



## **Touchstone Release 12.0**

**WebGUI Reference (DOCSIS 3.1), STANDARD Revision 1.0**

August 2022

# Table of contents

<b>Chapter 1: Getting started.....</b>	<b>4</b>
Connect to the Gateway.....	4
Connect to the Gateway using Ethernet.....	4
Connect to the Gateway using Wi-Fi.....	5
Log in to the configuration interface.....	6
Password requirements.....	8
How Do I.....	9
change my Wi-Fi network name?.....	10
change my Wi-Fi network password?.....	11
change my Gateway password?.....	11
hide my Wi-Fi network from other users?.....	12
see what devices are using my Gateway?.....	13
connect older devices to my Gateway?.....	13
keep the kids from accessing certain websites?.....	14
block certain devices from accessing my Gateway?.....	15
extend the range of my Wi-Fi network?.....	17
bypass the firewall?.....	17
make changes from somewhere else?.....	18
see if the Gateway is connected to the Internet?.....	18
connect if I've forgotten my Wi-Fi password?.....	19
reset the Gateway?.....	19
fix interference problems?.....	20
fix a slow connection?.....	21
change the language for the Gateway configuration page?.....	21
troubleshoot my connection?.....	22
<b>Chapter 2: Gateway Setup.....</b>	<b>24</b>
Gateway > Summary.....	24
Gateway > Email Notification.....	25
Gateway > Connection.....	26
Gateway > Connection > Status.....	26
Gateway > Connection > WAN Network.....	28
Gateway > Connection > Local IP Network.....	30
Gateway > Connection > Wi-Fi.....	34
Gateway > Connection > MoCA.....	46
Gateway > Connection > MTA.....	47
Gateway > Connection > CallP/QoS.....	51
Gateway > Connection > Voice Quality Metrics.....	52
Gateway > Firewall.....	52
Gateway > Firewall > IPv4.....	53
Gateway > Firewall > IPv6.....	54

Gateway > Software.....	55
Gateway > Hardware.....	56
Gateway > Hardware > System Hardware.....	56
Gateway > Hardware > Ethernet.....	57
Gateway > Hardware > Wireless.....	58
Gateway > Time.....	59
<b>Chapter 3: Connected Devices.....</b>	<b>60</b>
Connected Devices > Devices.....	60
Connected Devices > Static Addresses.....	62
<b>Chapter 4: Parental Control.....</b>	<b>64</b>
Parental Control > Managed Sites.....	64
Parental Control > Managed Services.....	67
Parental Control > Managed Devices.....	69
Parental Control > Reports.....	71
<b>Chapter 5: Advanced.....</b>	<b>72</b>
Advanced > Port Forwarding.....	72
Advanced > Port Triggering.....	73
Advanced > Remote Management.....	76
Advanced > DMZ.....	77
Advanced > ALG.....	78
Advanced > Routing.....	79
Advanced > Dynamic DNS.....	81
Advanced > Device Discovery.....	83
Advanced > MAC Bridging.....	84
<b>Chapter 6: Wi-Fi MESH.....</b>	<b>85</b>
Wi-Fi Mesh Settings.....	85
AHNC.....	86
Wi-Fi MESH > AHNC > Network Topology.....	86
<b>Chapter 7: Troubleshooting.....</b>	<b>87</b>
Troubleshooting > Logs.....	87
Troubleshooting > Diagnostic Tools.....	88
Troubleshooting > Wi-Fi Spectrum Analyzer.....	89
Troubleshooting > DOCSIS Spectrum Analyzer.....	90
Troubleshooting > Restart/Restore.....	91

# Getting started

---

Before you can work with the Gateway, you have to connect and log in.

## Connect to the Gateway

Your first step is connecting to the Gateway. You can use Ethernet or Wi-Fi to connect.

### Connect to the Gateway using Ethernet

Ethernet is the preferred method to connect to the Gateway for setup.

► **Follow these steps:**

1. Locate the Ethernet jack on your computer. On desktop computers, the jack is usually on the back of the computer. On laptops, the jack may be in back or on side. The jack looks like a wide telephone jack.
2. Plug one end of the Ethernet cable into your computer. Plug the other end into any Ethernet jack on the back of the Gateway. Listen for a click as the cable latch snaps into place. Gently tug on the cable to confirm it is connected.
3. Wait several seconds for the computer to connect to the Internet. Depending on your operating system, you may see a notification.
4. Use a web browser to access an external website, such as [ARRIS documentation](#).  
If successful, proceed to [Log in to the configuration interface](#) (page 6).

If you have a problem, check the following:

- Make sure the Gateway is powered on and connected to the cable provider's network. The Online light on the front panel should be on.
- Check the Ethernet cable connection to your computer and the Gateway. The connectors should be latched in place and not pull out without squeezing the latch.
- Make sure you did not use a phone cable in place of the Ethernet cable. A phone cable connector is narrower. Phone cable connectors feel loose or may wiggle in the Ethernet jack.
- Check your network status by opening System Preferences (MacOS X) or Control Panel (Windows), then clicking the Network icon. Enable Ethernet and DHCP if necessary.
- Reset the Gateway by pushing the small Reset button on the back panel.

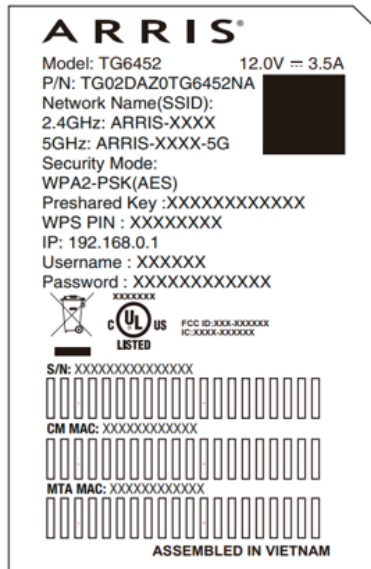
If you cannot solve the problem, contact your cable provider for help.

## Connect to the Gateway using Wi-Fi

► **To connect using Wi-Fi:**

1. Locate the sticker with the Wi-Fi network name and password (or "Preshared Key" or "Passcode" on some models).

The sticker is on the bottom or back of the Gateway, and looks like this:



**Bemærk:**

For at komme på Wi-Fi:

**Netværksnavnet (SSID)** er det, som fremgår af den seddel, du fik udleveret sammen med routeren, eller som fremgår af din side på selvbetjeningen for kabelnettet (hvor du selv kan ændre det).

**Kode til Wi-Fi** findes ligeledes dér.

Kun når du skal logge ind lokalt på selve routerens egen webside, så er brugernavnet **admin**, og dér skal benytte den Preshared Key der er trykt på etiketten, som password.

2. Connect to the network name (SSID) shown on the sticker. Some Gateway models may have two SSIDs on the sticker, one ending in -5 or -5G. The 5/5G network is faster, but not all devices support it. If your devices support both, connect to the 5/5G network.

Choose your operating system from the following list if you need help.

If your operating system is...	Then...
MacOS X	Open System Preferences, select the Network icon, then select the Wi-Fi tab. Choose the SSID from the dropdown menu that matches the name on your sticker.
iOS (iPad, iPhone, iPod touch)	Tap Settings, then Wi-Fi. Choose the SSID from the dropdown menu that matches the name on your sticker.
Windows	Open the Control Panel, select the Network and Sharing Center icon, then click Set Up a New Connection. Choose Connect to the Internet, and follow the instructions on the screen.
Android	Open Settings, tap Wireless & VPN, then Wi-Fi. Choose the SSID from the list that matches the name on your sticker.

3. When your device asks for a password, enter the password shown on the sticker.



**Important:** Be sure to enter the password exactly as shown.

- When the device indicates a successful connection, attempt to access an external website, such as [ARRIS documentation](#).

If successful, proceed to [Log in to the configuration interface](#) (page 6).

If you have a problem, check the following:

- Make sure the Gateway is powered on and connected to the cable provider's network. The Online and Wireless lights on the front panel should be lit.
- If your computer or tablet is in a different room from the Gateway, move it into the same room.
- Double-check the password. It must be entered exactly as printed on the sticker; you cannot use "A" in place of "a," for example. A capital I and lower-case L (l), or capital O and 0 (zero), can be easy to confuse. There are no spaces in the password. On some models, it might be easy to confuse the serial number or WPS PIN with the password. Make sure you use the string labeled "Password" or "Preshared Key." The print is very small, so strong lighting or a magnifying glass may help.
- Make sure your computer or tablet is connected to the network whose name matches the name printed on the sticker. This may be an issue in high-density dwellings, where many nearby Gateways could have similar names. The last four letters of the network name are unique to each Gateway, but could be easy to confuse.
- Make sure your computer or tablet supports WPA2PSK security. WPA2PSK is the default security mode for ARRIS Gateway products. Some older devices may not support WPA2PSK; if this is the case, use a newer device if possible.
- If possible, try connecting a computer using Ethernet, as described above.
- Reset the Gateway by pushing the small Reset button on the back panel.

If you cannot solve the problem, contact your cable provider for help.

## Log in to the configuration interface

### ► *To log into the Gateway configuration interface:*

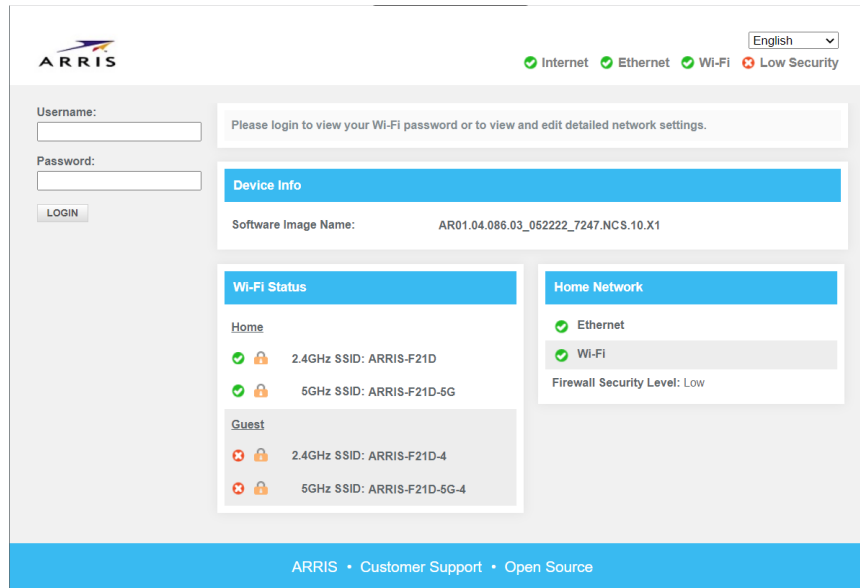
- Connect a computer or tablet to the Gateway, using the steps in [Connect to the Gateway](#) (page 4).
- In your browser's address bar, type `http://192.168.0.1/` and press Enter. <sup>\*)</sup>



**Note:** Your cable provider may have changed the default address. If so, look at the provided login information to find the right address.

The Login window appears.

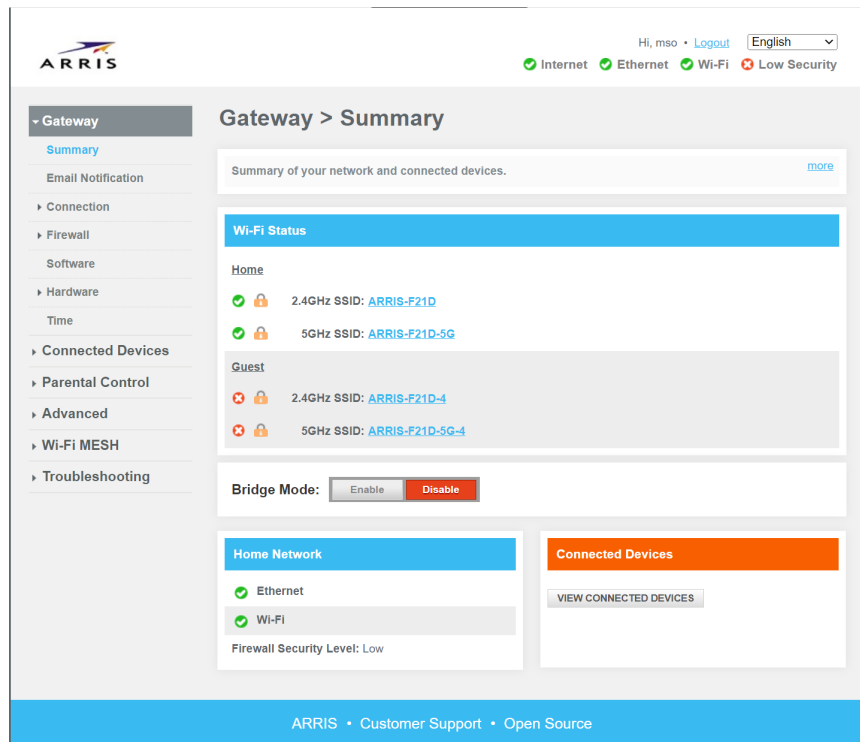
\*) Vi benytter en anden adresse:  
Den er enten `https://10.100.32.1/`  
eller `https://192.168.110.1/`



I stedet for **password**, så skriv den preshared key, som står på etiketten på bunden af routeren

3. Enter **admin** in the **Username** field, and **password** in the **Password** field, then click the **Login** button.

You should see the Gateway Summary screen:



4. Proceed to *How Do I...* (page 9).

If you cannot connect, perform the actions associated with the condition that best matches your situation.

- If you cannot connect to the Gateway at all:
  - Verify the Wireless light, on the Gateway's front panel, is on.

- If your computer shows more than one Wi-Fi network available, make sure you connected to the SSID shown on the Gateway's sticker.
- Verify that you entered the Wi-Fi password correctly.
- If you can connect to the Gateway, but cannot reach the Login page:
  - Make sure you typed the Gateway address properly, with periods between each set of numbers.
  - Check the cable provider's information packet for instructions.
- If you can see the Login page, but cannot log in:
  - Make sure you typed the user name and password correctly.
  - Check the cable provider's information packet for instructions.

## Password requirements

New passwords must meet the following requirements.

- 8 character minimum
- At least one lower-case alpha character
- At least one upper-case alpha character
- At least one numeric character
- At least one character from this string: ~!@#\$\$%^\* () -\_ =+ [] {} \ | ; : , . / ?

### Example:

Valid passwords include:

- **Brilliant\*Landscapel**
- **Turtle[24]**
- **Fi4-9Bz-22K**

Invalid passwords include:

- **joeBloggs** (no numeric or special characters)
- **Fox\*24** (too short)



## How Do I...

Find what you want to do in the following list and click the link to jump to that page.

How do I...

- [change my Wi-Fi network name?](#) (page 10) \*)
- [change my Wi-Fi network password?](#) (page 11) \*)
- [change my Gateway password?](#) (page 11)
- [hide my Wi-Fi network from other users?](#) (page 12)
- [see what devices are using my Gateway?](#) (page 13)
- [connect older devices to my Gateway?](#) (page 13)
- [keep the kids from accessing certain websites?](#) (page 14)
- [block certain devices from accessing my Gateway?](#) (page 15)
- [extend the range of my Wi-Fi network?](#) (page 17)
- [bypass the firewall?](#) (page 17)
- [make changes from somewhere else?](#) (page 18)
- [see if the Gateway is connected to the Internet?](#) (page 18)
- [connect if I've forgotten my Wi-Fi password?](#) (page 19)
- [reset the Gateway?](#) (page 19)
- [fix interference problems?](#) (page 20)
- [fix a slow connection?](#) (page 21)
- [change the language for the Gateway configuration page?](#) (page 21)
- [troubleshoot my connection?](#) (page 22)

\*)

Du kan ændre dit Wi-Fi netværksnavn (SSID) og koden til Wi-Fi via selvbetjeningen.

Derved overføres disse også automatisk til en ny router, hvis du får den udskiftet

## change my Wi-Fi network name?

1. Click **Gateway > Connection > Wi-Fi**.
2. Under **Home Wi-Fi Network**, locate the network you want to rename, and click **Edit**. The **Edit Wi-Fi Network** page displays:

The screenshot shows the ARRIS web interface for editing a Home 5 GHz Wi-Fi network. The breadcrumb trail is **Gateway > Connection > Wi-Fi > Edit Home 5 GHz**. The main content area includes the following settings:

- Wireless Network:**  Enable  Disable
- Network Name (SSID):**
- Security Mode:**  (Note: Please note 802.11 n/ac mode is only compatible with AES and Open encryption)
- Change Network Password:**   (Note: WPA2/3 requires a 8-63 ASCII character password)
- Broadcast Network Name (SSID):**  Enabled
- Enable WMM:**  Enabled

At the bottom of the settings area, there is a **Save Settings** section with a CAPTCHA challenge. The CAPTCHA code is **TL7Z**. Below the CAPTCHA is a text input field labeled "Type CAPTCHA Here" and two buttons:  and .

3. Change the network name (and anything else necessary), then click **Save Settings**. Devices connected to your Gateway may be disconnected after you make changes. Re-connect them with the new network name, and re-enter the password.

### Related information

[Gateway > Connection > Wi-Fi](#) (page 34)

Use these pages to manage Wi-Fi connection settings.

## change my Wi-Fi network password?

1. Click **Gateway > Connection > Wi-Fi**.
2. Change the password (and anything else necessary), then click **Save Settings**.  
Devices connected to your Gateway may be disconnected after you make changes. Re-connect them with the new network name, and re-enter the password.

### Related information

[Gateway > Connection > Wi-Fi](#) (page 34)

Use these pages to manage Wi-Fi connection settings.

## change my Gateway password?

1. Start the Home Network Wizard. To do this, click on the Gateway tab, then click **Wizard** in the side menu along the left.
2. Enter your current password in the Current Password field. If you have never changed this password, enter `password` here.
3. Enter the new password in the New Password field. To show what you typed, check the **Show Typed Password** box.  
Passwords are case-sensitive. Make sure your password conforms to the requirements listed. Do not use spaces.
4. Re-type the new password in the Re-enter New Password field.
5. Enter the captcha code in the Type CAPTCHA here field.
6. Click the **Next Step** button. Next time you access the Gateway configuration pages, you must enter the new password.

## hide my Wi-Fi network from other users?

1. Click **Gateway > Connection > Wi-Fi**.
2. Locate the network you want to hide, and click **Edit**.

The Edit Network page displays:

The screenshot shows the ARRIS web interface for editing Home 5 GHz network settings. The breadcrumb trail is 'Gateway > Connection > Wi-Fi > Edit Home 5 GHz'. The main content area includes a 'Home 5 GHz' section with the following settings:

- Wireless Network:  Enable  Disable
- Network Name (SSID):
- Security Mode:  (Note: Please note 802.11 n/ac mode is only compatible with AES and Open encryption!)
- Change Network Password:   (Note: WPA2/3 requires a 8-63 ASCII character password.)
- Broadcast Network Name (SSID):  Enabled
- Enable WMM:  Enabled

At the bottom, there is a 'Save Settings' section with a CAPTCHA code 'TL7Z' and a 'Type CAPTCHA Here' input field. The 'SAVE' button is visible.

3. Uncheck the **Broadcast Network Name (SSID)** box.
4. Click **Save Settings**.

This hides your network from a simple scan, but is not a good substitute for a strong password. With broadcast turned off, you must also remember your network names to connect new devices.

### Related information

[Gateway > Connection > Wi-Fi](#) (page 34)

Use these pages to manage Wi-Fi connection settings.

## see what devices are using my Gateway?

Click **Connected Devices > Devices**.

This screen displays a list of devices connected to this part of your network. The information includes:

- the name of the device (for example, "Joe Bloggs's iPad")
- the IP address the Gateway assigned to the device
- the MAC address of the device



**Tip:** If HomeAssure is enabled, you can also use [Wi-Fi MESH > AHNC > Network Topology](#) (page 86) to display connected devices by interface and network extender.

### Related information

[Connected Devices > Devices](#) (page 60)

This page shows devices connected to your network, as well as connection history.

## connect older devices to my Gateway?

Older devices may be limited in one or more of the following ways:

Limitation	Symptom
Supports only 2.4 GHz networks	Displays only 2.4 GHz networks when it scans
Supports only 802.11g or 802.11b operation	Entire Wi-Fi network slows down when the device is active
Supports only WEP security	Sees the network, but cannot connect

Of the three limitations, only the last requires a configuration change to support the device. If you have a mixture of old and new devices, dedicate the 2.4 GHz network to the older devices and use the 5 GHz network for those devices that can support it.



**Tip:** If possible, use Ethernet to connect older devices. This allows the Wi-Fi network to function with maximum performance and security.

### ► [To change the security mode to accommodate older devices:](#)

1. Click **Gateway > Connection > Wi-Fi**.
2. Choose the 2.4 GHz network you want to change, and click **Edit**.
3. Click the Security Mode dropdown, choose **Show More Security Mode Options**, then choose Open.



**CAUTION:** Anyone can connect to your network when the security mode is Open. If you have to use Open mode, disable your network when not in use.

### Related information

[Gateway > Connection > Wi-Fi](#) (page 34)

Use these pages to manage Wi-Fi connection settings.

## keep the kids from accessing certain websites?

Parental Control allows blocking specific web sites (URLs), and any webpage whose URL contains specified keywords. Blocking can be disabled for certain days and times if desired. In addition, you can specify up to two "trusted" devices that are not affected by blocking.



**Important:** No blocking system is foolproof.

1. To enable Parental Control:
  - a. Click **Parental Control > Managed Sites**.
  - b. At Managed Sites, click **Enable**.
  - c. To add trusted devices, click **Trusted** next to the MAC address of the devices you want to bypass parental controls.
2. To add a keyword filter:
  - a. Click **+Add** under Blocked Keywords.
  - b. In the dialog box:
    - enter the keyword that you want to block.
    - if you want to limit days or times the keyword is blocked, click **No** at Always Blocked.
    - check the days you want the block to take effect (or click **Select All**).
    - select the hours you want the block to take effect.
  - c. Click **Save** to complete the entry.
3. To add a web site filter:
  - a. Click **+Add** under Blocked Sites.
  - b. In the dialog box:
    - enter the web site that you want to block.
    - if you want to limit days or times the site is blocked, click **No** at Always Blocked.
    - check the days you want the block to take effect (or check ALL WEEK).
    - select the hours you want the block to take effect (or check ALL DAY).
  - c. Click **Save** to complete the entry.

New filters take effect immediately, but any filtered address already being displayed is not affected until the user follows another link.

### Related information

[Parental Control > Managed Sites](#) (page 64)

Use this page to block sites by URL or keyword.

## block certain devices from accessing my Gateway?

You can block devices in two ways:

- **Blacklist:** listed devices are not allowed to connect to the network. Use this method to prevent specific devices from connecting, even if the user knows the right password. (However, the user could use a different device not on the blacklist to connect.)
- **Whitelist:** only those devices listed may connect to the network.

Things to keep in mind:

- The blocking mechanism uses MAC addresses to uniquely identify each device on either list. You can find MAC addresses of connected devices by following the instructions in [see what devices are using my Gateway?](#) (page 13)
- The lists on your 2.4 GHz and 5 GHz networks are independent. This allows you to, for example, create a whitelist for your 5 GHz network while allowing any device (whose user has the password) to access the 2.4 GHz network.
- Users of whitelisted devices still need the correct password to access the network.
- Add devices before enabling blocking, especially whitelisting. The safest way to do this is to work from a computer connected to the Ethernet interface. If you make a mistake and block all devices, you can easily recover.



**Important:** No blocking system is foolproof.

1. To begin:
  - a. Click **Parental Control > Managed Devices**.
  - b. In Managed Devices, click **Enable**.
  - c. In Access Type, click **Allow All**.

2. To add devices to the list:



**Important:** Make sure Access Type is set to **Allow All** (blacklisting) for now. If you enable whitelisting without any devices in the list, nobody can access the network.

- a. Under Blocked Devices, click **+Add Blocked Device**.  
The Add Blocked Device page displays:

- b. If you want to block a device that has already connected to the Gateway, choose the devices from the Auto-Learned Devices list.
  - c. If you want to block a device not in the list, enter the MAC address to add to the list in the text box, then select the radio button next to the text box.
  - d. To set a list of times to block the device, set Always Block to **No**, then set the days and time range to block.
  - e. Click **Save** to save changes.
- Repeat this step as necessary to add more devices.
3. To remove devices from the list:
  - a. If necessary, click **Parental Control > Managed Devices**.
  - b. In the Blocked Devices list, click **X** in the device you want to remove.
4. To enable or disable blocking:
  - a. If necessary, click **Parental Control > Managed Devices**.
  - b. To disable blocking, set Managed Devices to **Disable**.
  - c. To enable blacklisting, set Access Type to **Allow All** (allow all devices except those listed).
  - d. To enable whitelisting, set Access Type to **Block All** (block all devices except those listed).

#### Related information

[Parental Control > Managed Devices](#) (page 69)

This screen lists managed devices.



## extend the range of my Wi-Fi network?

ARRIS Gateways support auto-configuration of the following network extenders:

- AR525 (Ethernet, Wi-Fi, MoCA)
- VAP4402 (Ethernet, Wi-Fi)

Place the extender within range of your Gateway, and follow the simple instructions to associate the Extender with your Gateway.

To see what extenders are connected to your Gateway, use one of:

- The [Wi-Fi MESH > AHNC > Network Topology](#) (page 86) page (if available)
- The HomeAssure mobile app (if available)

## bypass the firewall?

The Gateway provides a firewall that protects the devices on your home network from hacker attacks. Certain applications may not work properly through the firewall, and you can bridge a computer to bypass the firewall to accommodate those applications.

Before you attempt to do this:

- Make sure the bridged computer has the latest security updates, as it is not protected by the Gateway.
- Contact the application provider's technical support to determine whether there are workarounds that do not involve bridging.
- Contact your cable provider to learn whether there are any special requirements. The bridged computer must have its own public IP address.

▶ **To bridge a computer:**

1. Click **Advanced > DMZ**.
2. DMZ: Click **Enable**.
3. Enter the IP address of the computer you want to place outside the firewall. Use DMZ v4 Host unless you are using IPv6 addresses on your local network.
4. Click **Save**.

### Related information

[Advanced > DMZ](#) (page 77)

The DMZ page allows a single computer on the home network to bypass the firewall.

## make changes from somewhere else?

By default, the Gateway allows only locally-connected devices to access the configuration pages. If needed, a feature called Remote Management allows access to the configuration pages from specified Internet addresses.

Before you can enable Remote Management, you must change the default admin password. See [change my Gateway password?](#) (page 11) for instructions.

► **To set up Remote Management:**

1. Click **Advanced > Remote Management**.
2. If all the fields are disabled, you need to change the Gateway password as noted above.
3. Set HTTPS to **Enable**.
4. Note the IP address in the Remote Management Address (IPv4 or IPv6) box. This is the address of your Gateway.
5. Select an option from **Remote Access Allowed From**:

Option	Description
<b>Single Computer</b>	Allows access from one specific IP address. Use this option if you know exactly which IP address is used to access the Gateway.
<b>Range of IPs</b>	Allows access from any address in the specified range. Use this option if you know what network will be used to access the Gateway, but not the exact address.
<b>Any Computer</b>	Allows any computer to attempt to connect to the Gateway. This should only be done if there is no way to determine what IP address will be used to access the Gateway. Disable Remote Management as quickly as possible when using this option.

6. Fill in the IP address or range as needed.
7. Click **Save** to enable Remote Management from the selected IP addresses.
8. When finished, disable Remote Management by setting HTTPS to **Disable**.

### Related information

[Advanced > Remote Management](#) (page 76)

The Remote Management page allows computers outside the home network to access the Gateway's configuration pages.

## see if the Gateway is connected to the Internet?

1. First, check the front panel lights. The Power, US/DS, and Online lights should all be lit. If one or more of these three lights are off, the Gateway is not connected. Check the cable and power connections.
2. If the lights are on, connect a device to your network and attempt to access a known site such as <https://www.arris.com/consumers>.  
If you see the page, you are connected. If not, see [troubleshoot my connection?](#) (page 22) below.

## connect if I've forgotten my Wi-Fi password?

1. Look at the sticker on the bottom or back of the Gateway. The sticker lists the Wi-Fi network names and passwords used to access the Gateway using Wi-Fi.
2. If you have changed the default password and then forgotten it:
  - a. Connect to the Gateway without a password by using a computer with an Ethernet connection.
  - b. Access the Gateway configuration pages and use [change my Wi-Fi network password?](#) (page 11) to fix the password.

## reset the Gateway?

You may need to reset the Gateway if it begins working improperly, or to recover from misconfiguration. There are two kinds of reset available:

- **Restart:** similar to powering the Gateway off then turning it back on. If your Gateway provides telephone service, restarting it drops all calls as well as Internet connections. A restart does not affect your configuration settings. You also have the option of restarting only the router or the Wi-Fi module, which does not affect calls or the Gateway's Internet connection.
- **Factory reset:** restores the Gateway to the factory default settings, as if it were being set up for the first time. This includes network name, passwords, and all other configuration changes.
- To restart your Gateway, do one of the following:
  - If connected to the configuration pages, click **Troubleshooting > Restart/Restore**. Click **Restart Gateway**.
  - Locate the Reset button on the back of the Gateway. Use a non-metallic, pointed object to press the button once.
- To factory-reset your Gateway, do one of the following:
  - If connected to the configuration pages, click **Troubleshooting > Restart/Restore**. Click the **Restore Gateway Defaults** button.
  - Locate the Reset button on the back of the Gateway. Use a non-metallic, pointed object to press and hold the button for about ten seconds.

### Related information

[Troubleshooting > Restart/Restore](#) (page 91)

Restarts the entire Gateway, or selected components.

## fix interference problems?

When the Gateway starts up, it monitors all wireless channels and automatically selects the channel with the least activity (that is, signals from Wi-Fi devices and noise from other sources).

Many electric and electronic devices produce radio waves, intentionally or not, that can interfere with Wi-Fi signals. The most typical devices include:

- microwave ovens
- Bluetooth devices
- cordless telephones and base stations
- baby monitors
- wireless cameras, speakers, or game controllers
- electric motors (including refrigerators, dryers, and furnaces)
- ▶ ***To display a list of other Wi-Fi networks in the immediate area:***

1. Click **Troubleshooting > Wi-Fi Spectrum Analyzer**.
2. Wait for the scan to complete.
3. Locate your Wi-Fi network in the list and see whether there are other access points using the same or adjacent channels.
4. If there are no other networks sharing your channel, the problem is likely interference from non-Wi-Fi devices. Try to relocate such devices at least 6 feet (2m) from the Gateway.

### Related information

[Troubleshooting > Wi-Fi Spectrum Analyzer](#) (page 89)

Displays all Wi-Fi networks detected by the Gateway radios.

## fix a slow connection?

The following issues can cause a slow connection:

**Cause:** older 802.11g or 802.11b devices connected to the Wi-Fi network

**Solution:**

- If possible, put older devices on an Ethernet connection. If not, consider dedicating the 2.4 GHz network to older devices and move newer devices to the 5 GHz network.

**Cause:** a large number of devices on your Wi-Fi network all attempting to access the Internet

**Solution:**

- If possible, move your fastest devices to the 5 GHz network for best performance.

**Cause:** a computer downloading a large system update

**Solution:**

- Some operating systems provide the option of downloading system updates overnight. If possible, postpone the update.

**Cause:** one or more streaming video services in use

**Solution:**

- Wait for the show to finish.

**Cause:** many neighbors using the Internet (a neighborhood shares the same connection to the cable network's routers)

**Solution:**

- Ask your service provider to upgrade the network.

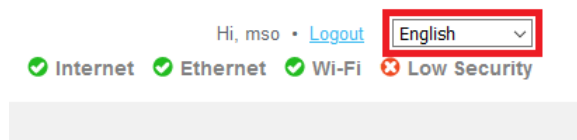
**Cause:** congestion on the Internet itself

**Solution:**

- If possible, try accessing the network later.

## change the language for the Gateway configuration page?

On any page, select the language you want from the dropdown menu at the top-right of the page.



---

## troubleshoot my connection?

**Solution:**

1. Always check the easy things first. Make sure the Gateway has power (the Power light on the front panel is lit) and the coax connection is finger-tight at both the Gateway and the wall jack.
2. If you have telephone service through the Gateway, pick up the phone. If you have dial tone and can call out, the Gateway is properly connected to the cable provider's network equipment.
3. Try to connect with a different device to see whether the problem is limited to one device. If possible, connect a device to the Gateway using Ethernet.

If the problems persist, find the item below that most closely matches your problem and follow the instructions.

**Cause:** My devices can't see the Wi-Fi networks.

**Solution:**

1. Using a computer connected to the Gateway Ethernet, see [hide my Wi-Fi network from other users?](#) (page 12) to see whether the Gateway is broadcasting its SSID. If needed, check the Broadcast Network Name (SSID) box and click **Save**.
2. Click **Gateway > Connection > Wi-Fi**.
  - Make sure the radios are enabled.
  - If the names in Home Wi-Fi Network do not look like what you expect, change them if needed.

When you have made any necessary changes, click **Save Network Settings**.

3. If you are still having problems, call your cable provider support line.

**Cause:** My devices see the Wi-Fi networks, but can't connect.

**Solution:**

1. If the devices having problems are older, see [connect older devices to my Gateway?](#) (page 13) for help.
2. Using a computer connected to the Gateway Ethernet:
  - a. Click **Gateway > Connection > Wi-Fi**.
  - b. If needed, click Edit on the network and change the Network Password.
  - c. Make any other changes necessary, then click **Save Settings**.
3. Follow the steps in to restore the Gateway to factory defaults, which should allow you to connecting using the password on the Gateway's sticker.
4. If you are still having problems, call your cable provider support line.

**Cause:** The connection is always slow.

**Solution:**

1. Try the suggestions in [fix a slow connection?](#) (page 21)
2. Connect to the Gateway, using Ethernet if possible, and access <http://speedtest.net/>. (Click the large **GO** button in the middle of the page.)

Make sure none of your other devices are active when you run the speed test. Note the results and run more speed tests at different times through the day.

Call your cable provider support line to find out what speeds you should expect.

**Cause:** The connection is usually OK, but sometimes it gets slow.

**Solution:**

1. Note the times when the connection gets slow, preferably over a week.  
If you discover a consistent pattern, the problem is likely network congestion during peak hours. Ask your cable provider when they plan to increase capacity in your area.
2. If the slow times happen at random, the problem is likely interference. See [fix interference problems?](#) (page 20) for tips.

**Related information**

[Gateway > Connection > Wi-Fi](#) (page 34)

Use these pages to manage Wi-Fi connection settings.

# Gateway Setup



In these pages, you can:

- configure the Gateway
- view information about the Gateway configuration



## Gateway > Summary

The Summary page provides a brief overview of your Gateway's configured networks (SSIDs) and connected devices.

The screenshot displays the 'Gateway > Summary' page. At the top right, it shows the user 'Hi, mso' with a 'Logout' link and a language dropdown set to 'English'. Below this, there are status indicators: a green checkmark for 'Internet', a green checkmark for 'Ethernet', a green checkmark for 'Wi-Fi', and a red 'X' for 'Low Security'. On the left, a navigation menu is visible with 'Gateway' selected, and sub-items like 'Summary', 'Email Notification', 'Connection', 'Firewall', 'Software', 'Hardware', 'Time', 'Connected Devices', 'Parental Control', 'Advanced', 'Wi-Fi MESH', and 'Troubleshooting'. The main content area is titled 'Gateway > Summary' and contains a 'Summary of your network and connected devices' section with a 'more' link. Below this is the 'Wi-Fi Status' section, which is divided into 'Home' and 'Guest' networks. Under 'Home', there are two entries: '2.4GHz SSID: ARRIS-F21D' (enabled, green checkmark) and '5GHz SSID: ARRIS-F21D-5G' (enabled, green checkmark). Under 'Guest', there are two entries: '2.4GHz SSID: ARRIS-F21D-4' (disabled, red X) and '5GHz SSID: ARRIS-F21D-5G-4' (disabled, red X). Below the Wi-Fi status is the 'Bridge Mode' section with 'Enable' and 'Disable' buttons. The 'Home Network' section shows 'Ethernet' and 'Wi-Fi' as enabled, with a 'Firewall Security Level: Low' indicator. The 'Connected Devices' section has a 'VIEW CONNECTED DEVICES' button. At the bottom of the page, there is a footer with 'ARRIS • Customer Support • Open Source'.

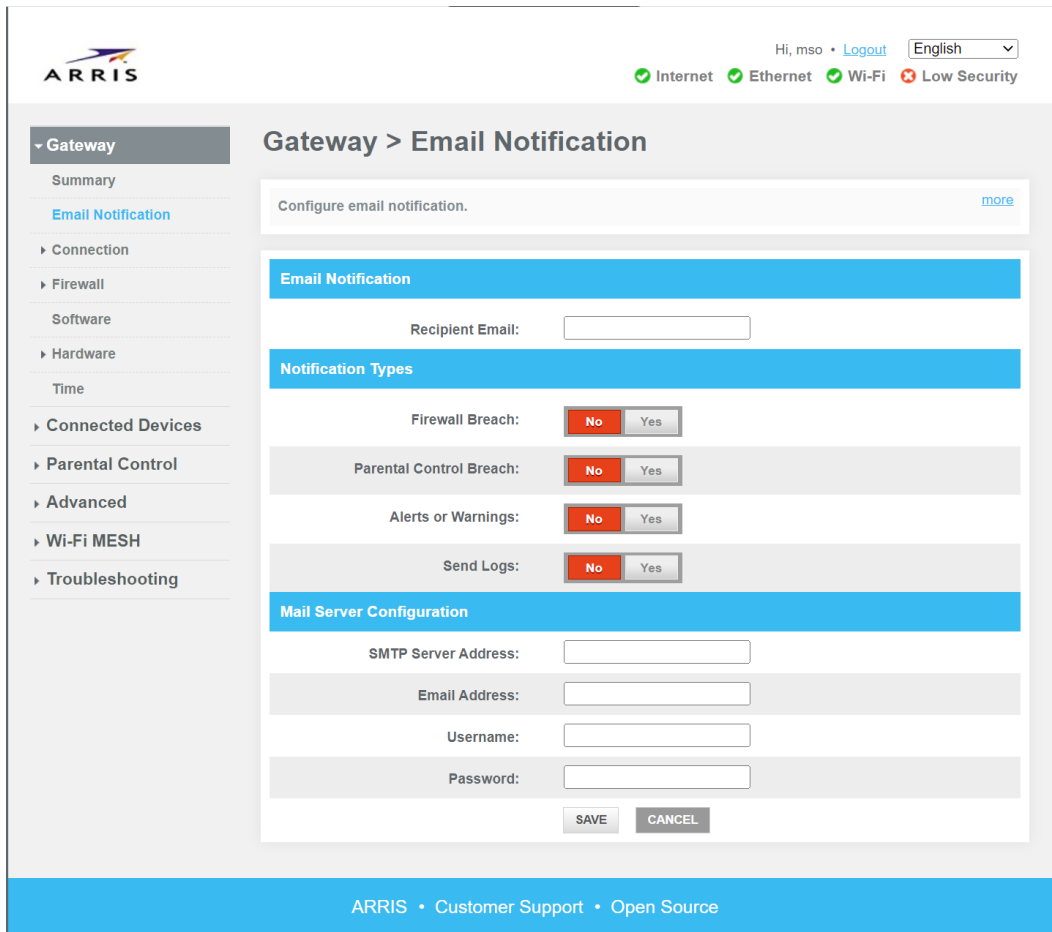
- **Wi-Fi Status:** Displays your configured Wi-Fi networks. Networks with a  are enabled, and those with a  are disabled. Click an SSID name to open the Edit page for that network.



- **Bridge Mode:** Click **Enable** to enable Bridge mode. In Bridge mode, most Gateway functionality is disabled. Your cable provider may limit the number of Bridge mode connections to one or two devices. Only enable Bridge mode when advised by your cable provider.
- **Home Network:** Displays the available interfaces on your Gateway. Interfaces with a  are enabled, and those with a  are disabled.
- **Connected Devices:** Shows a brief list of connected devices. Use the [Connected Devices > Devices](#) (page 60) page or the [Wi-Fi MESH > AHNC > Network Topology](#) (page 86) page to display all connected devices.





## Gateway > Email Notification

Email notification sends email to the specified address under a number of conditions.



ARRIS

Hi, mso • [Logout](#) English

 Internet  Ethernet  Wi-Fi  Low Security

Gateway > Email Notification

Configure email notification. [more](#)

**Email Notification**

Recipient Email:

**Notification Types**

Firewall Breach:

Parental Control Breach:

Alerts or Warnings:

Send Logs:

**Mail Server Configuration**

SMTP Server Address:

Email Address:

Username:

Password:

ARRIS • Customer Support • Open Source

- **Recipient Email:** The email address to receive notifications. Enter this address carefully.
- **Notification Types:** Click **Yes** for each condition that should trigger an email.
- **Mail Server Configuration:** Enter the following information:
  - **SMTP Server Address:** address of the SMTP server that controls email for the target address

- **Email Address:** the email address that receives the notifications (should match Recipient Email)
- **Username:** the user name for connecting to the SMTP server
- **Password:** the password for connecting to the SMTP server

Click **Save** to save your changes.



**Tip:** If you need help finding Mail Server Configuration items, look at the setup information for the email client on your computer or tablet.

## Gateway > Connection

These pages allow you to view and set network parameters.

## Gateway > Connection > Status

Displays the status for each supported Gateway network.

The image has been split vertically to make its sub-components easier to see.

The screenshot shows the ARRIS Gateway > Connection > Status page. The left side displays network connection details, and the right side displays the status of various Wi-Fi networks.

**Gateway > Connection > Status**

View information about your network connections.

**WAN**

- Internet: Active
- WAN IP Address: 10.19.191.183
- DHCP Client: Enabled
- DHCP Expire Time: 0d 15h 36m 57s

**Local IP Network**

- Number of Clients Connected: 0

**IPv4**

- IP Address (IPv4): 192.168.0.1
- Subnet Mask: 255.255.255.0
- DHCPv4 Server: Enabled
- DHCPv4 Lease Time: 0d 1h 0m 0s

**IPv6**

- Link Local Gateway Address (IPv6): fe80::9ecb:fcff:fe52:33c1
- Global Gateway Address (IPv6):
- Delegated prefix:
- DHCPv6 Lease Time: 7d 0h 0m 0s
- IPv6 DNS: ::

**Home Wi-Fi Network (2.4 GHz)**

- SSID: ARRIS-F21D
- Status: Active
- Supported Protocols: G,N
- Security: WPA2-PSK (AES)
- Number of Clients Connected: 0

**Guest Wi-Fi Network (2.4 GHz)**

- SSID: ARRIS-F21D-4
- Status: Inactive
- Supported Protocols: G,N
- Security: WPA2-PSK (AES)
- Number of Clients Connected: 0

**Guest Wi-Fi Network (5 GHz)**

- SSID: ARRIS-F21D-5G-4
- Status: Inactive
- Supported Protocols: A,N,AC
- Security: WPA2-PSK (AES)
- Number of Clients Connected: 0

**Public Wi-Fi Network (2.4 GHz)**

- SSID: ARRIS-F21D-3
- Arris Wi-Fi Capable: Yes
- Status: Inactive
- Time Since Last Status: 16d 18h 25m 7s
- WLAN Gateway: 0.0.0.0/0.0.0.0
- Supported Protocols: G,N
- Security: WPA2-Enterprise (AES)
- Number of Clients Connected: 0

**Public Wi-Fi Network (5 GHz)**

- SSID: ARRIS-F21D-5G-3
- Arris Wi-Fi Capable: Yes
- Status: Inactive
- Time Since Last Status: 16d 18h 25m 7s
- WLAN Gateway: 0.0.0.0/0.0.0.0
- Supported Protocols: A,N,AC
- Security: WPA2-Enterprise (AES)
- Number of Clients Connected: 0

ARRIS • Customer Support • Open Source

The network types are:

- WAN Network (the connection to the cable system)
- Local IP Network (the information common to all Ethernet and Wi-Fi interfaces on this Gateway)
- Home Wi-Fi Network (the Wi-Fi networks your household devices use)

- Guest Wi-Fi Network (Wi-Fi networks reserved for your guests)
- Home Security Network (Wi-Fi networks reserved for remotely-monitored home security devices)
- Public Wi-Fi Network (Wi-Fi networks operated by the cable provider)
- Out of service (Wi-Fi networks available for use, but not enabled)

The Edit button in...	Opens...
WAN	<a href="#">Gateway &gt; Connection &gt; WAN Network</a> (page 28)
IPv4	<a href="#">Gateway &gt; Connection &gt; Local IP Network</a> (page 30) (IPv4)
IPv6	<a href="#">Gateway &gt; Connection &gt; Local IP Network</a> (page 30) (IPv6)
Home Wi-Fi Network (2.4 GHz)	<a href="#">Gateway &gt; Connection &gt; Wi-Fi &gt; Edit 2.4 Ghz</a> (page 35)
Home Wi-Fi Network (5 GHz)	<a href="#">Gateway &gt; Connection &gt; Wi-Fi &gt; Edit 5 Ghz</a> (page 37)
Guest Wi-Fi Network (2.4 GHz)	<a href="#">Gateway &gt; Connection &gt; Wi-Fi &gt; Edit 2.4 Ghz</a> (page 35)
Guest Wi-Fi Network (5 GHz)	<a href="#">Gateway &gt; Connection &gt; Wi-Fi &gt; Edit 5 Ghz</a> (page 37)
Public Wi-Fi Network (2.4 GHz)	<a href="#">Gateway &gt; Connection &gt; Wi-Fi &gt; Edit 2.4 Ghz</a> (page 35)
Public Wi-Fi Network (5 GHz)	<a href="#">Gateway &gt; Connection &gt; Wi-Fi &gt; Edit 5 Ghz</a> (page 37)

# Gateway > Connection > WAN Network

Provides detailed information about the connection between the Gateway and the cable provider.

The image has been split vertically to make its sub-components easier to see.

The screenshot displays the 'Gateway > Connection > WAN Network' configuration page. The left sidebar shows a navigation tree with sections like WAN Network, WAN DHCP Parameters, WAN IP Time Remaining, WAN Cable Modem, WAN Downstream QAM, WAN Downstream OFDM, WAN Upstream QAM, and WAN Upstream OFDMA. The main content area is split into two vertical panels. The right panel shows detailed information for each section, including IP addresses, DNS servers, DHCP parameters, cable modem statistics, and channel status tables.

- **WAN Network:** Information about the WAN IP address, DNS servers, and the local DHCP server.
- **Initialization Procedure:** The status of each step in the connection procedure. This information may be useful if your Gateway is having trouble connecting to the cable provider.
- **CM DHCP Parameters:** Information that the cable modem module received from the cable provider's DHCP server.
- **CM IP Time Remaining:** Various DHCP timers.
- **Cable Modem:** Information about the cable modem module's hardware and firmware.
- **Downstream QAM:** Shows downstream QAM channels status. Your cable provider can use this information to diagnose connection issues.
- **Downstream OFDM:** Shows downstream OFDM channels status. Your cable provider can use this information to diagnose connection issues.
- **Upstream QAM:** Shows upstream QAM channels status.
- **Upstream OFDMA:** Shows upstream OFDMA channel status.
- **CM Error Codewords:** Shows codeword statistics by channel.

## Gateway &gt; Connection &gt; WAN Configuration

Configures WAN IP and DNS connection information.

ARRIS

Hi, mso • [Logout](#) English

Internet Ethernet Wi-Fi Low Security

Gateway > Connection > WAN Configuration

Manage your WAN settings [more](#)

**IPv4**

WAN IP Settings:  Obtained automatically  Statically configured

WAN IP Address: 10 . 19 . 191 . 183

Subnet Mask: 255 . 255 . 255 . 192

Default Gateway: 10 . 19 . 191 . 190

Host Name: arrisatom

Domain Name: dev192

WAN DNS:  Obtained automatically  Statically configured

Primary DNS Server: 10 . 1 . 50 . 96

Secondary DNS Server: - . - . - . -

**Save Settings**

Please type this CAPTCHA code or click on it for a new code:

2 Y W W

Type CAPTCHA Here

SAVE CANCEL

ARRIS • Customer Support • Open Source

- **WAN IP Settings:** Unless instructed by your service provider, use **Obtained automatically**. Select **Statically configured** to manually configure these WAN IP settings.
  - **WAN IP Address:** The IP address for your WAN connection.
  - **Subnet Mask:** The IP subnet mask.
  - **Default Gateway:** The IP address of the gateway (in the service provider's office, not your Gateway product).
  - **Host Name:** The host name for your Gateway.
  - **Domain Name:** The domain name for your Gateway.
- **WAN DNS:** Unless instructed by your service provider, use **Obtained automatically**. Select **Statically configured** to manually configure these DNS server settings.

- **Primary DNS Server:** The IP address of the primary DNS server.
- **Secondary DNS Server:** The IP address of a secondary DNS server. Your Gateway uses this server to resolve domain names if the primary server is unreachable.

To save changes to the WAN settings, enter the captcha text beneath the image, then click **Save**.

## Gateway > Connection > Local IP Network

Use these pages to manage home network settings. In most cases, the defaults are suitable.

### Gateway > Connection > Local IP Network > IPv4

Use these pages to manage IPv4 home network settings.

The screenshot shows the ARRIS web interface for configuring IPv4 settings. The breadcrumb navigation is 'Gateway > Connection > Local IP Network > IPv4'. The main content area is titled 'Manage your home network settings.' and contains the following settings:

- Gateway Address:** 192 . 168 . 0 . 1 / 24
- Subnet Mask:** 255 . 255 . 255 . 0
- Enable DHCP Server:**  Enabled
- DHCP Beginning Address:** 192 . 168 . 0 . 2
- DHCP Ending Address:** 192 . 168 . 0 . 253
- DHCP Lease Time:** 1 Hours
- Enable IPv4/IPv6 DNS Relay:**  Enabled
- LAN DNS:**  Obtained automatically  Statically configured
- Primary DNS Server:** 10 . 1 . 50 . 96
- Secondary DNS Server:** [Empty fields]

A CAPTCHA challenge is displayed at the bottom of the settings area with the text: 'Please type this CAPTCHA code or click on it for a new code:'. The CAPTCHA image shows the characters 'P77L'. Below the image is a text input field labeled 'Type CAPTCHA Here' and a 'SAVE SETTINGS' button.

- **Gateway Address:** The IP address of the Gateway. Connecting to this address, using a browser, shows these pages. The last field is the subnet length; use the default of 24 unless you have special needs.

- **Subnet Mask:** The IP subnet mask. XXX if you change the subnet field above, does this adjust? XXX
- **Enable DHCP Server:** Check to enable the Gateway DHCP server. This allows the Gateway to assign local IP addresses to connecting clients.
- **DHCP Beginning Address:** Enter the lowest address of the DHCP pool, a block of dynamic addresses.
- **DHCP Ending Address:** Enter the highest address of the DHCP pool. You can use subnet addresses outside this range to assign static addresses to devices such as media servers, that should always have the same address.
- **DHCP Lease Time:** The time a device "owns" an IP address. When the lease time expires, a device may attempt to renew the lease or request a new address.
- **Enable IPv4/IPv6 DNS Relay:** Check to enable DNS Relay on the gateway. When DNS Relay is active, devices on the LAN send DNS requests to the Gateway. The Gateway in turn caches addresses, and queries the service provider's DNS server for addresses it does not have in the cache. This increases network performance by eliminating some external DNS queries.  
When the checkbox is cleared, the LAN DNS field is enabled.
- **LAN DNS:** Unless instructed by your service provider, use the default **Obtained automatically** setting. Selecting **Statically configured** enables the next two fields.
  - **Primary DNS Server:** The IP address of the primary DNS server.
  - **Secondary DNS Server:** The IP address of a secondary DNS server. Your devices use this server to resolve domain names if the primary server is unreachable.

To save changes to the network settings, enter the captcha text beneath the image, then click **Save Settings**.

## Gateway &gt; Connection &gt; Local IP Network &gt; IPv6

Use these pages to manage IPv6 home network settings.

ARRIS

Hi, mso • Logout English

Internet Ethernet Wi-Fi Low Security

Gateway > Connection > Local IP Network > IPv6

Manage your home network settings. [more](#)

**IPv6**

Link-Local Gateway Address: fe80 : 0 : 0 : 0 : 9ec8 : fcff : fe52 : 33c1

Global Gateway Address: : : : : : : : :

LAN IPv6 Address Assignment

Enable Stateful (DHCP Server):  Enabled

DHCPv6 Beginning Address: : : : : 0 : 0 : 0 : 0001 /

DHCPv6 Ending Address: : : : : 0 : 0 : 0 : fffe /

DHCP Lease Time: 1 Weeks

Enable IPv4/IPv6 DNS Relay:  Enabled

LAN DNS:  Obtained automatically  Statically configured

Primary DNS Server: : : : : : : : :

Secondary DNS Server: : : : : : : : :

Please type this CAPTCHA code or click on it for a new code:

637L

Type CAPTCHA Here

SAVE SETTINGS

ARRIS • Customer Support • Open Source

- **Link-Local Gateway Address:** The IPv6 address of the Gateway, on the LAN. This address is automatically generated using the MAC address of the network interface.
- **Global Gateway Address:** The IPv6 global address of the Gateway. Global addresses are meant to be reachable from anywhere in the IPv6 internet.
- **Enable Stateful (DHCP Server):** Check to enable the Gateway DHCPv6 server. This allows the Gateway to assign local IPv6 addresses to connecting clients.
- **DHCPv6 Beginning Address:** Enter the lowest address of the DHCP pool, a block of dynamic addresses.



- **DHCPv6 Ending Address:** Enter the highest address of the DHCP pool. You can use subnet addresses outside this range to assign static addresses to devices such as media servers, that should always have the same address.
- **DHCP Lease Time:** The time a device "owns" an IP address. When the lease time expires, a device may attempt to renew the lease or request a new address.
- **Enable IPv4/IPv6 DNS Relay:** Check to enable DNS Relay on the gateway. When DNS Relay is active, devices on the LAN send DNS requests to the Gateway. The Gateway in turn caches addresses, and queries the service provider's DNS server for addresses it does not have in the cache. This increases network performance by eliminating some external DNS queries.

When the checkbox is cleared, the LAN DNS field is enabled.

- **LAN DNS:** Unless instructed by your service provider, use the default **Obtained automatically** setting. Selecting **Statically configured** enables the next two fields.
  - **Primary DNS Server:** The IP address of the primary DNS server.
  - **Secondary DNS Server:** The IP address of a secondary DNS server. Your devices use this server to resolve domain names if the primary server is unreachable.

To save changes to the network settings, enter the captcha text beneath the image, then click **Save Settings**.

## Gateway > Connection > Wi-Fi

Use these pages to manage Wi-Fi connection settings.

### Gateway > Connection > Wi-Fi > Networks

Use this page to manage Wi-Fi networks on this Gateway.

The screenshot shows the 'Networks' page in the ARRIS Gateway web interface. The page title is 'Gateway > Connection > Wi-Fi > Networks'. The main content area is divided into three sections: Home Wi-Fi Network, Guest Wi-Fi Network, and Public Wi-Fi Network. Each section contains a table with columns for Name, Frequency Band, MAC Address, and Security Mode, along with an 'EDIT' button. Below each table are checkboxes for 'Band Steering' and 'AP Isolation'. At the bottom, there is a 'Network Options' section with a 'Network Priorities' checkbox and a 'SAVE NETWORK SETTINGS' button.

Home Wi-Fi Network			
Name	Frequency Band	MAC Address	Security Mode
ARRIS-F21D	2.4 GHz	9C:C8:FC:52:33:BF	WPA2-PSK (AES)
ARRIS-F21D-5G	5 GHz	9C:C8:FC:52:33:C0	WPA2-PSK (AES)

Guest Wi-Fi Network			
Name	Frequency Band	MAC Address	Security Mode
ARRIS-F21D-4	2.4 GHz	9E:C8:FC:52:33:AF	WPA2-PSK (AES)
ARRIS-F21D-5G-4	5 GHz	9E:C8:FC:52:33:A0	WPA2-PSK (AES)

Public Wi-Fi Network			
Name	Frequency Band	MAC Address	Security Mode
ARRIS-F21D-3	2.4 GHz	9E:C8:FC:52:33:9F	WPA2-Enterprise (AES)
ARRIS-F21D-5G-3	5 GHz	9E:C8:FC:52:33:90	WPA2-Enterprise (AES)

- Home Wi-Fi Network:** Lists 2.4 GHz and 5 GHz SSIDs for the primary home network. Click **Edit** to configure each SSID.
    - Band Steering:** Enables or disables band steering on the home network.
    - AP isolation:** Check this box to enable AP isolation. This disables direct connections between two clients on the same network; any connections go through the Internet.
  - Guest Wi-Fi Network:** Lists 2.4 GHz and 5 GHz SSIDs for the guest network. Click **Edit** to configure each SSID.
    - AP isolation:** Check this box to enable AP isolation. This disables direct connections between two clients on the same network; any connections go through the Internet.
  - Public Wi-Fi Network:** Lists 2.4 GHz and 5 GHz SSIDs for the public (hotspot) network. Click **Edit** to configure each SSID.
  - Network Priorities:** When enabled, the Gateway displays a slider, allowing you to split air time between the home and guest networks. Note that this applies only when both networks are sending or receiving data at the same time; if you set the guest network to 0%, devices on that network still get air time when the home network is idle.
- Click **Save Network Settings** to commit your changes.

Gateway > Connection > Wi-Fi > Edit 2.4 GHz

Use this page to configure the 2.4 GHz networks. Guest and Public networks have the same settings as Home networks.

The screenshot displays the ARRIS web interface for configuring Home 2.4 GHz network settings. The page title is "Gateway > Connection > Wi-Fi > Edit Home 2.4 GHz". The main content area is titled "Home 2.4 GHz" and contains the following settings:

- Wireless Network:** Enable (selected) / Disable
- Network Name (SSID):** ARRIS-F21D
- Security Mode:** WPA2-PSK (AES) (Recommended) (selected)
- Change Network Password:** [Empty field] / SHOW
- Broadcast Network Name (SSID):**  Enabled
- Enable WMM:**  Enabled

A "Save Settings" button is located at the bottom of the form. A CAPTCHA dialog is overlaid on the page, asking the user to "Please type this CAPTCHA code or click on it for a new code:". The CAPTCHA code is "KWXK". The dialog includes a "Type CAPTCHA Here" input field, a "SAVE" button, and a "CANCEL" button.

- **Wireless Network:** Enables or disables the network.
- **Network Name (SSID):** Enter the name for this network.
- **Security Mode:** Select the security mode for this network. The choice "Show More Security Mode Options" displays this dialog:

**Security Mode**

The recommended security mode is "WPA2-PSK (AES)" as it provides the best security and performance.

**WPA2-PSK (AES) (Recommended)**  
This is the recommended option, but it requires that all the Wi-Fi devices in your network support WPA2 with AES encryption. Any older Wi-Fi devices which do not support WPA2 and AES encryption will not be able to connect to your Wi-Fi network in this mode.

**WPAWPA2-PSK (TKIP/AES)**  
This option is compatible with the most Wi-Fi devices. It allows Wi-Fi devices to connect with WPA (with TKIP or AES encryption) or WPA2 (with TKIP or AES encryption). To achieve best Wi-Fi performance in this mode, the Wi-Fi devices must connect using WPA2 with AES encryption.

**Open (Risky)**  
This is not recommended as it does not have any security and anybody can connect to your Wi-Fi network.

Save Cancel

- **Change Network Password:** Enter a new password in the text box. Click **SHOW** to show the password in the clear (to make sure you entered it correctly).
- **Broadcast Network Name (SSID):** Check this box to list this network as available when a client is looking for networks. If unchecked, clients must enter the name manually.
- **Enable WMM:** Check this box to enable Wi-Fi Multimedia (WMM). When WMM is enabled, multimedia content streaming through this network is prioritized. This may reduce video buffering.

To save changes to the network settings, enter the captcha text beneath the image, then click **Save**.

Gateway > Connection > Wi-Fi > Edit 5 Ghz

Use this page to configure the 5 GHz networks. Guest and Public networks have the same settings as Home networks.

The screenshot shows the ARRIS web interface for configuring a Home 5 GHz network. The breadcrumb trail is 'Gateway > Connection > Wi-Fi > Edit Home 5 GHz'. The page title is 'Gateway > Connection > Wi-Fi > Edit Home 5 GHz'. The main content area is titled 'Home 5 GHz' and contains the following settings:

- Wireless Network:** Enabled (with a 'Disable' button)
- Network Name (SSID):** ARRIS-F21D-5G
- Security Mode:** WPA2-PSK (AES) (Recommended) (with a dropdown arrow)
- Please note 802.11 n/ac mode is only compatible with AES and Open encryption!
- Change Network Password:** (with a 'SHOW' button)
- WPA2/3 requires a 8-63 ASCII character password.
- Broadcast Network Name (SSID):**  Enabled
- Enable WMM:**  Enabled

At the bottom of the settings area is a blue 'Save Settings' button. A CAPTCHA dialog is overlaid on this button, displaying the text 'Please type this CAPTCHA code or click on it for a new code:' and the CAPTCHA code 'TL7Z'. Below the CAPTCHA is a text input field labeled 'Type CAPTCHA Here' and 'SAVE' and 'CANCEL' buttons.

The footer of the page contains the text: ARRIS • Customer Support • Open Source

- **Wireless Network:** Enables or disables the network.
- **Network Name (SSID):** Enter the name for this network.
- **Security Mode:** Select the security mode for this network. The choice "Show More Security Mode Options" displays this dialog:

**Security Mode**

The recommended security mode is "WPA2-PSK (AES)" as it provides the best security and performance.

**WPA2-PSK (AES) (Recommended)**  
This is the recommended option, but it requires that all the Wi-Fi devices in your network support WPA2 with AES encryption. Any older Wi-Fi devices which do not support WPA2 and AES encryption will not be able to connect to your Wi-Fi network in this mode.

**WPAWPA2-PSK (TKIP/AES)**  
This option is compatible with the most Wi-Fi devices. It allows Wi-Fi devices to connect with WPA (with TKIP or AES encryption) or WPA2 (with TKIP or AES encryption). To achieve best Wi-Fi performance in this mode, the Wi-Fi devices must connect using WPA2 with AES encryption.

**Open (Risky)**  
This is not recommended as it does not have any security and anybody can connect to your Wi-Fi network.

Save Cancel

- **Change Network Password:** Enter a new password in the text box. Click **SHOW** to show the password in the clear (to make sure you entered it correctly).
- **Broadcast Network Name (SSID):** Check this box to list this network as available when a client is looking for networks. If unchecked, clients must enter the name manually.
- **Enable WMM:** Check this box to enable Wi-Fi Multimedia (WMM). When WMM is enabled, multimedia content streaming through this network is prioritized. This may reduce video buffering.

To save changes to the network settings, enter the captcha text beneath the image, then click **Save**.

## Gateway &gt; Connection &gt; Wi-Fi &gt; 2.4 GHz Radio

Use this page to configure the 2.4 GHz radio.

The screenshot displays the ARRIS web GUI for configuring the 2.4 GHz Wi-Fi radio. The page title is "Gateway > Connection > Wi-Fi > 2.4 GHz Radio". The left sidebar shows a navigation menu with options like Gateway, Connection, WAN, Local IP Network, Wi-Fi (selected), Networks, 2.4 GHz Radio (selected), 5 GHz Radio, MAC Filtering, WPS, GRE, MTA, CallIP/QoS, VQM, Firewall, Software, Hardware, Time, Connected Devices, Parental Control, Advanced, Wi-Fi MESH, and Troubleshooting. The main content area is titled "2.4 GHz Wi-Fi Radio Configuration" and contains the following settings:

- Wireless Radio:**  Enable  Disable
- Mode:** 802.11 g/n
- Tx Power:** 100%
- Channel Selection:**  Manual  Automatic
- Channel:** 11
- Channel Bandwidth:**  20  20/40  Auto
- Dynamic Channel Selection:**  Disable  Enable
- DCS Scan Interval:** 8 Hours
- BG Protection Mode:** Manual
- IGMP Snooping:**  Disable  Enable
- Operation Mode:**  Mixed Mode  Green Field
- Guard Interval:**  400ns  800ns  Auto
- Extension Channel:** Auto
- Aggregation MSDU(A-MSDU):**  Disable  Enable
- Auto Block Ack:**  Disable  Enable
- Decline BA Request:**  Disable  Enable
- WMM Power Save:** 

This item depends on WMM. Enable WMM in at least one SSID to make this work.
- STBC:**  Disable  Enable

A "SAVE SETTINGS" button is located at the bottom of the configuration area. The footer of the page contains the text "ARRIS • Customer Support • Open Source".

- **Wireless Radio:** Enables or disables the 2.4 GHz radio.
- **Mode:** Select one of:
  - 802.11 n
  - 802.11 g/n
  - 802.11 b/g/n
- **Tx Power:** Select the transmit power, as a percentage of maximum power.

- **Channel Selection:** Select **Manual** only if instructed by your service provider.
- **Channel:** When **Channel Selection** is Manual, select a channel from the drop-down.
- **Channel Bandwidth:** Select one of **20**, **20/40**, or **Auto** (recommended).
- **Dynamic Channel Selection:** Select **Enable** to allow the Gateway to change Wi-Fi channels based on current noise and interference levels.
- **DCS Scan Interval:** When Dynamic Channel Selection is enabled, select the time between DCS scans.
- **BG Protection Mode:** Sets the BG protection mode. Options are Manual (default) or Auto.

BG protection allows you to operate 802.11b client devices in 802.11g networks. Set to Auto (checked) to allow 802.11b client devices to operate in the 802.11g wireless network. This impacts the performance of the 802.11g client devices on the network. If your network consists only of 802.11g client devices, set this to Manual for maximum performance.

802.11b devices require the Gateway to add overhead to most transmissions. Performance improves if no 802.11b devices are present and this feature is disabled (Manual). The Gateway auto-detects 802.11b devices and sets the feature accordingly when the BG protection is enabled (Auto).
- **IGMP Snooping:** Set to **Enable** to enable IGMP Snooping.
- **Operation Mode:** Sets the 802.11n Operation Mode. Options are Mixed Mode or Greenfield. The default, Mixed Mode, is for networks with a mix of 802.11a/b/g/n client devices. The optional Greenfield mode improves efficiency of networks using only 802.11n devices by eliminating support for the 802.11a/b/g client devices.
- **Guard Interval:** The spacing between transmission of symbols, in nanoseconds. Can be set to AUTO, 400ns or 800ns. The default is AUTO. Selecting 400ns provides higher throughput in networks where the coverage distance is small (indoors). Selecting 800ns provides higher throughput in networks where the coverage distance is large (outdoors).
- **Extension Channel:** When **Channel Bandwidth** is set to 20/40, sets the second channel to use (or **Auto** to pick the best channel).
- **Aggregation MSDU (A-MSDU):** Enables aggregation of MAC Service Data Units (MSDUs, or data frames) destined for the same device. This provides higher throughput in networks with a high signal-to-noise ratio (SNR). If a network has significant noise or interference, disabling A-MSDU provides the best throughput.
- **Auto Block Ack:** Enables Block Acknowledgement, where the Gateway sends a single acknowledgement for multiple frames. This provides higher throughput in networks with a high SNR.
- **Decline BA Request:** Set to Enable to effectively disable Block Acknowledgement.
- **WMM Power Save Mode:** Click this checkbox to enable WMM Power Save Mode. WMM Power Save delivery is a more efficient power management method than legacy 802.11 power save polling.
- **STBC:** Controls Space-Time Block Coding, a technique that transmits multiple copies of the same data from multiple antennas. This improves transmission reliability in a network where signal scattering and reflection exist.

Click **Save Settings** to put your configuration changes into effect.



## Gateway &gt; Connection &gt; Wi-Fi &gt; 5 GHz Radio

Use this page to configure the 5 GHz radio.

The screenshot shows the ARRIS web interface for configuring the 5 GHz Wi-Fi radio. The page title is "Gateway > Connection > Wi-Fi > 5 GHz Radio". The left sidebar shows navigation options like Gateway, Connection, and Wi-Fi. The main content area is titled "5 GHz Wi-Fi Radio Configuration" and contains various settings such as Wireless Radio (Enable/Disable), Mode (802.11 a/n/ac), Tx Power (100%), DFS (Disable/Enable), Channel Selection (Manual/Automatic), Channel (36), Channel Bandwidth (20/20/40/20/40/80/Auto), Dynamic Channel Selection (Disable/Enable), DCS Scan Interval (8 Hours), IGMP Snooping (Disable/Enable), Operation Mode (Mixed Mode/Green Field), Guard Interval (400ns/800ns/Auto), Aggregation MSDU(A-MSDU) (Disable/Enable), Auto Block Ack (Disable/Enable), Decline BA Request (Disable/Enable), WMM Power Save (checked), and STBC (Disable/Enable). A "SAVE SETTINGS" button is at the bottom.

- **Wireless Radio:** Enables or disables the 2.4 GHz radio.
- **Mode:** Select one of:
  - 802.11 n
  - 802.11 ac
  - 802.11 n/ac
  - 802.11 a/n/ac
- **Tx Power:** Select the transmit power, as a percentage of maximum power.
- **DFS:** Enables or disables selection of 5 GHz DFS channels. These channels may be shared with local radar installations, and may not be supported in all locations.
- **Channel Selection:** Select **Manual** only if instructed by your service provider.

- **Channel:** When **Channel Selection** is Manual, select a channel from the drop-down.
- **Channel Bandwidth:** Select one of **20**, **20/40**, **20/40/80**, or **Auto** (default). The Gateway bonds multiple channels together to create 40 or 80 MHz channels.
- **Dynamic Channel Selection:** Select **Enable** to allow the Gateway to change Wi-Fi channels based on current noise and interference levels.
- **DCS Scan Interval:** When Dynamic Channel Selection is enabled, select the time between DCS scans.
- **IGMP Snooping:** Set to **Enable** to enable IGMP Snooping.
- **Operation Mode:** Only **Mixed Mode** is supported.
- **Guard Interval:** The spacing between transmission of symbols, in nanoseconds. Can be set to AUTO, 400ns or 800ns. The default is AUTO. Selecting 400ns provides higher throughput in networks where the coverage distance is small (indoors). Selecting 800ns provides higher throughput in networks where the coverage distance is large (outdoors).
- **Aggregation MSDU (A-MSDU):** Enables aggregation of MAC Service Data Units (MSDUs, or data frames) destined for the same device. This provides higher throughput in networks with a high signal-to-noise ratio (SNR). If a network has significant noise or interference, disabling A-MSDU provides the best throughput.
- **Auto Block Ack:** Enables Block Acknowledgement, where the Gateway sends a single acknowledgement for multiple frames. This provides higher throughput in networks with a high SNR.
- **Decline BA Request:** Set to Enable to effectively disable Block Acknowledgement.
- **WMM Power Save Mode:** Click this checkbox to enable WMM Power Save Mode. WMM Power Save delivery is a more efficient power management method than legacy 802.11 power save polling.
- **STBC:** Controls Space-Time Block Coding, a technique that transmits multiple copies of the same data from multiple antennas. This improves transmission reliability in a network where signal scattering and reflection exist.

Click **Save Settings** to put your configuration changes into effect.

## Gateway > Connection > Wi-Fi > MAC Filtering

Use this page to manage which clients can connect to your networks.

The screenshot displays the ARRIS WebGUI interface for configuring MAC Filtering. The top navigation bar shows the user is logged in as 'Hi, mso' with a 'Logout' link and a language dropdown set to 'English'. Status indicators for Internet, Ethernet, Wi-Fi, and Low Security are visible. The left sidebar contains a menu with 'Gateway' expanded, showing options like Summary, Email Notification, Connection, WAN, Local IP Network, Wi-Fi (selected), Networks, 2.4 GHz Radio, 5 GHz Radio, MAC Filtering (selected), WPS, GRE, MTA, CallP/QoS, VQM, Firewall, Software, Hardware, Time, Connected Devices, Parental Control, Advanced, Wi-Fi MESH, and Troubleshooting. The main content area is titled 'Gateway > Connection > Wi-Fi > MAC Filtering' and includes a 'more' link. The 'MAC Filter Settings' section shows the SSID set to 'ARRIS-F21D' and the MAC Filtering Mode set to 'Allow-All'. Below this are three sections: 'Wi-Fi Control List (up to 16 items)', 'Auto-Learned Wi-Fi Devices', and 'Manually-Added Wi-Fi Devices'. Each section has a table with columns for '#', 'Device Name', and 'MAC Address'. The 'Manually-Added' section includes input fields for these fields and an 'ADD' button. A 'SAVE FILTER SETTINGS' button is located at the bottom of the main content area. The footer of the page reads 'ARRIS • Customer Support • Open Source'.

- **SSID:** Select the SSID that you want to manage.
- **MAC Filtering Mode:** Select one of:
  - **Allow-All:** Allow any device to connect to this SSID, effectively disabling filtering.
  - **Allow:** Allow listed devices to connect to this SSID.
  - **Deny:** Block listed devices from connecting to this SSID.
- **Wi-Fi Control List:** Displays the managed clients for this SSID.
- **Auto-Learned Wi-Fi Devices:** Displays devices that have previously connected to this SSID.
- **Manually-Added Wi-Fi Devices:** Enter a device name and MAC address, and click **Add**. Click **Save Filter Settings** to put your changes in effect.

## Gateway > Connection > Wi-Fi > Add Wireless Client

Use this page to control Wi-Fi Protected Setup (WPS), and to manually connect devices to the Gateway using WPS.

The screenshot displays the ARRIS Gateway WebGUI interface for configuring Wi-Fi Protected Setup (WPS). The top navigation bar shows the user is logged in as 'mso' and the language is set to 'English'. The status bar indicates that Internet, Ethernet, and Wi-Fi are active, while Low Security is disabled. The left sidebar contains a navigation menu with categories like Gateway, Connection, and Wi-Fi. The main content area is titled 'Gateway > Connection > Wi-Fi > Add Wireless Client'. It features a blue header for 'Add Wi-Fi Client (WPS)'. Below this, there are toggle buttons for 'WPS Protected Setup (WPS)' (currently 'Enable') and 'WPS PIN Method' (currently 'Disable'). The 'AP PIN' is displayed as 31914161. Two connection methods are available: 'Push Button (recommended)' and 'PIN Method'. The 'Push Button' method is selected, and instructions indicate to click the 'PAIR' button to begin pairing. The 'PIN Method' section is currently disabled. At the bottom of the page, there is a footer with 'ARRIS • Customer Support • Open Source'.

- **Wi-Fi Protected Setup (WPS):** Enables or disables WPS on this Gateway.
- **AP PIN:** For devices that support the PIN connection method.
- **WPS PIN Method:** Enables or disables the PIN connection method.
- **Push Button:** Selects the Push Button connection method. Click **PAIR** to start pairing with a client.
- **PIN Method:** If the PIN is enabled, selects the PIN connection method. Enter the client's PIN in the text box, and the Gateway's PIN in the client's text box.

## Gateway &gt; Connection &gt; Wi-Fi &gt; GRE

Use this page to manage GRE (Hotspot or Public network) connections.

ARRIS

Hi, mso • [Logout](#) English

Internet Ethernet Wi-Fi Low Security

Gateway > Connection > Wi-Fi > GRE

Manage your GRE configuration. [more](#)

**GRE Configuration**

DSCP:

Primary IP (IPv4/IPv6):

Secondary IP (IPv4/IPv6):

Ping Count:

Ping Interval:  sec

Failover Threshold:  pings

Failure Ping Interval:  min

Retry Interval:  hrs

Circuit ID:

Remote ID:

ARRIS • Customer Support • Open Source

- **DSCP:** The value of the Differentiated Services Field Codepoint (DSCP) to be assigned to GRE packets.
- **Primary IP (IPv4/IPv6):** The IP address of the primary GRE server.
- **Secondary IP (IPv4/IPv6):** The IP address of the secondary GRE server.
- **Ping Count:** The number of pings to send to test the server connection.
- **Ping Interval:** The time, in seconds, between sending pings.
- **Failover Threshold:** The number of failed pings allowed before the Gateway switches to the secondary GRE server.
- **Failure Ping Interval:** The time, in minutes, that the number of failed pings trigger a failover.

- **Retry Interval:** The time, in hours, after which the Gateway retries the primary server after a failover.
- **Circuit ID:** Enables or disables Circuit ID on this Gateway.
- **Remote ID:** Enables or disabled Remote ID on this Gateway.

Click **Save Settings** to put your changes in effect.

## Gateway > Connection > MoCA

MoCA is available on some Gateways. If you have no other MoCA devices, you can disable MoCA on the Gateway.

- **MoCA:** Click Enable to enable MoCA.
- **Channel Selection:** Unless you have specific requirements, accept the default of Scan.
- **Channel:** When Channel Selection is Manual, select the channel used for MoCA communications.
- **Beacon Power Reduction(dB):** Choose an attenuation factor from the drop-down menu. The default, 0, is usually acceptable.
- **Taboo Frequency:** Check boxes to indicate frequencies that the MoCA network should not use. This is usually unnecessary, except in the newest cable plants where DOCSIS 3.1 channels can overlap with MoCA channels.
- **Preferred Network Controller:** Leave set to Enabled unless you have another MoCA device you want to use to control your home network.

- **MoCA Privacy:** When enabled, other MoCA devices required a password to join the network. This can be useful in high-density dwellings.
- **Network Password:** A 12- to 17-digit number, used when MoCA Privacy is enabled.
- **Show Network Password:** Check this box to show the network password.
- **Network Controller MAC:** The MAC address of the MoCA network controller (usually the Gateway's MoCA interface MAC address).

After making changes, click **Save**.

## Gateway > Connection > MTA

Use these pages to manage and test telephone connections in Telephony Gateways.

- **ID: mta** (hiding this ID hides the entire MTA sub-menu)

## Gateway > Connection > MTA > Line Status

Displays information about the telephone interface and phone lines.

The screenshot shows the ARRIS web GUI interface. At the top, there is a navigation bar with the ARRIS logo, user information (Hi, mso), a Logout button, and a language dropdown menu set to English. Below the navigation bar, there are status indicators for Internet, Ethernet, Wi-Fi, and Low Security. The main content area is titled 'Gateway > Connection > MTA > Line Status'. On the left side, there is a sidebar menu with various options, including Gateway, Connection, MTA, and Line Status. The main content area displays the following information:

- Information related to the MTA Line Status.**
- MTA Initialization Procedure**
  - DHCP: Complete
  - TFTP: Complete
  - Registration: In Progress
- MTA Line Status**
  - Line 1 Status: On-Hook
  - Line 2 Status: On-Hook

At the bottom of the page, there is a footer with the text 'ARRIS • Customer Support • Open Source'.

## Gateway &gt; Connection &gt; MTA &gt; Line Diagnostics

Displays information about the telephone interface and phone lines.

The screenshot displays the ARRIS web GUI interface for the 'Line Diagnostics' page. The top navigation bar shows the user is logged in as 'Hi, mso' with a 'Logout' link and a language dropdown set to 'English'. System status indicators show 'Internet', 'Ethernet', and 'Wi-Fi' are active, while 'Low Security' is disabled. The left sidebar contains a menu with categories like Gateway, Connection, MTA, and Connected Devices. The main content area is titled 'Gateway > Connection > MTA > Line Diagnostics' and contains two diagnostic sections: 'MTA Line 1 Diagnostics' and 'MTA Line 2 Diagnostics'. Each section lists five diagnostic tests: 'Hazardous Potential', 'Foreign EMF', 'Resistive Faults', 'Receiver Off Hook', and 'Ringer Equivalency', all of which are currently in a 'Not Started' state. A 'START DIAGNOSTICS' button is located at the bottom of each diagnostic section. The footer of the page includes the text 'ARRIS • Customer Support • Open Source'.

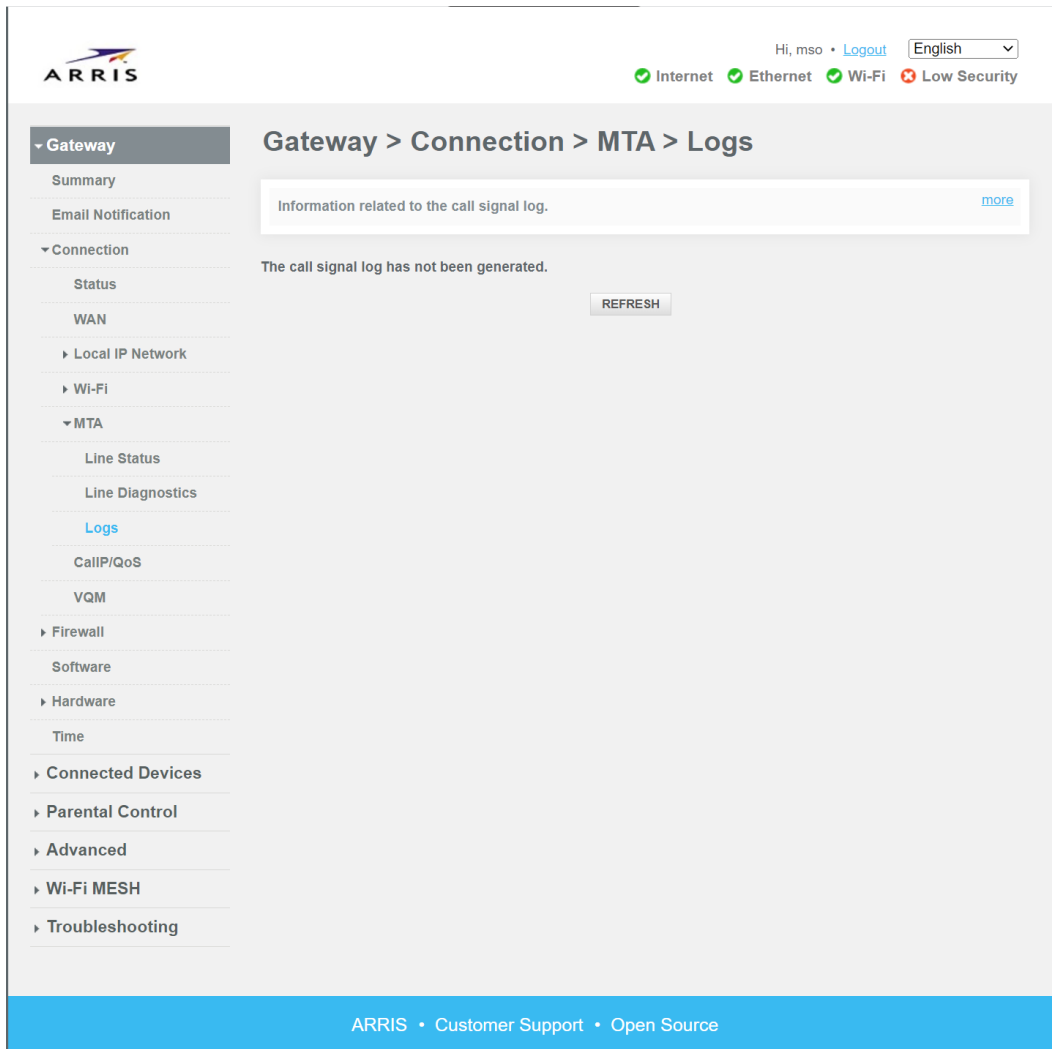
To run a test, make sure the phone is on-hook (hung up) and click **Start Diagnostics**. The tests take several seconds to run.



- **Hazardous Potential:** Tests for high levels of foreign voltage between the phone lines (tip, ring) and ground. This test failing indicates issues with inside wiring. Connected phones may not operate.
- **Foreign EMF:** Tests for low levels of foreign voltage between the phone lines and ground. This test failing indicates issues with inside wiring. Connected phones may not operate.
- **Resistive Faults:** Tests for proper isolation between tip, ring, and ground. This test failing indicates inside wiring issues such as staples or nails shorting tip and ring, or moisture in the lines. Connected phones may not operate, or may have noise on the line.
- **Receiver Off Hook:** Tests for all phones hung up. This test failing means one or more phones are not hung up, or a phone is malfunctioning.
- **Ringer Equivalency:** Tests ringer impedance on connected phones. Passing scores are between 0.175 and 5.0 REN (Ringer Equivalence Number; 1 REN is the impedance of a mechanical ringer). This test failing may mean no phone is connected (or the line is broken), too many phones are connected, or a connected phone is malfunctioning. Some phones with electronic ringers may have REN less than 0.175, and can function even if this test fails.

## Gateway > Connection > MTA > Logs

Displays the call signaling log. Your service provider may use this information to troubleshoot telephony issues.



The screenshot shows the ARRIS web interface. At the top left is the ARRIS logo. At the top right, it says "Hi, mso" with a "Logout" link and a language dropdown set to "English". Below this are status indicators for "Internet", "Ethernet", "Wi-Fi" (all green), and "Low Security" (red). The left sidebar has a "Gateway" section expanded, with "Logs" selected under the "MTA" section. The main content area is titled "Gateway > Connection > MTA > Logs". It contains a message box: "Information related to the call signal log." with a "more" link. Below this, it says "The call signal log has not been generated." and a "REFRESH" button. At the bottom of the page, there is a blue footer with the text "ARRIS • Customer Support • Open Source".

Click **Refresh** to update the display with the latest logs.

## Gateway > Connection > CallP/QoS

Displays the configuration of phone lines and Quality of Service (QoS) statistics.

The screenshot shows the ARRIS web interface for 'Gateway > Connection > CallP/QoS'. At the top right, there is a user profile 'Hi, mso' with a 'Logout' link and a language dropdown set to 'English'. Below this, there are status indicators for 'Internet', 'Ethernet', 'Wi-Fi', and 'Low Security'. The left sidebar contains a navigation menu with 'Gateway' selected, and sub-items like 'Summary', 'Email Notification', 'Connection', 'Status', 'WAN', 'Local IP Network', 'Wi-Fi', 'MTA', 'CallP/QoS', 'VQM', 'Firewall', 'Software', 'Hardware', 'Time', 'Connected Devices', 'Parental Control', 'Advanced', 'Wi-Fi MESH', and 'Troubleshooting'. The main content area has a heading 'Gateway > Connection > CallP/QoS' and a sub-heading 'This Page shows CallP/QoS statistics of your Gateway.' with a 'more' link. Below this is a 'CALLP' table with columns 'Line', 'LC State', 'CallP State', and 'Loop Current'. The table shows two lines, both in 'Idle' state with 'Boosted' loop current. Below the table are buttons for 'SHOW CALL SIGNALLING LOG', 'DISABLE LOGGING', and 'CLEAR'. Underneath is a 'QoS' table with columns 'SFID', 'Service Class Name', 'Direction', 'Primary Flow', 'Traffic Type', and 'Packets'. The table lists four service flows with their respective statistics. Below the table are buttons for 'SHOW DSX LOG', 'DISABLE LOGGING', and 'CLEAR'. At the bottom of the page, there is a footer with 'ARRIS • Customer Support • Open Source'.

Line	LC State	CallP State	Loop Current
1	Idle	Idle	Boosted
2	Idle	Idle	Boosted

SFID	Service Class Name	Direction	Primary Flow	Traffic Type	Packets
308093		upstream	false	----	29309
308095		upstream	false	----	1024
308094		downstream	false	----	0
308096		downstream	false	----	0

- **CALLP:** Displays the status of the phone lines on Telephony Gateways. These buttons control the signalling log:
  - **Show Call Signalling Log:** Displays the signalling log. Your service provider may use this to troubleshoot telephony issues.
  - **Disable Logging:** Disables the call signalling log.
  - **Clear:** Clears the call signalling log.
- **QoS:** Shows configured Service Flows and statistics. These buttons control the DSx (Dynamic Services) log:
  - **Show DSx Log:** Displays the DSx log. Your service provider may use this to troubleshooting telephony or data issues.
  - **Disable Logging:** Disables the DSx log.
  - **Clear:** Clears the DSx log.

## Gateway > Connection > Voice Quality Metrics

Displays voice quality metrics for recent calls.

The screenshot shows the ARRIS web interface for the 'Voice Quality Metrics' page. The top navigation bar includes the ARRIS logo, user information ('Hi, mso'), a 'Logout' link, and a language dropdown set to 'English'. Below the navigation bar, there are status indicators for Internet, Ethernet, Wi-Fi, and Low Security. The left sidebar contains a menu with 'Gateway' expanded, showing options like Summary, Email Notification, Connection, Status, WAN, Local IP Network, Wi-Fi, MTA, CallIP/QoS, VQM (highlighted), Firewall, Software, Hardware, Time, Connected Devices, Parental Control, Advanced, Wi-Fi MESH, and Troubleshooting. The main content area displays the page title and a message: 'This page displays the voice quality metrics of your Telephone lines.' Below this is a form with three dropdown menus: 'Line Number' (set to 1), 'Call Number' (set to Table), and 'Action' (set to Display Stats), followed by a 'Submit' button. A message below the form states: 'There is no data to display for Line 1'. The footer of the page contains the text 'ARRIS • Customer Support • Open Source'.

- **Line Number:** Select the phone line (1 or 2) whose metrics you want to display.
- **Call Number:** Select **Table** to display all VQM statistics for the selected line in tabular format, **All** to display all VQM statistics as a list, or select the call number (1 is most recent).
- **Action:** Select **Display Stats** to show the statistics, **Clear Line Stats** to clear statistics for the selected line, or **Clear All Stats** to clear statistics for all lines.
- **Submit:** Click to start the specified action.

## Gateway > Firewall

Your Gateway has a built-in firewall that protects your client devices from direct access by hackers or hacking tools. In addition, the firewall can control device access and restrict access to certain websites.

## Gateway > Firewall > IPv4

Use this page to manage firewall settings.

The screenshot shows the ARRIS web interface for managing Firewall IPv4 settings. The top right corner displays the user 'Hi, mso', a 'Logout' link, and a language dropdown set to 'English'. Below this, there are status indicators for Internet, Ethernet, Wi-Fi, and Low Security. The left sidebar contains a navigation menu with 'Gateway' selected, and sub-items like Summary, Email Notification, Connection, Firewall (with IPv4 selected), IPv6, Software, Hardware, Time, Connected Devices, Parental Control, Advanced, Wi-Fi MESH, and Troubleshooting. The main content area is titled 'Gateway > Firewall > IPv4' and includes a 'Manage your firewall settings' link. The 'Firewall Security Level' section has four radio button options: 'Maximum Security (High)', 'Typical Security (Medium)', 'Minimum Security (Low)', and 'Custom Security'. A CAPTCHA challenge is shown below the options, and there are 'SAVE SETTINGS' and 'RESTORE DEFAULT SETTING' buttons at the bottom. The footer contains 'ARRIS • Customer Support • Open Source'.

Select one of the following:

- **Maximum Security (High):** Blocks all incoming requests that are not part of a locally-initiated session.
- **Typical Security (Medium):** Blocks P2P applications (for example, Torrent) and ICMP (Ping) to the Gateway, but allows all other traffic.
- **Minimum Security (Low):** No application or traffic is blocked. This is the default setting.
- **Custom Security:** Choose the types of incoming WAN traffic to block:
  - **Block http (TCP port 80, 443):** blocks locally-managed web servers from public access.
  - **Block ICMP:** blocks Pings to the Gateway.
  - **Block Multicast:** blocks multicast sessions from initiating requests.
  - **Block Peer-to-peer applications:** blocks Torrent and similar applications.
  - **Block IDENT (port 113):** blocks IDENT requests. Disable this if you notice long delays in connecting to certain services.
  - **Disable entire firewall:** not recommended unless you understand the risks.

## Gateway > Firewall > IPv6

Use this page to manage firewall settings.

Select one of the following:

- **Typical Security (Default):** Blocks all incoming requests that are not part of a locally-initiated session.
- **Custom Security:** Choose the types of incoming WAN traffic to block:
  - **Block http (TCP port 80, 443):** blocks locally-managed web servers from public access.
  - **Block ICMP:** blocks Pings to the Gateway.
  - **Block Multicast:** blocks multicast sessions from initiating requests.
  - **Block Peer-to-peer applications:** blocks Torrent and similar applications.
  - **Block IDENT (port 113):** blocks IDENT requests. Disable this if you notice long delays in connecting to certain services.
  - **Disable entire firewall:** not recommended unless you understand the risks.

# Gateway > Software

This page displays details about the Gateway firmware. This may be useful for troubleshooting.

The screenshot shows the ARRIS Gateway web interface. At the top left is the ARRIS logo. At the top right, it displays the user 'Hi, mso', a 'Logout' link, and a language dropdown set to 'English'. Below this, there are status indicators for 'Internet', 'Ethernet', 'Wi-Fi' (all with green checkmarks), and 'Low Security' (with a red X). A left sidebar contains a navigation menu with items: Gateway (expanded), Summary, Email Notification, Connection, Firewall, Software (highlighted in blue), Hardware, Time, Connected Devices, Parental Control, Advanced, Wi-Fi MESH, and Troubleshooting. The main content area is titled 'Gateway > Software' and contains a summary box with the text 'View details about the Gateway's software.' and a 'more' link. Below this is a 'System Software Version' section with the following details:

Software Image Name:	AR01.04.086.03_052222_7247.NCS.10.X1
Firmware Version:	01.04.086.03.NCS
Packet Cable:	2.0
RDK-B-LLC:	rdkb-20200207
SDK:	N/A
Wi-Fi Driver:	4.7.23.63.1.0

At the bottom of the page, there is a blue footer bar with the text 'ARRIS • Customer Support • Open Source'.

## Gateway > Hardware

These pages display information about the Gateway hardware components.

### Gateway > Hardware > System Hardware

Displays information about the Gateway system hardware.

The screenshot displays the ARRIS Gateway System Hardware page. The page includes a navigation menu on the left with options like Gateway, Summary, Email Notification, Connection, Firewall, Software, Hardware (with sub-options for System Hardware, Ethernet, and Wireless), Time, Connected Devices, Parental Control, Advanced, Wi-Fi MESH, and Troubleshooting. The main content area shows the title 'Gateway > Hardware > System Hardware' and a summary of hardware information. A 'more' link is available for further details. The footer contains the text 'ARRIS • Customer Support • Open Source'.

System Hardware	
Model:	TG3442A
Vendor:	ARRIS Group, Inc.
Hardware Revision:	1
Serial Number:	A3A4DG111102005
Processor Speed:	3999.70 MHz
DRAM Total Memory:	540672 MB
DRAM Used Memory:	413 MB
DRAM Available Memory:	117760 MB
Flash Total Memory:	462 MB
Flash Used Memory:	424 MB
Flash Available Memory:	38 MB



## Gateway > Hardware > Ethernet

Use this page to display and control Ethernet port configuration. Click **Save** after making changes.

The screenshot displays the 'Gateway > Hardware > Ethernet' configuration page. The left sidebar contains a navigation menu with options like Gateway, Summary, Email Notification, Connection, Firewall, Software, Hardware, System Hardware, Ethernet, Wireless, Time, Connected Devices, Parental Control, Advanced, Wi-Fi MESH, and Troubleshooting. The main content area shows four LAN Ethernet ports, each with a set of configuration options. The 'Port' toggle is set to 'Enable', 'Link Status' is 'Inactive', 'MAC Address' is '9c:c8:fc:52:33:c1', 'Energy Efficient Ethernet' is 'Enable', 'Auto Configuration' is checked, 'Connection Speed' is '0 Mbps', 'Duplex Mode' is 'Full', and 'Bridging' is 'Disable'. A 'Save' button is located below each port's configuration panel. The top of the page shows the user 'Hi, mso', a 'Logout' link, and a language dropdown set to 'English'. There are also status indicators for Internet, Ethernet, Wi-Fi, and Low Security. The footer contains the text 'ARRIS • Customer Support • Open Source'.

- **Port:** Click **Enable** to enable the Ethernet port.
- **Link Status:** The current link-level status of the port. The status is Inactive if no device is connected, or a connected device is powered off.
- **MAC Address:** The MAC address of the Ethernet port.
- **Energy Efficient Ethernet:** Click **Enable** to reduce power consumption during periods of low data activity.

- **Auto Configuration:** Check to allow the Gateway and device to negotiate the most compatible connection speed. When unchecked, the following two fields are available:
  - **Connection Speed:** Set the Ethernet connection speed: 10, 100, or 1000 Mbps.
  - **Duplex Mode:** Set to Full unless connected devices are only capable of half-duplex operation.
- **Bridging:** Controls bridging on this Ethernet port.

## Gateway > Hardware > Wireless

Displays information about the Gateway's wireless hardware.

To configure wireless networks, use the pages under *Gateway Setup* (page 24).

The screenshot shows the ARRIS Gateway WebGUI interface. At the top, there is a navigation bar with the ARRIS logo, user information (Hi, mso), a Logout link, and a language dropdown (English). Below the navigation bar, there are status indicators for Internet, Ethernet, Wi-Fi, and Low Security. The main content area is titled 'Gateway > Hardware > Wireless' and contains a summary box with a 'more' link. Below this, there are two panels for 'Wi-Fi LAN port (2.4 GHZ)' and 'Wi-Fi LAN port (5 GHZ)'. Each panel displays the following information:

Wi-Fi LAN port (2.4 GHZ)	Wi-Fi LAN port (5 GHZ)
Link Status: Active	Link Status: Active
Link Uptime: 0d 20h 48m 44s	Link Uptime: 0d 20h 49m 5s
Radio Status: Active	Radio Status: Active
MAC Address: 9C:C8:FC:52:33:BF	MAC Address: 9C:C8:FC:52:33:C0

At the bottom of the page, there is a footer with the text 'ARRIS • Customer Support • Open Source'.

# Gateway > Time

Use this page to configure Time (NTP) services.

The screenshot displays the ARRIS Gateway Time configuration interface. At the top, there's a user greeting 'Hi, mso' with a 'Logout' link and a language dropdown set to 'English'. Below this, connection status indicators show 'Internet', 'Ethernet', and 'Wi-Fi' as active (green checkmarks), and 'Low Security' as disabled (red X). The left sidebar lists various configuration categories, with 'Time' highlighted. The main content area is titled 'Gateway > Time' and includes a 'Manage your time settings.' link. The 'Router Time' section shows the current time as '06/08/2022 12:52:02'. The 'Time Server' section features an 'Enable Time Server' toggle with 'Enable' and 'Disable' buttons, and three input fields for Time Server URLs. The 'Time Zone' section has a 'Time Zone Selection' radio button set to 'Automatic', and dropdown menus for 'Time Format' (set to '24 hour format') and 'Date Format' (set to 'MM/DD/YYYY'). A 'SAVE TIME SETTINGS' button is located at the bottom of the configuration area.

- **Enable Time Server:** Click **Enable** to use a network time server.
- **Time Server:** Enter up to three URLs or IP addresses to Time (NTP) servers.
- **Time Zone Selection:** Select **Automatic** to automatically determine your time zone. Select **Manual** if the result is incorrect.
- **Time Format:** Choose **12 hour format** or **24 hour format**.
- **Date Format:** Choose **MM/DD/YYYY** (US style), **DD/MM/YYYY** (European style), or **YYYY/MM/DD**.

Click **Save Time Settings** to save any changes.

# Connected Devices

These pages list devices that have automatically or manually connected to your Gateway.

## Connected Devices > Devices

This page shows devices connected to your network, as well as connection history.

The screenshot shows the ARRIS web interface. At the top left is the ARRIS logo. At the top right, it says "Hi, mso" with a "Logout" link and a language dropdown set to "English". Below this are status indicators: "Internet" (green check), "Ethernet" (green check), "Wi-Fi" (green check), and "Low Security" (red X). The main navigation sidebar on the left includes: Gateway, Connected Devices (selected), Static Addresses, Parental Control, Advanced, Wi-Fi MESH, and Troubleshooting. The main content area is titled "Connected Devices > Devices" and contains a text box: "View information about the devices currently connected to your network." Below this is a "Prefer Private Connection" checkbox. A table titled "Online Devices" has columns for Host Name, IPv4 Address, RSSI, Speed, and Connection. The table is currently empty with the text "There are no devices to display." Below the table is a button labeled "ADD WI-FI PROTECTED SETUP (WPS) CLIENT". At the bottom of the page, there is a blue footer bar with the text "ARRIS • Customer Support • Open Source".

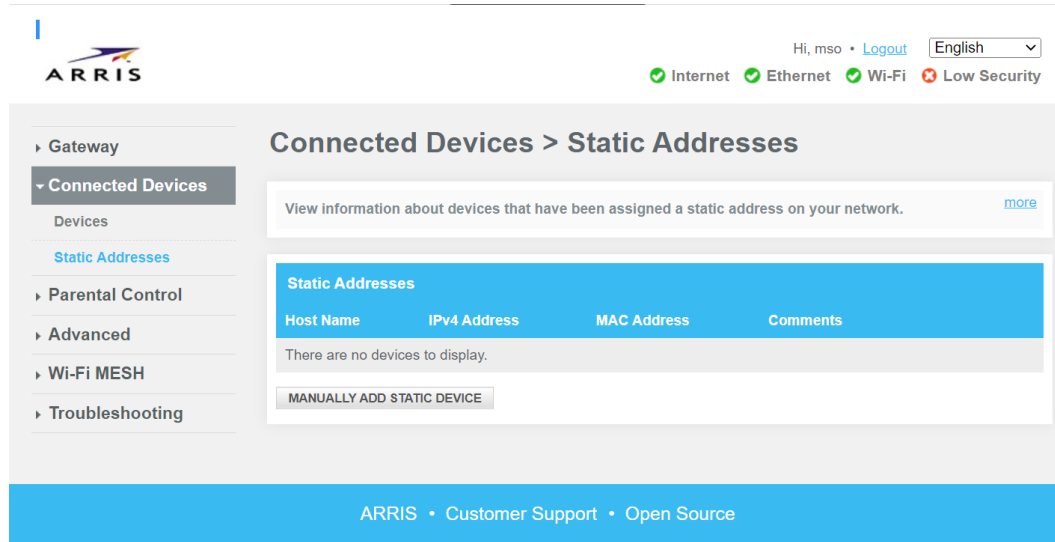
- To add a WPS client, click **Add Wi-Fi Protected Setup (WPS) Client**, then make changes as needed.

The screenshot shows the ARRIS WebGUI interface for configuring a wireless client. The top navigation bar includes the ARRIS logo, user information (Hi, mso), a Logout button, and a language dropdown set to English. A status bar below the navigation bar shows indicators for Internet, Ethernet, Wi-Fi, and Low Security. The main content area is titled 'Gateway > Connection > Wi-Fi > Add Wireless Client'. On the left, a navigation menu lists various settings categories, with 'Wi-Fi' and 'WPS' highlighted. The main content area contains a blue header 'Add Wi-Fi Client (WPS)' and a section for 'Wi-Fi Protected Setup (WPS)'. This section includes a 'Wi-Fi Protected Setup (WPS)' toggle set to 'Enable', an 'AP PIN' of 31914161, and a 'WPS PIN Method' toggle set to 'Disable'. Below this, there are two radio button options: 'Push Button (recommended)' and 'PIN Method'. The 'Push Button' option is selected. Under 'PIN Method', there is a text input field for 'Enter Wireless Client's PIN' and a 'PAIR' button. A footer at the bottom of the page contains the text 'ARRIS • Customer Support • Open Source'.

- **Wi-Fi Protected Setup (WPS):** Click **Enable** to enable WPS.
- **WPS Pin Method:** Click **Enable** to allow using a PIN to connect a device using WPS.
- **Connection Options:** Select **Push Button** (preferred) or **PIN Method**.
- To connect a WPS client using the Push Button method, click **Pair** or push the WPS button on the Gateway housing, then configure the client device to connecting using WPS.
- To connect a WPS client using the PIN method, enter the client PIN in the text box. On the client device, enter the number shown in **AP PIN** above.

# Connected Devices > Static Addresses

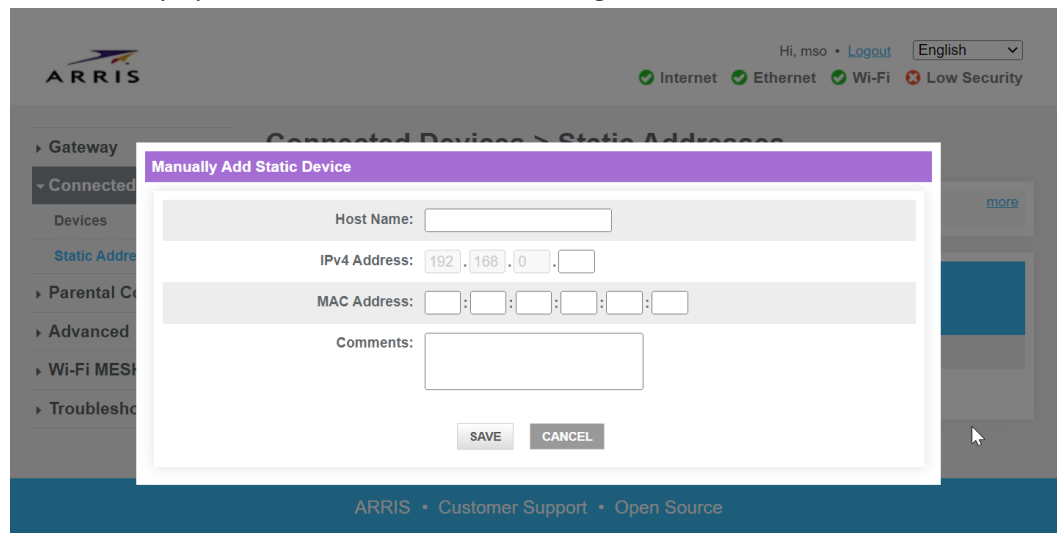
Use this page to view and add devices using a static address.



► **To assign a static address to a device:**

1. Click **Manually Add Static Device**.

The Gateway opens the Add Static Device dialog:



2. Add the following information:

- **Host Name:** (optional) The name of this device as it appears on the LAN.
- **IPv4 Address:** The suffix of the IP address you want to assign to the device (the prefix is filled out and cannot be changed). The upper range is a good choice, as it is less likely to clash with dynamically -assigned addresses.
- **MAC Address:** The MAC address of the device's interface. Use the WLAN interface MAC address for Wi-Fi connections, or the Ethernet MAC address for Ethernet connections.

- **Comments:** (optional) Any other information you want to add about this device; for example: `Upstairs printer`.

3. Click **Save**.

The device appears in the Static Addresses table.

# Parental Control

Use these pages to manage the sites and services that non-trusted devices can access.

## Parental Control > Managed Sites

Use this page to block sites by URL or keyword.

The screenshot displays the ARRIS web interface for the 'Parental Control > Managed Sites' page. The top navigation bar includes the ARRIS logo, user information 'Hi, mso', a 'Logout' link, and a language dropdown set to 'English'. Below the navigation bar, there are status indicators for 'Internet', 'Ethernet', 'Wi-Fi', and 'Low Security'. The main content area features a sidebar on the left with a 'Parental Control' menu. The main panel has a title 'Parental Control > Managed Sites' and a subtitle 'Manage access to specific websites by network devices.' with a 'more' link. Below the subtitle, there is a 'Managed Sites' section with 'Enable' and 'Disable' buttons. The 'Blocked Sites' section contains a table with columns 'URL' and 'When', and an '+ADD' button. The 'Blocked Keywords' section contains a table with columns 'Keyword' and 'When', and an '+ADD' button. The 'Auto-Learned Devices' section contains a table with columns 'Device Name', 'MAC Address', and 'Trusted'. The footer of the page reads 'ARRIS • Customer Support • Open Source'.

**Managed Sites:** click **Enable** to filter sites.

### Blocking sites by URL

**Blocked Sites:** lists blocked URLs. To add a new blocked site, click **+Add**. After adding the information, click **Save** to save your changes.



- **URL:** The site to block.
- **Always Block?:** Click **No** to schedule blocking by day of week and time of day.
- **Set Block Time:** Set the beginning and ending times of day to block the site.
- **Set Block Days:** Check the day of week during which you want the site blocked.

### Block sites by keyword

**Blocked keywords:** blocks sites by strings appearing in the URL (for example, **.xxx** blocks all sites whose URL contains **.xxx**). To add a keyword, click **+Add**. After adding the information, click **Save** to save your changes.

ARRIS

Hi, mso • Logout English

Internet Ethernet Wi-Fi Low Security

Parental Control > Managed Sites > Add Blocked Keyword

**Add Keyword to be Blocked**

Keyword:

Always Block?  No  Yes

**Set Blocked Time**

Start from:

End on:

**Set Blocked Days** [Select All](#) | [Select None](#)

Monday  
 Tuesday  
 Wednesday  
 Thursday  
 Friday  
 Saturday  
 Sunday

ARRIS • Customer Support • Open Source

- **Keyword:** The keyword to block.
- **Always Block?:** Click **No** to schedule blocking by day of week and time of day.
- **Set Block Time:** Set the beginning and ending times of day to block the site.
- **Set Block Days:** Check the day of week during which you want the site blocked.

### Auto-learned Devices

**Auto-learned Devices:** lists devices that are or have connected to the Gateway. A trusted computer is not affected by site or keyword blocking.

To make a device trusted, click **Yes** next to its entry.

# Parental Control > Managed Services

Use this page to block access to specific services.

The screenshot shows the ARRIS web interface for Parental Control > Managed Services. The top navigation bar includes the ARRIS logo, user information (Hi, mso), a Logout button, and a language dropdown (English). Status indicators for Internet, Ethernet, Wi-Fi, and Low Security are shown. The left sidebar contains navigation options: Gateway, Connected Devices, Parental Control (selected), Managed Sites, Managed Services (highlighted), Managed Devices, Reports, Advanced, Wi-Fi MESH, and Troubleshooting. The main content area is titled 'Parental Control > Managed Services' and includes a description: 'Manage network devices' access to specific services and applications.' Below this is a 'Managed Services' section with 'Enable' and 'Disable' buttons. The 'Blocked Services' section features a table with columns for Services, TCP/UDP, Start Port, End Port, and When, and a '+ADD' button. The 'Auto-Learned Devices' section features a table with columns for Device Name, MAC Address, and Trusted.

**Managed Services:** click **Enable** to enable managed services.

Block services by port or port range

The **Blocked Services** page lists services blocked by port or port range. Click **+Add** to block a service.

ARRIS

Hi, mso • Logout English

Internet Ethernet Wi-Fi Low Security

Parental Control > Managed Services > Add Blocked Service

**Add Service to be Blocked**

User Defined Service:

Protocol: TCP

Start Port:

End Port:

Always Block?

Set Blocked Time

Start from: 00 00

End on: 23 59

Set Blocked Days

Select All | Select None

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

ARRIS • Customer Support • Open Source

- **User Defined Service:** A brief description of the service you want to block.
  - **Protocol:** The protocols the service uses: **TCP**, **UDP**, or **Both**.
  - **Start Port:** The port to block, or the lowest port number in a range to block.
  - **End Port:** (optional) The highest port number in a range to block.
  - **Always Block?:** Click **No** to schedule blocking by day of week and time of day.
  - **Set Block Time:** Set the beginning and ending times of day to block the site.
  - **Set Block Days:** Check the day of week during which you want the site blocked.
- Click **Save** to add the blocked service.

## Parental Control > Managed Devices

This screen lists managed devices.

The screenshot displays the ARRIS web interface for the 'Parental Control > Managed Devices' section. At the top left is the ARRIS logo. The top right shows the user 'Hi, mso' with a 'Logout' link and a language dropdown set to 'English'. Below this, there are status indicators for 'Internet', 'Ethernet', 'Wi-Fi', and 'Low Security'. The left sidebar contains a navigation menu with items like 'Gateway', 'Connected Devices', 'Parental Control', 'Managed Sites', 'Managed Services', 'Managed Devices', 'Reports', 'Advanced', 'Wi-Fi MESH', and 'Troubleshooting'. The main content area is titled 'Parental Control > Managed Devices' and includes a sub-header 'Managed Devices'. Underneath, there are two rows of controls: 'Managed Devices' with 'Enable' and 'Disable' buttons, and 'Access Type' with 'Allow All' and 'Block All' buttons. Below these is a 'Blocked Devices' section with a '+ADD BLOCKED DEVICE' button and a table with columns for 'Device Name', 'MAC Address', and 'When Blocked'. The footer of the page reads 'ARRIS • Customer Support • Open Source'.

- **Managed Devices:** Click **Enable** to manage devices in the list.
- **Access Type:**
  - click **Allow All** to allow access to all devices except those in the list (blacklist).
  - click **Block All** to block access to all devices except those in the list (whitelist).
- **+Add Blocked Device:** Click to add a device to the block list.

ARRIS

Hi, mso • Logout English

Internet Ethernet Wi-Fi Low Security

Parental Control > Managed Devices > Add Blocked Device

Gateway

Connected Devices

Parental Control

Managed Sites

Managed Services

Managed Devices

Reports

Advanced

Wi-Fi MESH

Troubleshooting

Add Device to be Blocked

Set Blocked Device

Auto-Learned Devices:

Device Name	MAC Address

Custom Device:

Device Name	MAC Address
<input type="text"/>	<input type="text"/>

Always Block?

Set Blocked Time

Start from:

End on:

Set Blocked Days

Select All | Select None

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

ARRIS • Customer Support • Open Source

See How do I *block certain devices from accessing my Gateway?* (page 15) to add devices to the list.

# Parental Control > Reports

Generates reports about parental control activity.

The screenshot displays the ARRIS web interface for the 'Parental Control > Reports' section. At the top left is the ARRIS logo. The top right shows the user 'Hi, mso' with a 'Logout' link and a language dropdown set to 'English'. Below this are status indicators for 'Internet', 'Ethernet', 'Wi-Fi', and 'Low Security'. The left navigation menu includes 'Gateway', 'Connected Devices', 'Parental Control' (highlighted), 'Managed Sites', 'Managed Services', 'Managed Devices', 'Reports', 'Advanced', 'Wi-Fi MESH', and 'Troubleshooting'. The main content area is titled 'Parental Control > Reports' and contains a sub-header: 'Generate, download, and print reports based on your parental controls.' Below this is a 'Report Filters' section with two dropdown menus: 'Report Type' (set to 'All') and 'Time Frame' (set to 'Today'). A 'GENERATE REPORTS' button is located to the right of the dropdowns. The footer of the page contains the text 'ARRIS • Customer Support • Open Source'.

- **Report Type:** Select one of **All**, **Managed Sites**, **Managed Services**, or **Managed Devices**.
- **Time Frame:** Select one of **Today**, **Yesterday**, **Last Week**, **Last Month**, or **Last 90 days**.
- **Generate Reports:** Click to create reports based on the selected type and time frame. The All Reports pane contains the reports.
- **Print:** Click to send the reports to a printer.
- **Download:** Click to download the reports to a file on your computer.

# Advanced

Use these pages to display and configure advanced features. In most cases, the default settings are sufficient.

## Advanced > Port Forwarding

Port Forwarding allows devices outside the home network to access designated devices on the home network (for example, a personal web server).

The screenshot shows the ARRIS web interface. At the top right, there is a user greeting 'Hi, mso', a 'Logout' link, and a language dropdown set to 'English'. Below this, there are status indicators for 'Internet', 'Ethernet', 'Wi-Fi', and 'Low Security'. The main navigation menu on the left includes 'Gateway', 'Connected Devices', 'Parental Control', 'Advanced' (selected), 'Port Forwarding', 'Port Triggering', 'Remote Management', 'DMZ', 'ALG', 'Routing', 'Dynamic DNS', 'Device Discovery', 'MAC Bridging', 'Wi-Fi MESH', and 'Troubleshooting'. The main content area is titled 'Advanced > Port Forwarding' and contains the text 'Manage external access to specific ports on your network.' with a 'more' link. Below this, the 'Port Forwarding' status is shown as 'Disable' with 'Enable' and 'Disable' buttons. At the bottom of the main content area, there is a blue bar with 'Port Forwarding' and a '+ADD SERVICE' button. The footer of the page contains the text 'ARRIS • Customer Support • Open Source'.



**Important:** Check your cable provider's terms of service before enabling Port Forwarding. Some providers require a business services account for deploying servers.

- **Port Forwarding:** Click **Enable** to turn on Port Forwarding.
- **+Add Service:** Click to add a service.



- **Common Service:** If you are deploying a web server, select **HTTP** or **HTTPs**. If the service is not listed, select **Other**. By selecting a common service, you can simplify configuration.
- **Service Name:** (Other only) Enter a name for the service.
- **Service Type:** One of **TCP**, **UDP**, or **TCP/UDP** (the default).
- **Server IPv4 Address:** If you are using IPv4 addresses on your home network (the normal situation), enter the IPv4 address of the server. Or, click the **Connected Device** button to choose the server from a list.
- **Server IPv6 Address:** If you are using IPv6 addresses on your home network, enter the IPv6 address of the server. Or, click the **Connected Device** button to choose the server from a list.
- **Start Port:** (Other only) The first in a range of ports used to connect to your server.
- **End Port:** (Other only) The last in a range of ports used to connect to your server. If your service uses only one port, use the same value as **Start Port**.
- **Save:** Click to save the new service.

## Advanced > Port Triggering

Port Triggering allows devices external to your network to connect with services on your LAN. Port Triggering maps a port on your Gateway to the destination port on your server.

ARRIS

Hi, mso • Logout English

Internet Ethernet Wi-Fi Low Security

Gateway

Connected Devices

Parental Control

Advanced

Port Forwarding

Port Triggering

Remote Management

DMZ

ALG

Routing

Dynamic DNS

Device Discovery

MAC Bridging

Wi-Fi MESH

Troubleshooting

## Advanced > Port Triggering

Manage external access to specific ports on your network. [more](#)

Port Triggering:

Port Triggering

Service Name	Service Type	Trigger Port(s)	Target port(s)	Active
--------------	--------------	-----------------	----------------	--------

ARRIS • Customer Support • Open Source



**Important:** Check your cable provider's terms of service before enabling Port Triggering. Some providers require a business services account for deploying servers.

- **Port Triggering:** Click **Enable** to turn on Port Triggering.
- **+Add Port Trigger:** Click to add a trigger.

ARRIS

Hi, mso • Logout English

Internet Ethernet Wi-Fi Low Security

Gateway

Connected Devices

Parental Control

Advanced

Port Forwarding

Port Triggering

Remote Management

DMZ

ALG

Routing

Dynamic DNS

Device Discovery

MAC Bridging

Wi-Fi MESH

Troubleshooting

## Advanced > Port Triggering > Add Port Trigger

Add a rule for port triggering services by user. [more](#)

Add Port Trigger

Service Name:

Service Type:


Trigger Start Port:

Trigger End Port:

Target Start Port:

Target End Port:

ARRIS • Customer Support • Open Source

- **Service Name:** Enter a name for the service.
- **Service Type:** One of **TCP**, **UDP**, or **TCP/UDP** (the default).
- **Trigger Start Port:** The first in a range of ports that your Gateway listens for connections on.
- **Trigger End Port:** The last in a range of ports that your Gateway listens for connections on. If your service uses only one port, use the same value as **Trigger Port From**.
- **Target Start Port:** The first in a range of ports that your Gateway maps to the LAN.
- **Target End Port:** The last in a range of ports that your Gateway maps to the LAN. If your service uses only one port, use the same value as **Target Port From**.
  -  **Note:** The trigger port range and target port range should have an identical number of ports.
- **Add:** Click to save the new trigger.

# Advanced > Remote Management

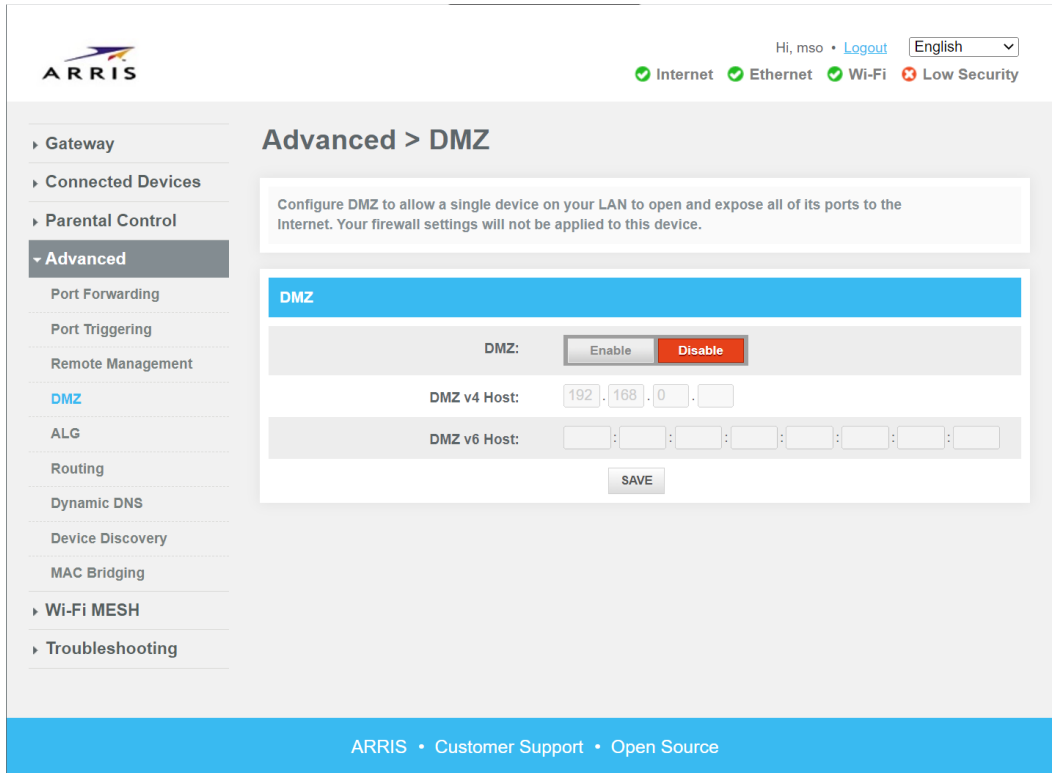
The Remote Management page allows computers outside the home network to access the Gateway's configuration pages.

The screenshot displays the ARRIS Gateway web interface. At the top right, it shows the user 'Hi, mso' with a 'Logout' link and a language dropdown set to 'English'. Below this, there are status indicators for 'Internet', 'Ethernet', 'Wi-Fi', and 'Low Security'. The left sidebar contains a navigation menu with 'Advanced' selected. The main content area is titled 'Advanced > Remote Management' and features a descriptive text box with a 'more' link. Below this is a 'Remote Management' toggle switch, currently set to 'Disable'. The 'IP Whitelist' section offers three radio button options: 'Single IP Address', 'Range Of IP Addresses', and 'Any IP Address'. Each option has corresponding input fields for IPv4 and IPv6 addresses. A note below the 'Any IP Address' option states: 'Note: This option will allow any device on the Internet to access your network and may cause a security risk.' A CAPTCHA verification box is located below the note, with a 'SAVE SETTINGS' button at the bottom. The footer of the page includes 'ARRIS • Customer Support • Open Source'.

See How do I *make changes from somewhere else?* (page 18) for instructions and cautions about using this feature.

## Advanced > DMZ

The DMZ page allows a single computer on the home network to bypass the firewall.



The screenshot displays the ARRIS web interface for configuring DMZ. At the top left is the ARRIS logo. The top right shows the user 'Hi, mso' with a 'Logout' link and a language dropdown set to 'English'. Below this are status indicators for 'Internet', 'Ethernet', 'Wi-Fi', and 'Low Security'. A left sidebar contains a navigation menu with items like Gateway, Connected Devices, Parental Control, Advanced (selected), Port Forwarding, Port Triggering, Remote Management, DMZ, ALG, Routing, Dynamic DNS, Device Discovery, MAC Bridging, Wi-Fi MESH, and Troubleshooting. The main content area is titled 'Advanced > DMZ' and contains a descriptive text box: 'Configure DMZ to allow a single device on your LAN to open and expose all of its ports to the Internet. Your firewall settings will not be applied to this device.' Below this is a 'DMZ' section with a blue header. It features a 'DMZ:' label followed by 'Enable' and 'Disable' buttons. Underneath are input fields for 'DMZ v4 Host' (pre-filled with '192.168.0') and 'DMZ v6 Host'. A 'SAVE' button is located at the bottom of the configuration area. The footer of the page includes 'ARRIS • Customer Support • Open Source'.

See [How do I bypass the firewall?](#) (page 17) for instructions on using this page.

## Advanced > ALG

Application Level Gateway (ALG) allows the Gateway to recognize certain network protocols for special treatment.

- **ID:** `a1g`
- **URL:** `alg.php`

The screenshot shows the ARRIS web interface for the 'Advanced > ALG' settings. The page includes a navigation menu on the left with options like Gateway, Connected Devices, Parental Control, Advanced (selected), Port Forwarding, Port Triggering, Remote Management, DMZ, ALG, Routing, Dynamic DNS, Device Discovery, MAC Bridging, Wi-Fi MESH, and Troubleshooting. The main content area has a header with 'ARRIS' logo, user info 'Hi, mso', a 'Logout' link, and a language dropdown set to 'English'. Below this, there are status indicators for Internet, Ethernet, Wi-Fi, and Low Security. The main heading is 'Advanced > ALG'. A text box explains that ALG settings allow the router to recognize and treat certain network protocols specially. Below this is a table titled 'Application Layer Gateway' with a 'Check All' checkbox and several protocol checkboxes, all of which are checked. A 'SAVE SETTINGS' button is located at the bottom of the table.

Application Layer Gateway			
<input type="checkbox"/> Check All	<input checked="" type="checkbox"/> SIP	<input checked="" type="checkbox"/> FTP	<input checked="" type="checkbox"/> TFTP
<input checked="" type="checkbox"/> PPTP	<input checked="" type="checkbox"/> H323	<input checked="" type="checkbox"/> IRC	<input checked="" type="checkbox"/> RTSP

SAVE SETTINGS

By default, all supported protocols are enabled for ALG. Uncheck any of the boxes to disable ALG for that protocol.

# Advanced > Routing

Configures Router Information Protocol (RIP) for the router.

The screenshot shows the ARRIS web GUI interface for configuring the Router Information Protocol (RIP). The page is titled "Advanced > Routing". On the left, there is a sidebar with navigation options: Gateway, Connected Devices, Parental Control, Advanced (selected), Port Forwarding, Port Triggering, Remote Management, DMZ, ALG, Routing (selected), Dynamic DNS, Device Discovery, MAC Bridging, Wi-Fi MESH, and Troubleshooting. The main content area is titled "Advanced > Routing" and contains three sections:

- RIP (Routing Information Protocol)**: This section has a "RIP:" toggle set to "Enable". Below it are fields for "Interface Name" (set to "Ethernet"), "RIP Send Version" (set to "RIP2"), "RIP Receive Version" (set to "Do Not Receive"), "Update Interval" (set to "5" sec), "Default Metric" (set to "1"), "Authentication Type" (set to "No Authentication"), "Authentication Key & ID" (with an "ID:" field), and "Neighbor" (set to "0.0.0.0").
- Routed Subnet Configuration**: This section has a "Routed Subnet:" toggle set to "Enable". Below it are fields for "Routed Subnet Address" and "Routed Subnet Netmask", both currently empty.
- Static Routing Settings**: This section has fields for "Destination Address", "Subnet Mask", and "Gateway Address", all currently empty.

At the bottom of the main content area, there is a "SAVE" button. The footer of the page reads "ARRIS • Customer Support • Open Source".

This is useful mainly for business services, when connecting remote locations together as a centralized network. Consult with your cable provider if you think you need this functionality.

- **RIP:** Click **Enable** to enable RIP.
- **Interface Name:** The interface (Ethernet or cable) that should send RIP information.
- **RIP Send Version:** Choose the RIP version to use when sending information to other routers, or Do Not Send to disable RIP.

- **RIP Receive Version:** Choose the RIP version to expect when receiving information, or Do Not Receive to disable RIP.
- **Update Interval:** The time between sending router updates.
- **Default Metric:** The relative cost to a link using this router as a hop (intermediate). Slower (or high-traffic) links should have a higher metric.
- **Authentication Type:** The method used to authenticate routers attempting to join the RIP network.
- **Authentication Key & ID:** The required credentials for networks requiring authentication.
- **Neighbor:** The IP address of the router to receive unicast information from the RIP router.
- **Routed Subnet Enable:** Click **Enable** to enable a routed subnet.
- **Routed Subnet Address:** The address to route this subnet to.
- **Routed Subnet Netmask:** The prefix of the routed subnet.



## Advanced > Dynamic DNS

Dynamic DNS (DDNS) allows servers using dynamic IP addresses to use a Fully Qualified Domain Name (FQDN) to access its services.

The screenshot displays the ARRIS WebGUI interface for configuring Dynamic DNS. The top right shows the user 'Hi, mso' with a 'Logout' link and a language dropdown set to 'English'. Status indicators for 'Internet', 'Ethernet', 'Wi-Fi', and 'Low Security' are visible. The left sidebar lists various configuration categories, with 'Advanced' selected. The main content area is titled 'Advanced > Dynamic DNS' and includes a sub-header: 'Configure the Gateway's router functionality as a Dynamic DNS client.' Below this, there is a 'Dynamic DNS:' section with 'Enable' and 'Disable' buttons. A table below lists columns for 'Service Provider', 'Username', 'Password', 'Host Name', and 'Token', with a '+ ADD DDNS' button in the top right corner of the table area. The footer contains 'ARRIS • Customer Support • Open Source'.

The Gateway periodically refreshes its IP information with one of several known DDNS services.

**Dynamic DNS:** click Enable to use DDNS.

The screenshot displays the ARRIS web interface for configuring Dynamic DNS. The breadcrumb trail is 'Advanced > Dynamic DNS > ADD'. A message states: 'You can configure a new DDNS entry by entering the following details.' with a 'more' link. The 'Dynamic DNS' section contains the following fields:

- Service Provider:
- Username:
- Password:
- Host Name:
- Token:

A 'SAVE SETTINGS' button is located at the bottom of the form. The footer of the page reads 'ARRIS • Customer Support • Open Source'.

- **Service Provider:** Choose from one of several known DDNS services.
- **Username:** The user account for the chosen DDNS service.
- **Password:** The password for the DDNS account.
- **Host Name:** The FQDN of the server using DDNS.

Click **Save Settings** to finish adding the service.

# Advanced > Device Discovery

Controls auto-configuration for devices that support it.

The screenshot displays the ARRIS web interface for configuring Device Discovery. At the top, the ARRIS logo is on the left, and user information (Hi, mso), a Logout link, and a language dropdown (English) are on the right. Below this, network status indicators show Internet, Ethernet, and Wi-Fi as active (green checkmarks), and Low Security as inactive (red X). The left sidebar lists navigation options: Gateway, Connected Devices, Parental Control, Advanced (selected), Port Forwarding, Port Triggering, Remote Management, DMZ, ALG, Routing, Dynamic DNS, Device Discovery (highlighted in blue), MAC Bridging, Wi-Fi MESH, and Troubleshooting. The main content area is titled 'Advanced > Device Discovery' and contains a 'Manage UPnP network.' link. Below this is a 'Device Discovery' section with the following settings:

- UPNP:  Enable  Disable
- Advertisement Period:  minutes
- Time To Live:  hops
- Zero Config:  Enable  Disable

A 'SAVE' button is located at the bottom of the configuration area. The footer of the page contains the text 'ARRIS • Customer Support • Open Source'.

- **UPNP:** Click **Enable** to allow client devices that support Universal Plug and Play (UPnP) to automatically configure themselves in the network.
- **Advertisement Period:** The interval between Gateway broadcasts, advertising UPnP information.
- **Time To Live:** The number of hops a UPnP packet may travel from the source.
- **Zero Config:** Click **Enable** to enable the zeroconf protocol, a discovery protocol that allows devices to connect to a network without using DHCP or similar services.

Click **Save** to save any changes.

# Advanced > MAC Bridging

Use this page to bridge individual devices directly to the WAN.

The screenshot shows the ARRIS web interface for MAC Bridging. At the top, there is a navigation bar with the ARRIS logo, user information (Hi, mso), a Logout button, and a language dropdown set to English. Below this, there are status indicators for Internet, Ethernet, Wi-Fi, and Low Security. The main content area is titled "Advanced > MAC Bridging" and contains a descriptive text box explaining MAC bridging. Below the text are four sections: "MAC Bridged Addresses" (empty), "Auto-Learned Devices" (empty table), "Custom Device" (input field for MAC address), and "Custom Range" (input fields for MAC Range Prefix and Bridged Range).

Bridged devices obtain an IP address from the service provider, and do not have access to the local network.

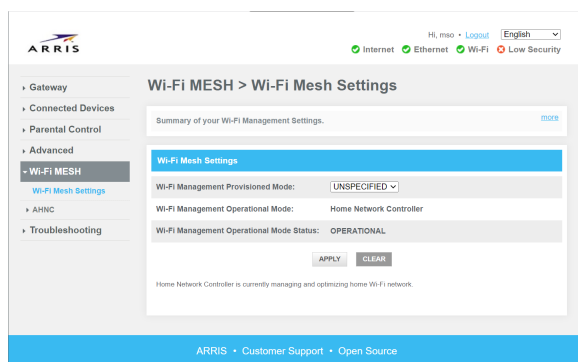
- **MAC Bridged Addresses:** Displays the MAC addresses of bridged devices, if any.
- **Auto-Learned Devices:** Displays devices that have previously connected to the local networks. You can check off a device to immediately begin bridging it.
- **Custom Device:** Enter the MAC address of the device you want to bridge, and click **Add**.
- **Custom Range:** Enter the MAC address range to bridge a group of related devices, and click **Add**.

# Wi-Fi MESH

Use these pages to select and manage your home network management system.

## Wi-Fi Mesh Settings

Displays and selects the Wi-Fi management mode.



- **Wi-Fi Management Provisioned Mode:** The management mode specified in the Gateway's configuration, or `UNSPECIFIED` if no setting was made.  
If you change the management mode, click **APPLY** to confirm the change, or **CLEAR** to return to the previous setting.
- **Wi-Fi Management Operational Mode:** The management mode in use. If the provisioned mode is `UNSPECIFIED`, this is the default mode for this firmware.
- **Wi-Fi Management Operational Mode Status:** The management mode status.

# AHNC

ARRIS Home Network Controller (AHNC), also called HomeAssure 1.3, allows management of your home network, either from the Gateway itself or using the HomeAssure app on a mobile device.

## Wi-Fi MESH > AHNC > Network Topology

Displays the Ethernet and Wi-Fi interfaces, and devices connected to each interface.

The screenshot shows the ARRIS Home Network Controller (AHNC) interface. At the top, there is a navigation bar with the ARRIS logo, user information (Hi, mso), a Logout button, and a language dropdown set to English. Below this, there are status indicators for Internet, Ethernet, Wi-Fi, and Low Security. The main content area is titled "Wi-Fi MESH > AHNC > Network Topology". On the left, there is a sidebar menu with options: Gateway, Connected Devices, Parental Control, Advanced, Wi-Fi MESH (selected), and Troubleshooting. Under Wi-Fi MESH, there are sub-options: Wi-Fi Mesh Settings, AHNC (selected), Network Topology (highlighted), and Steering History. The main content area shows a "View the Arris Home Network Topology." message with a "more" link. Below this, there are two panels: "Topology Structure" and "Topology Details". The "Topology Structure" panel shows a tree view of the network topology, starting with the gateway TG3442A, which has two radio interfaces: Radio-2.4GHz and Radio-5GHz. Radio-2.4GHz is connected to ARRIS-F21D, and Radio-5GHz is connected to ARRIS-F21D-5G. Both radio interfaces are connected to Ethernet interfaces. The "Topology Details" panel shows the following information for the selected interface:

Topology Details	
Interface Type:	SSID
Enabled:	true
Interface Status:	up
Number of Clients:	0
BSSID:	9C:C8:FC:52:33:C0
SSID:	ARRIS-F21D-5G
Broadcast SSID:	true
Security Mode:	WPA2-Personal

At the bottom of the page, there is a footer with the text "ARRIS • Customer Support • Open Source".

Collapse or expand as needed to see the current connections. The topology automatically refreshes every 10 seconds.

# Troubleshooting

These pages provide utilities and information that can help to resolve connectivity issues.

## Troubleshooting > Logs

Displays Gateway activity logs.

The screenshot shows the ARRIS WebGUI interface for the 'Troubleshooting > Logs' page. At the top right, there is a user profile 'Hi, mso' with a 'Logout' link and a language dropdown set to 'English'. Below this, there are status indicators for 'Internet', 'Ethernet', 'Wi-Fi' (all green), and 'Low Security' (red). The left sidebar contains a navigation menu with 'Troubleshooting' selected. The main content area has a header 'Troubleshooting > Logs' and a sub-header 'System Logs > All logs from Today'. Below the sub-header is a table of log entries:

Log Type	Time	Severity
GUI: User:mso login	06/08/2022 12:26:09	Notice
GUI: User:mso logout	06/08/2022 11:50:00	Notice
GUI: User:mso login	06/08/2022 11:33:38	Notice

Below the table are 'PRINT' and 'DOWNLOAD' buttons. The footer of the page contains 'ARRIS • Customer Support • Open Source'.

- **Log Type:** Choose one of:
  - System Logs
  - Event Logs
  - Firewall Logs
- **Time Frame:** Choose the time frame for the log display.
- **Show Logs:** Click to display the selected logs.

# Troubleshooting > Diagnostic Tools

Use the tests on this page to check network connectivity.

The screenshot displays the ARRIS web interface for network diagnostic tools. At the top right, there are status indicators for Internet, Ethernet, Wi-Fi, and Low Security. The main navigation sidebar on the left includes options like Gateway, Connected Devices, Parental Control, Advanced, Wi-Fi MESH, Troubleshooting (selected), Logs, Diagnostic Tools, Wi-Fi Spectrum Analyzer, DOCSIS Spectrum Analyzer, and Restart/Restore. The main content area is titled 'Troubleshooting > Diagnostic Tools' and contains a sub-header 'Troubleshoot your network connectivity.' Below this, there are four distinct test sections: 'Test Connectivity' (with a 'Destination Address' field containing 'www.commscope.com' and a 'Count' dropdown set to '4'), 'Test IPv4 Address' (with an IPv4 address input field), 'Test IPv6 Address' (with an IPv6 address input field), and 'Traceroute' (with separate IPv4 and IPv6 address input fields). Each section includes a 'START TEST' button. The footer of the interface reads 'ARRIS • Customer Support • Open Source'.

- **Test Connectivity:** Enter an IP address or FQDN in the **Destination Address** box and click **Start Test**. The gateway uses ICMP (Ping) to test connectivity. Note that a failed test might mean the destination does not allow Ping, rather than no connectivity.
- **Test IPv4 Address:** Enter an IPv4 address and click **Start Test**.
- **Test IPv6 Address:** Enter an IPv6 address and click **Start Test**.
- **Traceroute:** Enter an IPv4 or IPv6 address in the appropriate line and click **Start Test**. The Gateway opens a window, displaying the intermediate hops (routers) between the Gateway and the destination address.



# Troubleshooting > Wi-Fi Spectrum Analyzer

Displays all Wi-Fi networks detected by the Gateway radios.

The screenshot shows the ARRIS WebGUI interface for the Wi-Fi Spectrum Analyzer. At the top, there is a navigation menu with options like Gateway, Connected Devices, Parental Control, Advanced, Wi-Fi MESH, and Troubleshooting (which is currently selected). Below the menu, there are links for Logs, Diagnostic Tools, Wi-Fi Spectrum Analyzer (highlighted), DOCSIS Spectrum Analyzer, and Restart/Restore. The main content area is titled 'Troubleshooting > Wi-Fi Spectrum Analyzer' and contains a description: 'The Wi-Fi Spectrum Analyzer allows you to view details about other Wi-Fi networks in your area.' Below this description is a blue box titled 'Wi-Fi Spectrum Analyzer Data' which contains a 'START SCAN' button, a 'VIEW GRAPH' button, and a dropdown menu currently set to '2.4 GHz'. The footer of the page includes 'ARRIS • Customer Support • Open Source'.

- **Start Scan:** Click to start scanning for other networks.
- **View Graph:** Click to display the scan in a graphical format. When viewing a graph, this button changes to **View Table**.
- **Band:** Select the band to scan: **2.4 GHz** or **5 GHz**.

# Troubleshooting > DOCSIS Spectrum Analyzer

Use this page to view the HFC RF spectrum.

The screenshot shows the ARRIS web interface for the DOCSIS Spectrum Analyzer. At the top left is the ARRIS logo. At the top right, it displays the user 'Hi, mso', a 'Logout' link, and a language dropdown set to 'English'. Below this, there are status indicators for 'Internet', 'Ethernet', 'Wi-Fi', and 'Low Security'. A left-hand navigation menu includes 'Gateway', 'Connected Devices', 'Parental Control', 'Advanced', 'Wi-Fi MESH', 'Troubleshooting' (which is expanded to show 'Logs', 'Diagnostic Tools', 'Wi-Fi Spectrum Analyzer', 'DOCSIS Spectrum Analyzer', and 'Restart/Restore'), and 'Restart/Restore'. The main content area is titled 'Troubleshooting > DOCSIS Spectrum Analyzer' and contains a text box stating 'The DOCSIS Spectrum analyzer allows you to view details about DOCSIS RF in your area.' Below this is a blue header for 'DOCSIS Spectrum Analyzer Data' with 'START SCAN' and 'VIEW GRAPH' buttons. At the bottom of the main area, there are input fields for 'Center (MHz)' (set to 500) and 'Width (MHz)' (set to 1000), along with an 'Update Continuously' checkbox.

- **Center (MHz):** The center frequency of the band to scan.
- **Width (MHz):** The frequency width, in MHz.
- **Start Scan:** Click to begin the spectrum analysis.
- **View Graph:** Click to view the results as a graph. The button title changes to **View Table**.
- **Update Continuously:** Check to continuously scan and display results.

# Troubleshooting > Restart/Restore

Restarts the entire Gateway, or selected components.

The screenshot displays the ARRIS WebGUI interface for the 'Restart/Restore' section. At the top, the ARRIS logo is on the left, and user information (Hi, mso) and language (English) are on the right. Below the logo, there are status indicators for Internet, Ethernet, Wi-Fi, and Low Security. The main navigation menu on the left includes Gateway, Connected Devices, Parental Control, Advanced, Wi-Fi MESH, Troubleshooting (selected), Logs, Diagnostic Tools, Wi-Fi Spectrum Analyzer, and DOCSIS Spectrum Analyzer. The 'Restart/Restore' page title is 'Troubleshooting > Restart/Restore'. The main content area shows 'Restart or restore the Gateway.' with a 'more' link. Below this, the 'Restart/Restore' section is highlighted in blue. It displays 'System Uptime: 0d 21h 20m 9s'. The actions listed are:
 

- RESTART GATEWAY**: Restarts the entire Gateway.
- RESTART WI-FI MODULE**: Restarts only the Wi-Fi module.
- RESTART WI-FI & ROUTER**: Restarts both the Wi-Fi and Router modules.
- RESTORE WI-FI DEFAULTS**: Restores Wi-Fi settings back to the factory defaults. **Any changes you made will be lost.**
- RESET ADMIN PASSWORD**: Resets the admin password back to the factory default.
- RESTORE GATEWAY DEFAULTS**: Restores all Gateway settings back to the factory defaults. **Any changes you made will be lost.**

 The 'Backup and Restore Settings' section is also highlighted in blue. It contains:
 

- BACKUP SETTINGS**: Backup your gateway config file. You can restore it later if your settings are lost.
- RESTORE SETTINGS**: Choose File No file chosen

 The footer of the page reads 'ARRIS • Customer Support • Open Source'.

- **Restart Gateway:** Click to restart the Gateway.
- **Restart Wi-Fi Module:** Click to restart only the Wi-Fi interfaces.
- **Restart Wi-Fi & Router:** Click to restart the Router module (which includes the Wi-Fi interfaces).
- **Restore Wi-Fi Defaults:** Click to restore Wi-Fi settings back to factory defaults. Any changes you have made are lost.
- **Reset Password:** Click to reset the admin password to the factory default (password).
- **Restore Gateway Defaults:** Click to restore all Gateway settings to factory defaults. Any changes you have made are lost.

# CommScope legal statements

---

© 2022 CommScope, Inc. All rights reserved. All trademarks identified by ™ or ® are trademarks or registered trademarks in the US and may be registered in other countries. All product names, trademarks and registered trademarks are property of their respective owners.

No part of this content 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 CommScope, Inc. and/or its affiliates (“CommScope”). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

## Export restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

*These items are controlled by the U.S. government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.*

## Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES (“MATERIALS”), ARE PROVIDED “AS IS” AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, CommScope DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability, or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

## Limitation of liability

IN NO EVENT SHALL CommScope, CommScope AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIES, LICENSORS, AND THIRD-PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF CommScope HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

## Trademarks

ARRIS and the ARRIS Logo are trademarks of CommScope, Inc. and/or its affiliates. All other trademarks are the property of their respective owners.

# Contacts

---

## Technical services

For technical support, you can contact us by phone, email, or on the web.

### By telephone

The Technical Support Center may be reached at:

- +1-215-323-2346
- +1-888-944-HELP (4357).

Additional support numbers are located at: <https://www.commscope.com/globalassets/digizuite/294037-arris-combined-contact-information-phone.pdf>. For faster service, use your IVR support ID.

### On the web

Please visit [Ask ARRIS](#), which is the Technical Support web portal. You will need to register for this tool using your support contract ID and email address. There you will be able to access:

- Support Contact Information for all products
- Knowledge Base Information (also known as Solutions)
- User Documentation
- Current open support cases
- Ability to create a new support case (for technical support or repair and return)
- Training Webcasts

### By email

The Technical Support Center may also be reached by email:

Provider group	Products	Email address
Home Broadband	Touchstone, SURFboard, NVG without ECO, Extenders, HAV3, Plume, Assia	<a href="mailto:homebroadbandsupport@commscope.com">homebroadbandsupport@commscope.com</a>
HomeAssure Support	ECO, Edge, Andromeda	<a href="mailto:homeassuresupport@commscope.com">homeassuresupport@commscope.com</a>
Home Media Devices	QAM STB – Not supported by LTTS, IP STB	<a href="mailto:homemediadevicesupport@commscope.com">homemediadevicesupport@commscope.com</a>


Provider group	Products	Email address
Home Media Software	KreaTV	<a href="mailto:homemediasoftwaresupport@commscope.com">homemediasoftwaresupport@commscope.com</a>

Additional email addresses for ARRIS products are located at: <https://www.commscope.com/globalassets/digizuite/1651-techsupport-contact-information-email.pdf>.

## Technical training

For more information about our Global Knowledge Services Department and the programs we offer, email us at: [techtraining@commscope.com](mailto:techtraining@commscope.com).





**Corporate Headquarters**  
**CommScope · Hickory · North Carolina · 28602 · USA**  
T: 1-828-324-2200  
[www.commscope.com](http://www.commscope.com)