) and Password Screen

4. Check that the **Enable Wireless** checkbox is selected.
This turns ON Wi-Fi networking on your home network.
5. Delete the current network name in the Network Name (SSID) field and then enter a new name of your choice for your Wi-Fi network.
The network name can contain any combination of up to 32 alphanumeric characters.
6. Check that the Broadcast Network Name (SSID) checkbox is selected.

7. Click **Apply** at the bottom of the screen, when you are finished.

The new Wi-Fi network name should appear in the list of available Wi-Fi networks when you reconnect your Wi-Fi devices.

Protecting & Monitoring Your Wi-Fi Network

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

Prevent Unauthorized Access



Caution: To prevent unauthorized access and configuration to your Wi-Fi home network, ARRIS recommends that you immediately change the default password after connecting to the Internet and logging on to your wireless gateway for the first time.

One of the most important recommendations for securing your Wi-Fi home network is to change the default user password on your wireless gateway and other Wi-Fi devices as well. Default passwords are commonly used and shared on the Internet.

To ensure that your Wi-Fi home network is secure, ARRIS recommends that you follow these best practices for user passwords:

- 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.
- Continue to change your administrator password on a regular basis.



Note: *If your service provider supplied your wireless gateway, you may not have the necessary user privileges to change the log in user name.*

Change the Default User Password

To change the default user password:

1. From any web manager screen, click the **Basic Setup** main menu button on the gateway Web Manager menu bar.
2. Click **LOGIN SETTINGS** from the Basic Setup submenu options list.
The Login Settings screen displays.

Login Settings

You can change the password for admin account. Use a password that will not be easy to guess. Passwords are case-sensitive. Valid characters are the numbers 0 to 9, the letters a through z and A through Z, and printable special characters (such as \$, !, ?, &, #, @, and others.)

Change Password

Old Password ?

New Password ?

Repeat New Password ?

Other Settings

Login Timeout ?

Figure 29: Wireless Gateway Login Settings Screen

3. Enter your current password in the Old Password field.
4. Enter your new password in the New Password field.



Note: Remember that 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: **! @ # \$ % & ***

5. Enter your new password again in the Repeat New Password field.
6. Click **Apply** to update your password.

The **Applying Changes...** message displays.



Note: The **Login Timeout** setting under the **Other Settings** section applies to the amount of inactivity time (in seconds) allowed before the gateway Web Manager automatically logs out. The Login Timeout range is between **30** and **900** seconds.

7. Find a secure place to write down and keep your new password for future reference, if needed.

The System Basic Setup screen displays.

Basic Setup

Language ?

Host Name ?

Routing Enabled ?

[More LAN Settings...](#)

Wireless 2.4 GHz

Enable Wireless ?

Wireless Network Name (SSID) ?

Pre-Shared Key ?

[More Wireless Settings...](#)

Wireless 5 GHz

Enable Wireless ?

Wireless Network Name (SSID) ?

Pre-Shared Key ?

[More Wireless Settings...](#)

2.4G/5G WPS Settings

WPS Enable ?

Device PIN Enable ?

Device PIN Code ?

WPS Mode ?

Enrollee PIN Code ?

Start WPS Association  ?

Figure 30: Wireless Gateway Firewall Settings Screen

Set Up Firewall Protection

You can set up firewall filters to protect your computer and other network devices on your home network from hackers, viruses, and other attacks from the Internet.

To set the firewall protection level:

1. From any gateway Web Manager screen, click the **Firewall** main menu button on the gateway Web Manager menu bar.

2. Click **FIREWALL SETTINGS** from the Firewall submenu options list to display the Firewall Settings screen (see Figure 31).
3. Select the **Enable Firewall** checkbox to turn ON firewall protection on your home network.
- or -

Deselect the **Enable Firewall** checkbox to turn OFF firewall protection on your home network.



Note: Turning OFF firewall protection on your home network could put your computer(s) and other Ethernet-enabled devices connected on your network at risk for possible attacks from viruses and hackers.

Firewall Enable/Disable
Enable Firewall ?

DoS Attack Protection
Enable DoS Attack Protection Firewall ?

Block Pings
Enable Ping Blocking ?

IPSec Pass Through
Enable IPSec Pass Through ?

PPTP Pass Through
Enable PPTP Pass Through ?

L2TP Pass Through
Enable L2TP Pass Through ?

Block Fragmented IP Packets
Enable Block Fragmented IP Packets ?

Apply

Figure 31: Firewall Protection Level Screen

4. Select or deselect any of the following to set up firewall protection on your home network:
 - Firewall Enable/Disable
 - DoS Attack Protection
 - Block Pings
 - IPSec Pass Through
 - PPTP Pass Through
 - L2TP Pass Through
 - Block Fragmented IP Packets
5. Click **Apply**, when you are finished.

Set Up Parental Controls



Note: Parental Controls in the gateway Web Manager is disabled. The **ARRIS Secure Home Internet by McAfee App** is now available for you to set up Parental Controls on your home network using your Apple or Android mobile device. It is available online as a free download from the App store and Google Play. For more information, refer to the **ARRIS Secure Home Internet User Guide**; available online at www.arris.com/selfhelp.

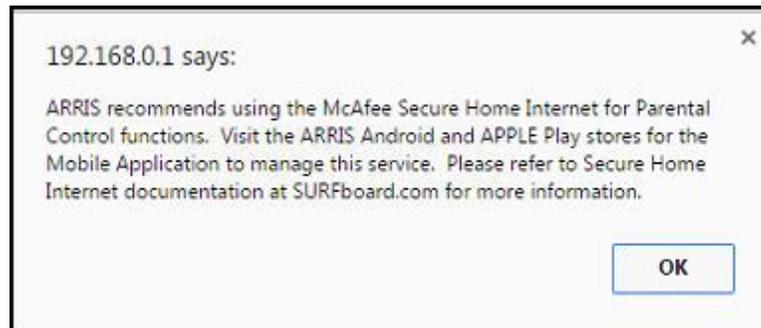


Figure 32: Parental Controls Access Message

Set Up IP Filtering

You can use IP Filtering to set up Internet access restrictions on specific network devices on your home network using their IP addresses. You will have to create IP address filters that contain the starting and ending IP address range of each device for which you want to block Internet access.

To configure IP filters:

1. From any web manager screen, click the **Firewall** menu button on the gateway Web Manager main menu bar.
2. Click **CLIENT IP FILTERS** from the Firewall submenu options list to display the Client IP Filters Configuration screen.

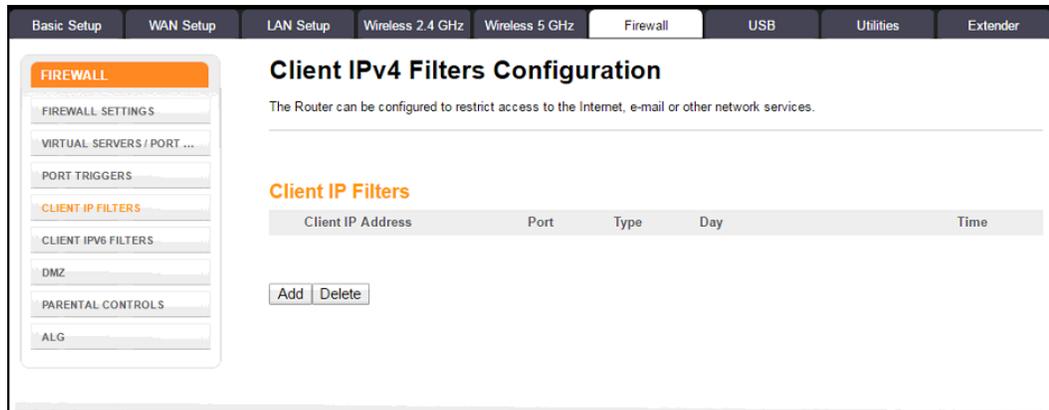


Figure 33: Set Up Client IP Filters Screen

3. Click **Add** button to open the Add Client IP Filter dialog.

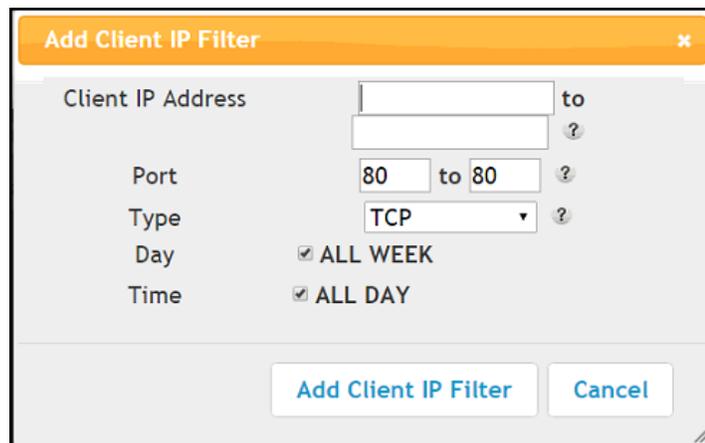


Figure 34: Add Client IP Filter Screen

4. Enter the starting and ending Client IP addresses for the range you are setting up in the Client IP Address field.
5. Enter the range of port numbers for the Port Filter range in the Port fields.
6. Select **UDP**, **TCP**, or **UDP and TCP** for the Port Filter type in the Type drop-down list.
7. Select **ALL WEEK** in the Day field to set the same access restrictions for every day of the week.
- or -
Deselect **ALL WEEK** to set access restrictions for specific days of the week .
8. Select **ALL DAY** in the Time field to set 24-hour access restrictions for the selected days of the week.
- or -
Deselect **ALL DAY** to set up a specific range of time for the selected days of the week.
9. Click **Add Client IP Filter** to create the IP filter.
10. Repeat steps 3 thru 9 for each additional range of IP addresses that you want to block Internet access.

Set Up MAC Address Filtering

MAC filtering allows you to define up to twenty Media Access Control (MAC) address filters to prevent computers from sending outgoing TCP/UDP traffic to the WAN via their MAC addresses. This is useful because the MAC address of a specific NIC card never changes, unlike its IP address, which can be assigned via the DHCP server or hard-coded to various addresses over time.

To configure MAC Address filters:

1. From any gateway Web Manager screen, click the **Wireless 2.4 GHz** or **Wireless 5 GHz** main menu button on the gateway Web Manager menu bar.
2. Click **MAC ADDRESS CONTROL** from the **Wireless** submenu options list to display the MAC Address Control screen.

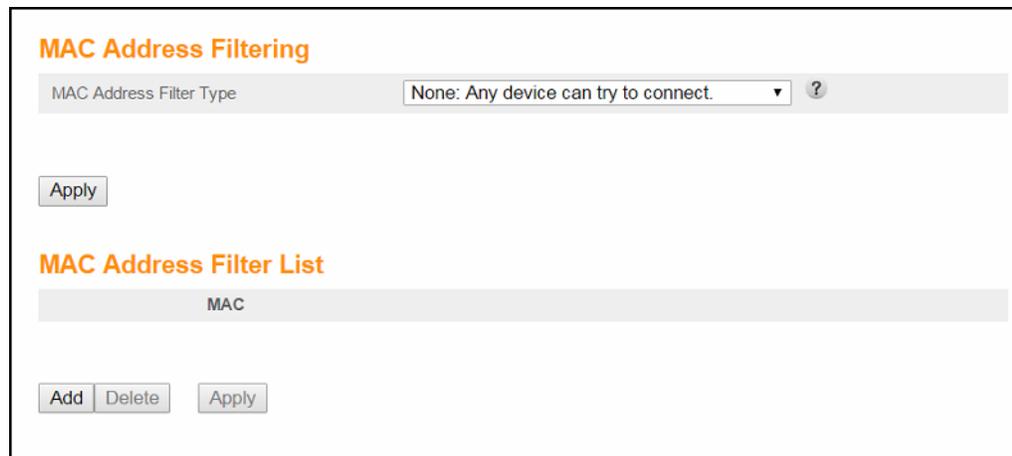


Figure 35: Set Up MAC Filters Screen

3. Select the MAC Address Filter Type from the drop-down list:
 - None:** Allows all Wi-Fi devices to connect.
 - Whitelist:** Allows only listed Wi-Fi devices to connect.
 - Blacklist:** Allows only Wi-Fi devices that are not listed to connect.
4. Click **Add** to enter the MAC Address of the client device that you want to block access to your home network.

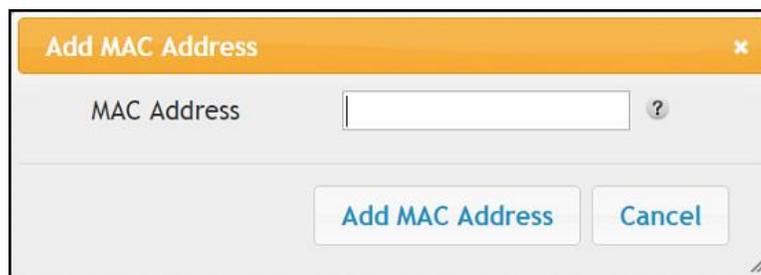


Figure 36: Set Up MAC Filters Screen

5. Enter the least significant byte of the starting IP address in the MAC Address field.
6. Click **Add MAC Address**.
7. Repeat steps 3 thru 6 for each MAC address that you want to add.
8. Click **Apply**, when done.

Set Up Port Triggers

You can use Port Triggers to configure dynamic triggers to specific devices on your LAN. This allows special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messaging program features may require these special settings.



Note: If you enable the firewall and set up custom port triggers, then you must configure the firewall to allow traffic through those custom ports. See [Set Up Firewall Protection \(page 45\)](#) for more information.

To configure Port Triggers:

1. From any gateway Web Manager screen, click the **Firewall** main menu button on the gateway Web Manager menu bar.
2. Click **PORT TRIGGERS** from the **Firewall** submenu options list to display the Port Triggers Configuration screen.

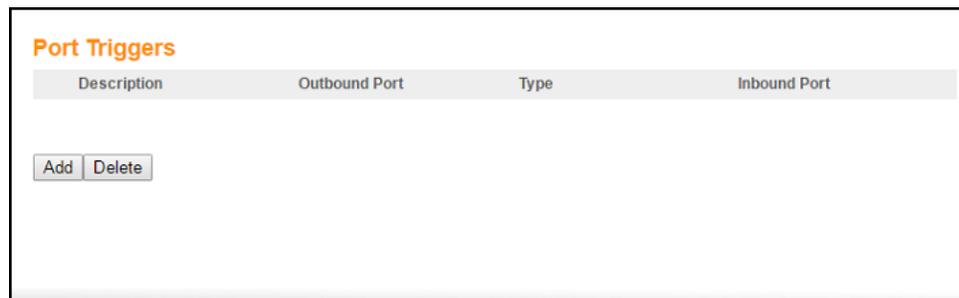


Figure 37: Advanced Port Triggers Screen

3. Click **Add** button to open the Add Port Trigger screen.

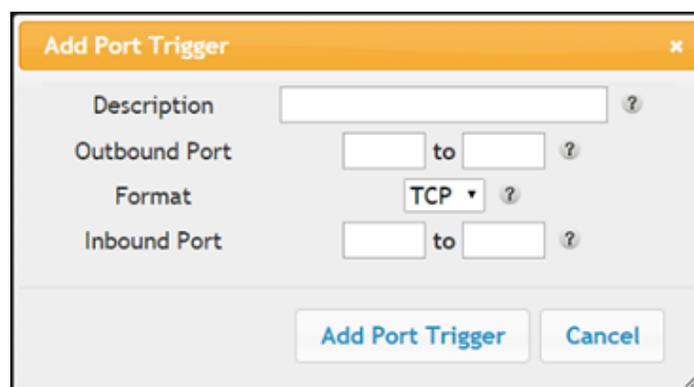


Figure 38: Add Port Triggers Screen

4. Enter a name or description for the Port Trigger in the Description field.
5. Enter the starting and ending port numbers of the Port Trigger range in the Outbound Port fields.
6. Select **TCP**, **UDP**, or **BOTH** for the Port Trigger from the Format drop-down list.
7. Enter the starting and ending port numbers of the Port Trigger range in the Inbound Port fields.
8. Click **Add Port Trigger** to create your port triggers.
9. Repeat steps 3 thru 8 to create additional port triggers.

Set Up the DMZ Host



WARNING! The gaming DMZ host is not protected by the gateway firewall. It is exposed to the Internet and thus vulnerable to attacks or hacking from any computer on the Internet. Consider carefully before configuring a device to be in the DMZ.

You can configure one computer on your home network to be the DMZ Host. That computer will operate outside of the gateway firewall and allow remote access from the Internet to your computer, 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 any gateway Web Manager screen, click the **Firewall** main menu button on the gateway Web Manager menu bar.
2. Click **DMZ** from the **Firewall** submenu options list to display the DMZ Settings screen.

IP Address Of Virtual DMZ Host	
Enable DMZ	<input type="checkbox"/> ?
WAN IP	206.19.87.36 ?
Private IP	0.0.0.0 ?
<input type="button" value="Apply"/>	

Figure 39: Advanced DMZ Host Screen

3. Select the **Enable DMZ** checkbox to set up the DMZ Host on your home network.
4. Enter the IP address of the computer or gaming device that you are setting up as the DMZ host.
5. Click **Apply**, when you are finished.



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.



Note: To disable the DMZ Host, deselect (uncheck) the **Enable DMZ** checkbox and then click **Apply**.

Managing Your Gateway and Connected Networks

Use the gateway Web Manager to view and monitor the network configuration settings and operational status of your gateway. You can also configure your network connections and wireless security settings. See [Protecting & Monitoring Your Wi-Fi Network](#) (page 43) for more information.

View the Gateway Status and Network Connection

You can use the Device Status button on the gateway Login screen to view the current gateway configuration and network connection status of your wireless gateway without having to login to the gateway Web Manager.

1. Open any web browser on the computer connected to your wireless gateway.
2. Type the default LAN IP address, **192.168.0.1**, in the address bar and then press **Enter**.

The gateway Login screen displays.

Figure 40: Gateway Login Screen

3. Click **Device Status** button to open the gateway Device Status screen.

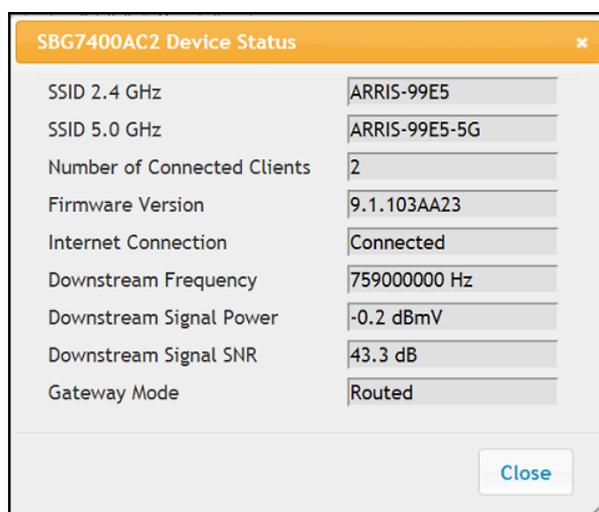


Figure 41: Gateway Device Status Screen

View the Gateway Product and Status Information

The System Information screen displays general product information, including the software (or firmware) version and the current network connection status of the gateway.

To open the System Information page:

1. From any gateway Web Manager screen, click the **Utilities** main menu button on the gateway Web Manager menu bar.
2. Click **SYSTEM INFORMATION** from the **Utilities** submenu options list to display the System Information screen.
3. Click the **Refresh** button (**F5**) in your web browser to reload the information on the screen.

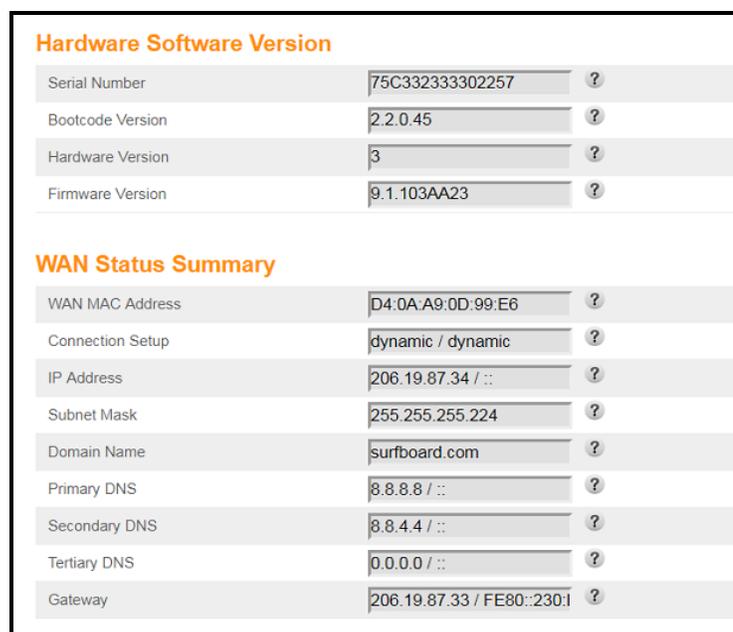


Figure 42: Gateway Status – System Information Screen (1 of 2)

Wireless 2.4GHz Status Summary		
Wireless SSID	ARRIS-99E5	?
Wireless Channel	Auto	?
Wireless Mode	Mixed GN	?
SSID Broadcast	Enabled	?
WMM	Enabled	?
MAC Address	90:9D:7D:6B:1A:AE	?
Number of Wi-Fi Clients	1	?
Radio Status	Enabled	?
WPS Status	Enabled	?
Wireless 5GHz Status Summary		
Wireless SSID	ARRIS-99E5-5G	?
Channel	Auto	?
Wireless Mode	Mixed ANAC	?
SSID Broadcast	Enabled	?
WMM	Enabled	?
MAC Address	90:9D:7D:6B:1A:AF	?
Number of Wi-Fi Clients	0	?
Radio Status	Enabled	?
WPS Status	Enabled	?
LAN Status Summary		
IP Address	192.168.0.1 / ::	?
DHCP Server	Enabled	?
Subnet Mask	255.255.255.0	?
UPnP	Enabled	?
Number of LAN Clients	1	?

Figure 43: Gateway Status – System Information Screen (2 of 2)

Back Up Your Gateway Configuration

You can save a backup copy of the current gateway configuration settings to your local computer. You can use the backup file to restore your custom gateway settings in the event that you made changes that you no longer want.



Caution: ARRIS recommends that you perform the gateway configuration backup using the gateway default login user name and password.

To create a backup copy of your gateway configuration settings:

1. From any gateway Web Manager screen, click the **Utilities** main menu button on the gateway Web Manager menu bar.
2. Click **SAVE/BACKUP SETTINGS** from the **Utilities** submenu options list to display the Save/Backup screen.

3. Click **Save**.
4. Click **OK** at the **This may take a few minutes. Continue?** prompt to save your gateway configuration settings.

Restore the Gateway Configuration Settings



WARNING! This action will delete your current gateway configuration settings and allow you to restore a previously saved gateway configuration.



Note: After the configuration settings are restored, your wireless gateway will automatically reboot and you will have to log on using the default user name (**admin**) and password (**password**).

To open the System Information page:

1. From any gateway Web Manager screen, click the **Utilities** main menu button on the gateway Web Manager menu bar.
2. Click **RESTORE SETTINGS** from the **Utilities** submenu options list to display the System Information screen.
3. Click **Backup and Restore** from the Basic submenu options

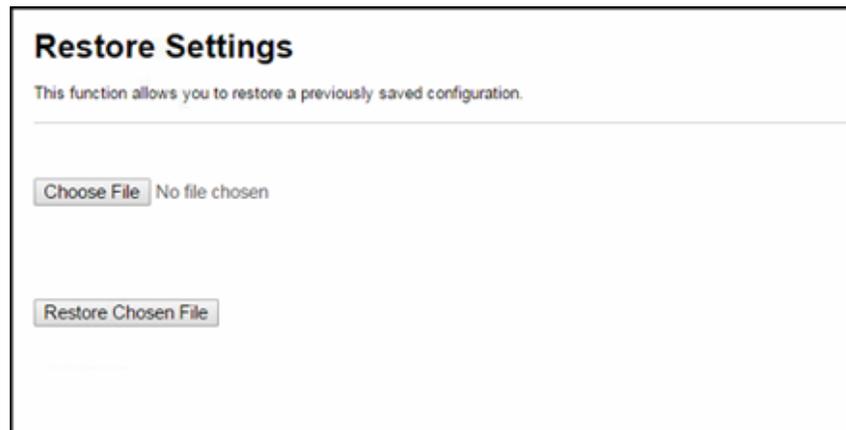


Figure 44: Gateway Restore Settings Screen

4. Click **Choose File** to search for a saved configuration file (**GatewaySettings.bin**) in the Downloads folder on your computer.
 5. Select the gateway configuration file from the list that you want to restore.
 6. Click **Open**.
- The selected configuration file will appear in the Choose File field.

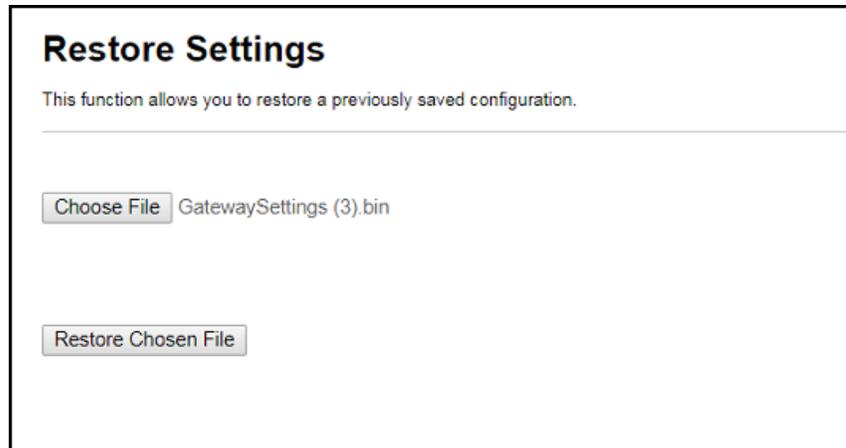


Figure 45: Sample Selected Gateway Config File Screen

7. Click **Restore Chosen File**.
The gateway will automatically reboot.

Reset the Gateway Configuration Settings



WARNING! This process also deletes any custom gateway configurations you may have already created. ARRIS recommends that you create a backup copy of your configuration before resetting your gateway. See [Back Up Your Gateway Configuration](#) (page 55) for more information.

From the gateway Web Manager, do the following to open the Status Security screen:

1. From any gateway Web Manager screen, click the **Utilities** main menu button on the gateway Web Manager menu bar.
2. Click **FACTORY DEFAULTS** from the **Utilities** submenu options list to display the Factory Defaults screen.

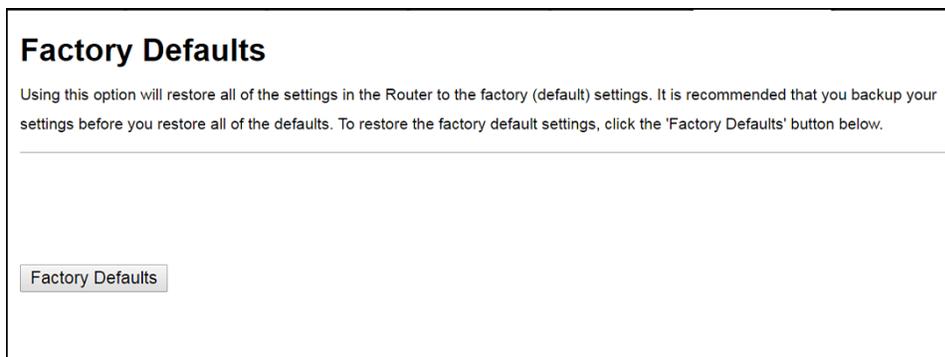


Figure 46: Reset Gateway Configuration to Factory Defaults Screen

3. Click **Factory Defaults** button.

The following message displays:

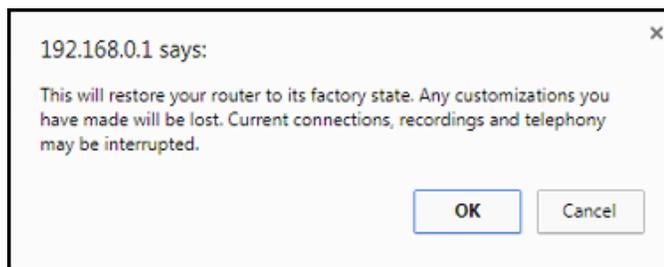


Figure 47: Reset Gateway Configuration Warning Message

4. Click **OK** to reset your current gateway configuration to the factory default configuration.
or
Click **Cancel** to close the message box.

Exit the Gateway Web Manager

To log out and close the gateway Web Manager:

- Click **Logout** button located on the gateway Web Manager menu bar.

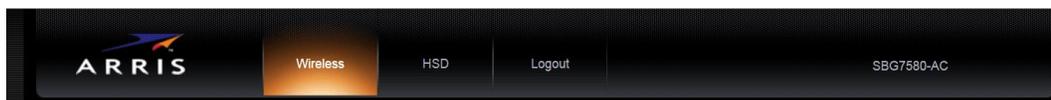


Figure 48: Gateway Web Manager Logout Button

Troubleshooting Tips

If the solutions listed in the Troubleshooting Solutions table below do not solve your problem, please contact your service provider for assistance. Your service provider may ask for the status of the gateway front panel LEDs, see [Front Panel LED Icons and Error Conditions](#) (page 60) for more information.

You may have to reset the gateway configuration to its original factory settings if the gateway is not functioning properly. See [Reset the Gateway Configuration Settings](#) (page 57) for more information.

Solutions

Table 5. Troubleshooting Solutions

Gateway Problem	Possible Solution
Power LED Icon is OFF	<ul style="list-style-type: none"> ■ Check the power connection on the gateway and to the electrical outlet. ■ Check that the electrical outlet is working. Is the outlet controlled by a light switch? If so, unplug the gateway power adapter and connect it to another electrical outlet that is not controlled by a wall switch.
Cannot Send or Receive Data	<ul style="list-style-type: none"> ■ Check each end of the coaxial cable connection on the gateway and cable wall outlet. Use your hand to tighten each connector, if necessary. ■ Check the Ethernet cable to make sure it is properly connected to the gateway and computer. ■ On the front panel, check the status of the LED icons and refer to Front Panel LED Icons and Error Conditions (page 60) to identify the problem. ■ If you have cable television service, check your television to ensure your cable service is operating properly. ■ If none of the above solutions resolves the problem, contact your service provider or call ARRIS Technical Support at 1-877-466-8646 for assistance.

Gateway Problem	Possible Solution
Cannot Access the Internet	<ul style="list-style-type: none"> ■ Check that all cable and power connections on your gateway and computer are properly connected. ■ Check that the Power, Online, and Wireless LED icons on the front panel are lit up solid. ■ Contact your service provider for assistance.
Wi-Fi Devices Cannot Send or Receive Data	<ul style="list-style-type: none"> ■ If the problem still continues after checking the coaxial cable and Ethernet connections and your IP address, check the wireless Security Mode setting on the Wireless screen. ■ If you enabled WPA and configured a passphrase on the gateway, 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 WPA. ■ If you enabled WEP and configured a key on the gateway, be sure each affected Wi-Fi client has the identical WEP key. If this does not solve the problem, check if the client's wireless adapter supports the type of WEP key configured on the gateway.

Front Panel LED Icons and Error Conditions

The gateway front panel LED icons provide status information for the following error conditions:

Table 6. Front Panel LED Icons and Error Conditions

Led Icon	Status	If, During Startup:	If, During Normal Operation
 POWER	OFF	Wireless gateway is not properly plugged into the electrical wall outlet	Wireless gateway is unplugged
 SEND RECEIVE	BLINKING	Upstream (send) channel or Downstream (receive) channel cannot be acquired	Upstream channel is lost Downstream channel is lost
 ONLINE	BLINKING	IP registration is unsuccessful	IP registration is lost
 WIRELESS	OFF	LED is disabled	LED is disabled
 WIRELESS	OFF	LED is disabled	LED is disabled

Warranty Information

SURFboard Wireless Gateways - SBG6450AC2 and SBG7400AC2

ARRIS Enterprises, LLC ("ARRIS")

Retail Purchasers: If you purchased this Product directly from ARRIS or from an authorized ARRIS retail reseller, ARRIS warrants to you, the original end user customer, that (A) the Product, excluding Software, will be free from defects in materials and workmanship under normal use, and (B) with respect to Software, (i) the media on which the Software is provided will be free from defects in material and workmanship under normal use, and (ii) the Software will perform substantially as described in its documentation. This Limited Warranty to you, the original end user customer, continues (A) for Software and the media upon which it is provided, for a period of ninety (90) days from the date of purchase from ARRIS or an authorized ARRIS reseller, and (B) for the Product (excluding Software), for a period of two (2) years from the date of purchase from ARRIS or from an authorized ARRIS reseller. To take advantage of this Limited Warranty or to obtain technical support, you must call the ARRIS toll-free telephone number **1-877-466-8646**. Technical support charges may apply. ARRIS' sole and exclusive obligation under this Limited Warranty for retail sales shall be to repair or replace any Product or Software that does not meet this Limited Warranty. All warranty claims must be made within the applicable Warranty Period.

Cable Operator or Service Provider Arrangements. If you did not purchase this Product directly from ARRIS or from a ARRIS authorized retail reseller, ARRIS does not warrant this Product to you, the end-user. A limited warranty for this Product (including Software) may have been provided to your cable operator or Internet Service Provider ("Service Provider") from whom you obtained the Product. Please contact your Service Provider if you experience problems with this Product.

General Information. The warranties described in this Section shall not apply: (i) to any Product subjected to accident, misuse, neglect, alteration, Acts of God, improper handling, improper transport, improper storage, improper use or application, improper installation, improper testing or unauthorized repair; or (ii) to cosmetic problems or defects which result from normal wear and tear under ordinary use, and do not affect the performance or use of the Product. ARRIS' warranties apply only to a Product that is manufactured by ARRIS and identified by ARRIS owned trademark, trade name or product identification logos affixed to the Product. ARRIS does not warrant to you, the end user, or to anyone else that the Software will perform error free or without bugs.

ARRIS IS NOT RESPONSIBLE FOR, AND PROVIDES "AS IS" ANY SOFTWARE SUPPLIED BY 3RD PARTIES. EXCEPT AS EXPRESSLY STATED IN THIS SECTION ("WARRANTY INFORMATION"), THERE ARE NO WARRANTIES OF ANY KIND RELATING TO THE PRODUCT, EXPRESS, IMPLIED OR STATUTORY, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR THE WARRANTY AGAINST INFRINGEMENT PROVIDED IN THE UNIFORM COMMERCIAL CODE. Some states do not allow for the exclusion of implied warranties, so the above exclusion may not apply to you.

What additional provisions should I be aware of? Because it is impossible for ARRIS to know the purposes for which you acquired this Product or the uses to which you will put this Product, you assume full responsibility for the selection of the Product for its installation and use. While every reasonable effort has been made to insure that you will receive a Product that you can use and enjoy, ARRIS does not warrant that the functions of the Product will meet your requirements or that the operation of the Product will be uninterrupted or error-free.

ARRIS IS NOT RESPONSIBLE FOR PROBLEMS OR DAMAGE CAUSED BY THE INTERACTION OF THE PRODUCT WITH ANY OTHER SOFTWARE OR HARDWARE. ALL WARRANTIES ARE VOID IF THE PRODUCT IS OPENED, ALTERED, AND/OR DAMAGED.

THESE ARE YOUR SOLE AND EXCLUSIVE REMEDIES for any and all claims that you may have arising out of or in connection with this Product, whether made or suffered by you or another person and whether based in contract or tort.

IN NO EVENT SHALL ARRIS BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION OR ANY OTHER PECUNIARY LOSS), OR FROM ANY BREACH OF WARRANTY, EVEN IF ARRIS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO CASE SHALL ARRIS' LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

These matters are governed by the laws of the State of Georgia of the United States of America, without regard to conflict of laws principles and excluding the provisions of the United Nations Convention on Contracts for the International Sale of Goods and the Uniform Computers Information Transactions Act.

Retail Purchasers Only. If you purchased this Product directly from ARRIS or from an ARRIS authorized retail reseller, please call the ARRIS toll-free phone number, **1-877-466-8646** for warranty service or technical support. Technical support charges may apply. For online technical support, please visit www.arris.com/selfhelp.

Cable Operator or Service Provider Arrangements. If you did not purchase this Product directly from ARRIS or from an ARRIS authorized retail reseller, please contact your Service Provider for technical support.

Corporate Headquarters

ARRIS · Suwanee · Georgia · 30024 · USA

T: 1-678-473-2000 F: 1-678-473-8470

www.arris.com