Global Knowledge Services

Touchstone

Router Web GUI User Guide

STANDARD 2.2

February 2017

ARRIS Copyrights and Trademarks

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

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

Table of Contents

Introduction

This section helps you set up your router and configure your wireless connection.

Before You Start

If your cable provider installed your Gateway, the installer may have already connected your primary devices and you may not need to do anything further. If you installed the Gateway yourself, gather the following materials and information:

- Find the quick installation sheet in the Gateway packaging. If the sheet is not available, you can download full manuals at *http://www.arrisi.com/support/guides/* (*http://www.arris.com/support/guides/*)
- A computer with an Ethernet jack (preferred), or a computer or tablet with Wi-Fi (acceptable).
- If you have a computer with Ethernet, obtain an Ethernet cable. The Gateway package may contain a yellow Ethernet cable; if not, the electronics department of most stores carry them.
- If your cable provider requires any special steps to connect your Gateway, the installer should leave a document with those steps provided.

When you have everything required above, proceed to *Connecting to the Gateway*.

Note: Your cable provider may have disabled or removed some of the configuration options in your Gateway. If you are unable to access certain screens or fields described in this document, contact your cable provider for help.

Connecting to the Gateway

Your first step is connecting to the Gateway. You can use either of the following methods.

Connecting using Ethernet (preferred):

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* (*http://www.arris.com/support/guides/*). If successful, proceed to *Accessing the Configuration Interface*.

If you have a problem (Ethernet):

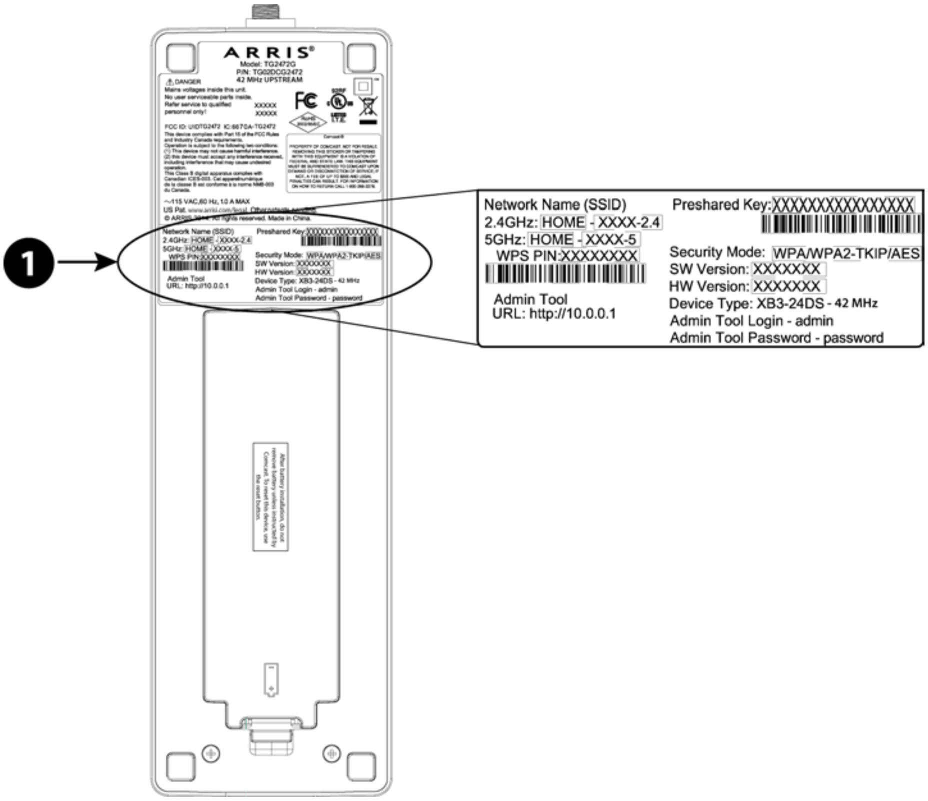
Check the following:

- 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.

Connecting 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:



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 supports both, connect to the 5/5G network.

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

   - 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.

   Be sure to enter the password exactly as shown.

4. When the device indicates a successful connection, attempt to access an external website, such as *ARRIS documentation* (*http://www.arris.com/support/guides/*). If successful, proceed to *Accessing the Configuration Interface*.

If you have a problem (Wi-Fi):

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.

Accessing the Configuration Interface

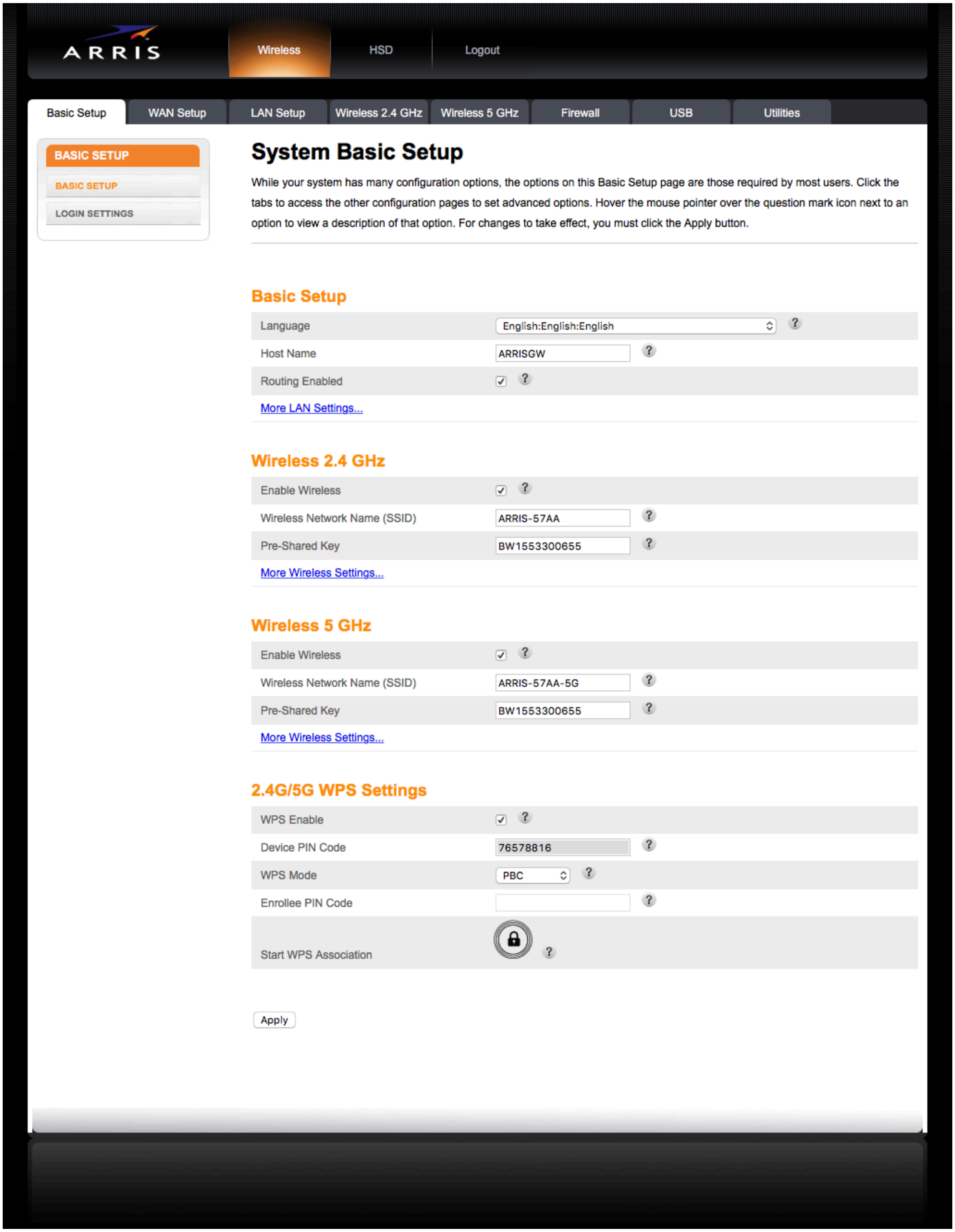
Perform the following steps to access the configuration interface.

Note: You should have already performed the steps described in *Connecting to the Gateway*.

1. In your web browser, open the page http://192.168.0.1/ to access the Gateway Login page.
2. Enter the user name and password and click the **Apply** button to log in.

   Note: The default user name is `admin`. The default password is `password`, in lower case letters.

3. You should now see the Basic Setup page:



System Basic Setup

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

Basic Setup

Language	English:English:English
Host Name	ARRISGW
Routing Enabled	☑

More LAN Settings...

Wireless 2.4 GHz

Enable Wireless	☑
Wireless Network Name (SSID)	ARRIS-57AA
Pre-Shared Key	BW1553300655

More Wireless Settings...

Wireless 5 GHz

Enable Wireless	☑
Wireless Network Name (SSID)	ARRIS-57AA-5G
Pre-Shared Key	BW1553300655

More Wireless Settings...

2.4G/5G WPS Settings

WPS Enable	☑
Device PIN Code	76578816
WPS Mode	PBC
Enrollee PIN Code	
Start WPS Association	

When you see this page, proceed to How Do I…

If you have a problem:

If you can access Internet sites, your device is properly connected. If not, look at the problem-solving tips in *Connecting to the Gateway*.

Some cable providers might change the default Gateway address used to access the configuration pages. Common alternative addresses include:

- http://192.168.10.1
- http://192.168.254.254

If your device is connected to the Gateway, it can show you the actual Gateway address. Find your operating system in the list below and proceed as follows:

- MacOS X: Open System Preferences, then select the Network icon. The address labeled "Router" is the Gateway address.
- iOS (iPad, iPhone, iPod touch): Tap Settings, then Wi-Fi, then your network name (there is a check mark next to the network). The address labeled "Router" is the Gateway address.
- Windows: Open the Control Panel, select the Network and Sharing Center icon, then click Local Area Connection. In the Local Area Connection Status window, click Details. The address labeled "IPv4 Default Gateway" is the Gateway address.
- Android: Tap Settings, then Wireless and VPN, then Wi-Fi, then your network name (there is a check mark next to the network). The address shown is the address your device is using. If the address is something like 192.168.10.5, try replacing the 5 with a 1 or 254 to find the Gateway address. If that does not work, use a third-party app (search for "Network Tools" in the Google Play store) to find the Gateway address.

If you still cannot connect to the configuration pages, contact your cable provider for help.

How Do I…

Find what you want to do in the following list and click the link to jump to that page. If you are an advanced user and want to see what is available in the configuration pages, proceed to *Web GUI Screens and Configuration Parameter Reference* (page 24).

How do I…

- *change my Wi-Fi network name?*
- *change my Wi-Fi network password?*
- *change my Gateway password?*
- *hide my Wi-Fi network from other users?*
- *see what devices are using my Gateway?*
- *connect older devices to my Gateway?*
- *keep the kids from accessing certain websites?*
- *block certain devices from accessing my Gateway?*
- *extend the range of my Wi-Fi network?*
- *back up or restore my Gateway settings?*
- *make changes from somewhere else?*
- *see if the Gateway is connected to the Internet?*
- *connect if I've forgotten my Wi-Fi password?*
- *reset the Gateway?*
- *fix interference problems?*
- *fix a slow connection?*
- *change the language for the Gateway configuration page?*
- *troubleshoot my connection?*

change my Wi-Fi network name?

1. If you are not on the Basic Setup page, click the Basic Setup tab.
2. Under both Wireless 2.4 GHz and Wireless 5 GHz, enter the names you want to use for each network in the Wireless Network Name (SSID) field.
3. At the bottom of the screen, click **Apply**.

Note: Devices connected to your Gateway may be disconnected after you change the network names. Re-connect them with the new network name, and re-enter the password.

change my Wi-Fi network password?

If you are not on the Basic Setup page, click the Basic Setup tab.

1. Under both Wireless 2.4 GHz and Wireless 5 GHz, enter the names you want to use for each network in the Pre-Shared Key field.
2. At the bottom of the screen, click **Apply**.

Note: Devices connected to your Gateway may be disconnected after you change the passwords. Re-connect them, and re-enter the password.

change my Gateway password?

1. Go to the Login Settings page. To do this, click on the Basic Setup tab, then click Login Settings in the side menu along the left.
2. Enter your current password in the Old Password field. If you have never changed this password, enter `password` here.
3. Enter the new password in the New Password field.

Note: Passwords are case-sensitive. Valid characters are the numbers 0 to 9, the letters a through z and A through Z, and printable special characters (such as $, !, ?, &, #, @, and others). Do not use spaces.

4. Re-type the new password in the Repeat New Password field.
5. Click the **Apply** 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 the Wireless 2.4 GHz tab to open the Basic Setup screen for the 2.4 GHz Wi-Fi network.
2. Uncheck the Broadcast Network Name (SSID) box.
3. Click **Apply**.
4. Click the Wireless 5 GHz tab to open the Basic Setup screen for the 5.0 GHz Wi-Fi network, and repeat steps 2 and 3.

Note: 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.

see what devices are using my Gateway?

1. Click the Wireless 2.4 GHz or Wireless 5 GHz tab.
2. In the side menu on the left, click Wireless Client List. 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
3. Repeat steps 1 and 2 for the other network (2.4 GHz or 5 GHz) to see what devices are connected to that part of your network.

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.

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, follow these steps.

1. Click the Wireless 2.4 GHz tab, then click BASIC in the side menu on the left.
2. Click the Wireless Security dropdown, and change the mode to WEP (64/128).

Note: WEP security is easier to attack than WPA. If you have to use WEP security, disable your network when not in use.

set up Band Steering?

First, make sure the SSID and passphrase for the 2.4 GHz and 5.0 GHz networks are identical. Then, in the Wireless 5.0 GHz Advanced Settings, check the Band Steering box.

keep the kids from accessing certain websites?

Note: No blocking system is foolproof.

Parental Controls allow 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.

To access the Parental Controls page, click the Firewall tab then click Parental Controls in the side menu on the left.

To enable Parental Controls:

1. Click the Enable Parental Controls box and then click **Apply**.
2. To add trusted devices, enter the MAC address of each device (up to two) in the Trusted MAC Addresses fields.

   To see the MAC addresses of connected devices, see How Do I *see what devices are using my Gateway?*

To add a keyword filter:

1. Click Add under Keyword Filtering.
2. In the dialog box:
   - enter the keyword that you want to block.
   - 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).
3. Click the **Add Keyword Filter** button to complete the entry.

To add a web site filter:

1. Click Add under Web Site Filtering.
2. In the dialog box:
   - enter the web site that you want to block.
   - 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).
3. Click the **Add Website Filter** button 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.

block certain devices from accessing my Gateway?

Note: No blocking system is foolproof.

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?*
- 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.

To add devices to the list:

Note: Do this before enabling blocking, especially whitelisting. If you enable whitelisting without any devices in the list, nobody can access the network.

1. Click the Wireless 2.4 GHz or Wireless 5 GHz tabs as desired, then click MAC Address Control in the side menu on the left.
2. Under MAC Address Filter List, click **Add**.
3. Enter the MAC address to add to the list in the dialog box, then click the **Add MAC Address** button.
4. Repeat steps 2 and 3 as necessary to complete the list.
5. When you have completed the list, click **Apply**.

To remove devices from the list:

1. If necessary, click the Wireless 2.4 GHz or Wireless 5 GHz tabs as desired, then click MAC Address Control in the side menu on the left.
2. Check the box next to each device you want to remove from the list.
3. Click **Delete** to remove the selected devices.
4. Click **Apply**.

To enable or disable blocking:

1. If necessary, click the Wireless 2.4 GHz or Wireless 5 GHz tabs as desired, then click MAC Address Control in the side menu on the left.
2. Choose one of the following from the MAC Address Filter Type dropdown:
   - To disable blocking, select **None**.
   - To enable a whitelist, select **Allowed List**. (Make sure you have entered MAC addresses first.)
   - To enable a blacklist, select **Blocked List**.
3. Click **Apply**.

extend the range of my Wi-Fi network?

The ARRIS WR2100 Universal Wi-Fi N Range Extender is a simple way to extend the range of any Wi-Fi network. Place the extender within range of your Gateway, and follow the simple instructions to associate the Extender with your Gateway.

The WR2100 is available at many local and online retailers.

back up or restore my Gateway settings?

Once you have the Gateway configured the way you want it, you should save the settings. If you need to reset the Gateway, you can quickly restore your settings. You may also need to restore the settings if you update the Gateway firmware.

To back up the Gateway settings:

1. Click the Utilities tab, then Save/Backup Settings from the side menu on the left.
2. Click the **Save** button.
3. When your browser prompts you to download the file, accept the download. If you make no changes, you should find a file named `router.data` in your Downloads folder. You can rename this file to indicate a special configuration. You can also move the file to a different location if you want.

To restore the Gateway settings:

1. Click the Utilities tab, then Restore Settings from the side menu on the left.
2. Click the Choose File button.
3. When your browser prompts you for a file, navigate to a previously-saved setting file (if you have not moved or renamed the file, look for `router.data` in your Downloads folder) and confirm the choice.
4. Click the **Restore Chosen File** button on the Gateway screen.

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?* for instructions.

To set up Remote Management:

1. Click the Utilities tab, then Remote Management from the side menu on the left.
2. If all the fields are disabled, you need to change the Gateway password as noted above.
3. Check the HTTP Enable (and if you want, HTTPS Enable) boxes.
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 the Allowed Type dropdown:
   - **Any Computer**: 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.
   - **Single Computer**: allows access from one specific IP address. Use this option if you know exactly which IP address will be used to access the Gateway.
   - **Range of IPs**: 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.
6. Fill in the IP address or range as needed.
7. When finished, disable Remote Management by unchecking the HTTP Enable and HTTPS Enable boxes.

see if the Gateway is connected to the Internet?

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.

If the lights are on, connect a device to your network and attempt to access a known site such as *http://www.arris.com/consumer* (*http://www.arris.com/consumers*) — if you see the page, you are connected. If not, see *troubleshoot my connection?* below.

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

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.

If you have changed the default password and then forgotten it, you can connect to the Gateway without a password by using a computer with an Ethernet connection. Access the Gateway configuration pages and use *change my Wi-Fi network password?* 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.
- *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. If you have downloaded a settings file, you can use it to restore your configuration settings.

To restart your Gateway:

There are two ways to restart your Gateway.

- If connected to the configuration pages, click the Utilities tab and then Restart Router from the side menu on the left. Click the **Restart** button.
- 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:

There are two ways to factory reset your Gateway.

- If connected to the configuration pages, click the Utilities tab and then Factory Defaults from the side menu on the left. Click the **Factory 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.

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)

The Gateway can display a list of other Wi-Fi networks in the immediate area. To do this:

1. Click the Wireless 2.4 GHz or Wireless 5 GHz tab, then click Active Access Points in the side menu on the left.
2. Click the **Scan** button.
3. Locate your Wi-Fi network on the graph and see whether there are other access points using the same or adjacent channels.

fix a slow connection?

The following issues can cause a slow connection:

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

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

  If possible, move your fastest devices to the 5 GHz network for best performance.
- a computer downloading a large system update

  Some operating systems provide the option of downloading system updates overnight. If possible, postpone the update.
- one or more streaming video services in use

  Wait for the show to finish.
- many neighbors using the Internet (a neighborhood shares the same connection to the cable network's routers)
- congestion on the Internet itself

change the language for the Gateway configuration page?

Click the Utilities tab, then click Language in the side menu on the left. If the current language is one you do not read:

- the Utilities tab is all the way to the right.
- the Language selection is the eighth selection, exactly in the middle of the side menu.

Select the language you want from the dropdown menu, and click **Apply** (the button below the dropdown).

troubleshoot my connection?

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.

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.

Next, 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.

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

Using a computer connected to the Gateway Ethernet, see *hide my Wi-Fi network from other users?* to see whether the Gateway is broadcasting its SSID. Check the Broadcast Network Name (SSID) box and click **Apply**.

If that was not the problem, click the Wireless 2.4 GHz or Wireless 5 GHz tab, then (if necessary) click Basic in the side menu on the left. Make sure the Enable Wireless box is checked. If the name in the Wireless Network Name (SSID) box does not look like what you expect, change it if needed. When you have made any necessary changes, click **Apply**.

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

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

If the devices having problems are older, see *connect older devices to my Gateway?* for help.

If that was not the problem, using a computer connected to the Gateway Ethernet, click the Wireless 2.4 GHz or Wireless 5 GHz tab, then (if necessary) click Basic in the side menu on the left. Check the Pre-Shared Key toward the bottom of the page to see whether it matches the password you expected. Make any changes necessary, then click **Apply**.

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

The connection is always slow.

First, try the suggestions in *fix a slow connection?*

Next, connect to the Gateway, using Ethernet if possible, and access *http://speedtest.net/* (*http://www.speedtest.net/*). (Click only the link in the middle of the page, ignore all the fake dialog boxes and "Begin Scan" buttons around it.) 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.

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

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.

If the slow times happen at random, the problem is likely interference. See *fix interference problems?* for tips.

Chapter 2

Web GUI Screens and Configuration Parameter Reference

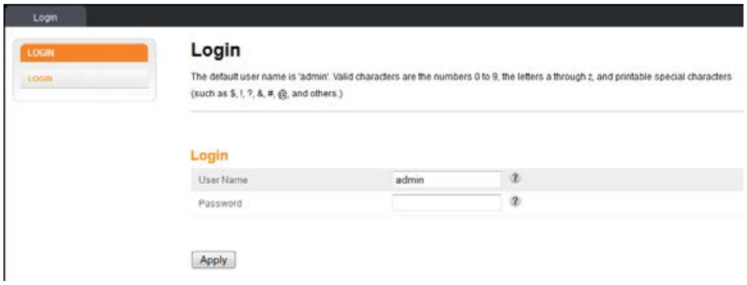
This section shows the ARRIS graphical user interface (GUI) router setup screens.

Each of the following six tabs in the GUI and their individual sub-menus and configuration parameters are explained in detail:

- *Basic Setup*
- *WAN Setup*
- *LAN Setup*
- *Wireless Setup*
- *Firewall*
- *Utilities*

Basic Setup

Basic Setup – Login



Login

The default user name is 'admin'. Valid characters are the numbers 0 to 9, the letters a through z, and printable special characters (such as $, !, ?, &, #, @, and others.)

Login

User Name	admin
Password	

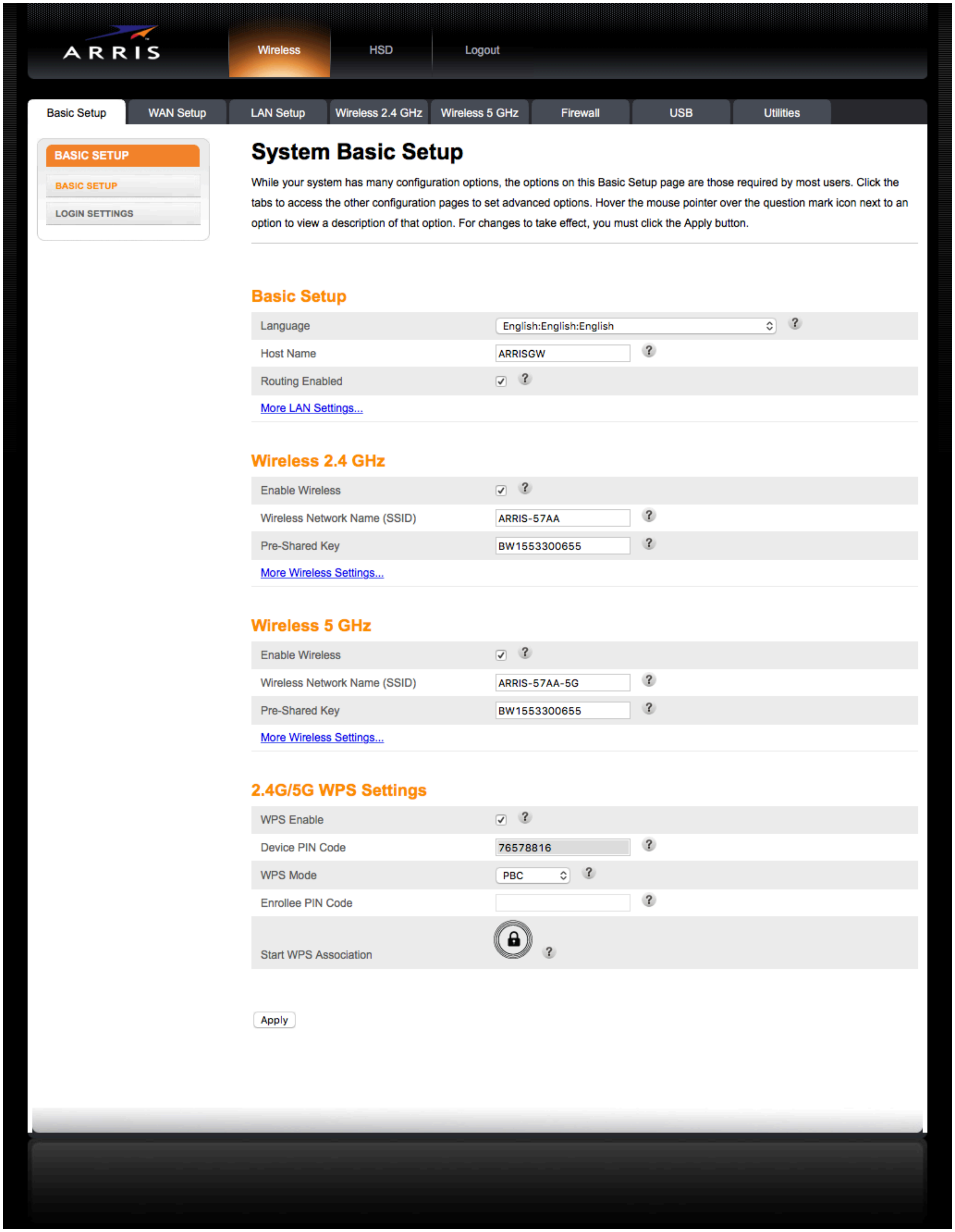
The default user name is "admin". Valid characters are the numbers 0 to 9, the letters a through z, and printable special characters (such as $, !, ?, &, #, @, and others.)

Login:

User Name – Current user name.

Password – Enter a password for this user. Passwords are case-sensitive. Valid characters are the numbers 0 to 9, the letters a through z and A through Z, and printable special characters (such as $, !, ?, &, #, @, and others.)

Basic Setup – System Basic Setup



System Basic Setup

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

Basic Setup

Language	English:English:English
Host Name	ARRISGW
Routing Enabled	☑

More LAN Settings...

Wireless 2.4 GHz

Enable Wireless	☑
Wireless Network Name (SSID)	ARRIS-57AA
Pre-Shared Key	BW1553300655

More Wireless Settings...

Wireless 5 GHz

Enable Wireless	☑
Wireless Network Name (SSID)	ARRIS-57AA-5G
Pre-Shared Key	BW1553300655

More Wireless Settings...

2.4G/5G WPS Settings

WPS Enable	☑
Device PIN Code	76578816
WPS Mode	PBC
Enrollee PIN Code	
Start WPS Association	

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

Basic Setup:

Language – Sets the language for the screen display text.

Host Name – The host name of the router.

Routing Enabled – Enables IP routing on your network. Change this setting only if your cable provider recommends it.

Wireless 2.4 GHz/Wireless 5 GHz:

Enable Wireless – Check this box to enable the wireless network on your system.

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

Pre-Shared Key – Sets your WPA Pre-Shared Key. This text string is used to generate a unique set of encryption keys for your network. Enter a text string in this field. The key can be either ASCII (text) or Hex (hexadecimal). An ASCII text key can be from 8 to 63 characters long. Valid characters are numbers "0" through "9" and letters "a" through "z", and any printable ASCII characters. A hexadecimal key must be 64 characters long. Valid characters are numbers "0" through "9" and letters "a" through "f".

2.4G/5G WPS Settings:

WPS Enable – Check this box to enable WPS (Wi-Fi Protected Setup) on your system. WPS is a standard method for easily configuring a secure connection between your router and computers or other wireless devices (known as enrollees) that support WPS. When WPS is enabled you can attach other wireless devices by pressing the WPS buttons on the device (if equipped) and on your router, or by entering the enrollee's PIN and then clicking the Start WPS Association icon.

Device PIN Code – Enter this code on your computer if requested during connection.

WPS Mode – Sets the encryption method for WPS. Can be set to PBC (Push Button Control) or PIN Code.

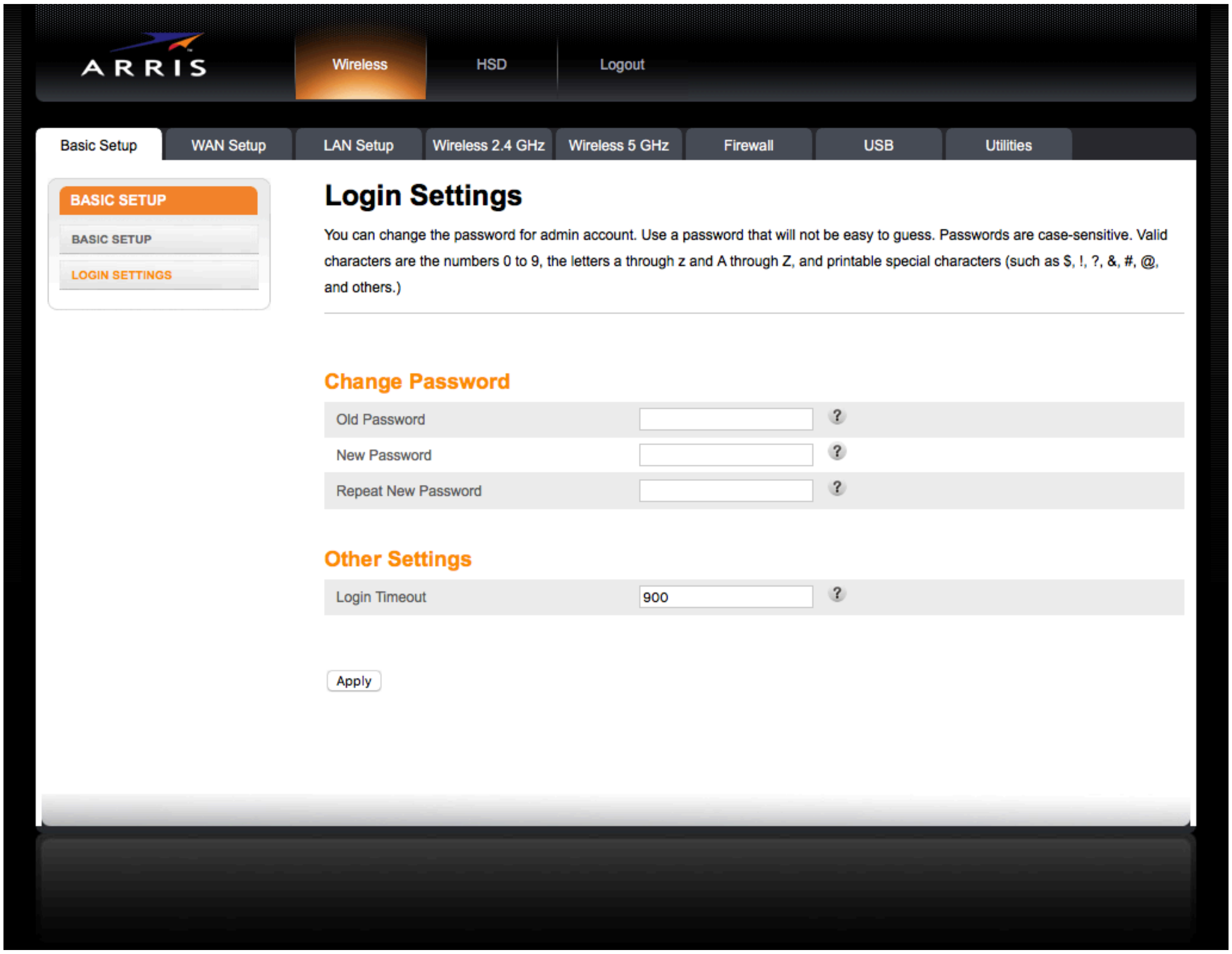
If using PBC, press the WPS buttons on the client device and on your router simultaneously to start the WPS association. If using PIN codes, enter the enrollee's PIN in the Enrollee PIN Code field, and then click the Start WPS Association icon.

If the connection is successful, the WPS indicator light on the router stops flashing and remains lit. If unsuccessful, the WPS light continues to flash for up to two minutes (indicating that it is ready to accept a client connection) and then turns off. If the WPS light turns off, start the association process over.

Enrollee PIN Code – If your client device has a WPS PIN number, enter it here, then click the Start WPS Association icon.

Start WPS Association – Click the WPS icon after (optionally) entering the enrollee's PIN to configure the network connection to the device.

Basic Setup – Login Settings



Login Settings

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

Change Password

Old Password	
New Password	
Repeat New Password	

Other Settings

Login Timeout	900

Apply

Click **Login Settings** in the side menu and follow the screen instructions to change the password for the `admin` account. Use a password that is not easy to guess. Passwords are case-sensitive. Valid characters are the numbers 0 to 9, the letters a through z and A through Z, and printable special characters (such as $, !, ?, &, #, @, and others). You must click the **Apply** button to save your new password.

Note: You must be logged into the configuration interface via a direct wired Ethernet connection to change your password.

Change Password:

Old Password – Enter your existing password.

New Password – Enter your new password.

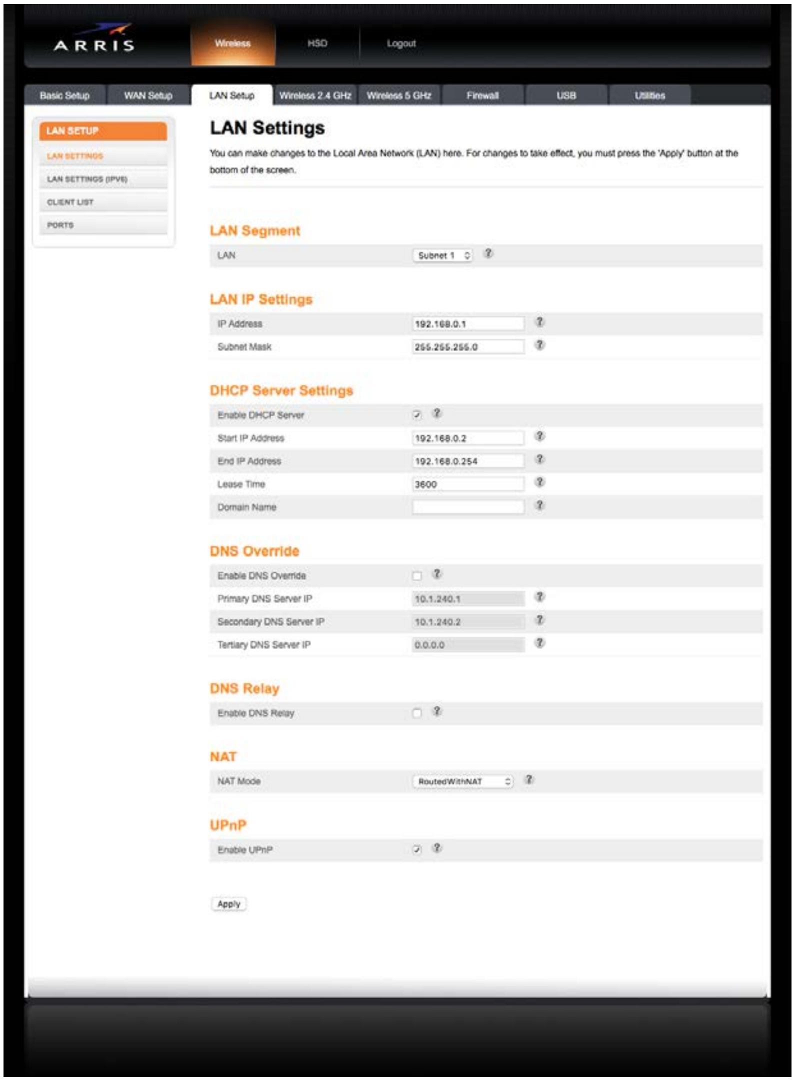
Repeat New Password – Re-enter your new password.

Other Settings:

Login Timeout – The time, in seconds, your session can remain idle until the Gateway automatically logs you out.

LAN Setup

LAN Setup – LAN Settings



LAN Settings

You can make changes to the Local Area Network (LAN) here. For changes to take effect, you must press the 'Apply' button at the bottom of the screen.

LAN Segment

LAN	Subnet 1

LAN IP Settings

IP Address	192.168.0.1
Subnet Mask	255.255.255.0

DHCP Server Settings

Enable DHCP Server	☑
Start IP Address	192.168.0.2
End IP Address	192.168.0.254
Lease Time	3600
Domain Name	

DNS Override

Enable DNS Override	☐
Primary DNS Server IP	10.1.240.1
Secondary DNS Server IP	10.1.240.2
Tertiary DNS Server IP	0.0.0.0

DNS Relay

Enable DNS Relay	☐

NAT

NAT Mode	RoutedWithNAT

UPnP

Enable UPnP	☑

You can make changes to the Local Area Network (LAN) configuration here. For changes to take effect, you must click the **Apply** button at the bottom of the page.

LAN Segment: (Technician Level Only)

LAN – Selects the LAN index or identifier for each individual LAN on your network.

Note: If this option is enabled, you can create a separate Wi-Fi LAN for guests or other uses. If used, you can set up all of the "LAN Setup" and "Wireless Setup" parameters independently for each LAN.

LAN IP Settings:

IP Address – This field displays the IP address of your LAN.

Subnet Mask – This field displays the subnet mask of your LAN.

DHCP Server Settings:

Enable DHCP Server – Check this box to enable the use of a Dynamic Host Configuration Protocol (DHCP) Server on your network.

DHCP is a set of rules used by devices such as a computer, router, or network adapter to allow the device to request and obtain an IP address from a server which maintains a list of addresses available for use.

The DHCP server ensures that all IP addresses are unique, e.g., no IP address is assigned to a second device while the first device's assignment is valid (its lease has not expired).

Without DHCP, the IP addresses must be entered manually at each computer in an organization and a new IP address must be entered each time a computer moves to a new location on the network.

Start IP Address – Enter the starting address in the range of IP addresses that the DHCP Server can assign to a network device.

End IP Address – Enter the ending address in the range of IP addresses that the DHCP Server can assign to a network device.

Lease Time – Enter the lease time in seconds before the assigned IP address expires. (After the lease time is up, the Gateway automatically assigns the device a new dynamic IP address.)

DHCP uses the concept of a "lease" or amount of time that a given IP address is valid for a computer or other network device. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. Using very short leases, DHCP can dynamically reconfigure networks where there are more computers than available IP addresses, such as educational environments.

Domain Name – This field displays the domain name.

DNS Override:

Enable DNS Override – Check this box to replace the Domain Name System (DNS) server addresses provided by DHCP.

Primary DNS Server IP – Enter the IP address of the primary DNS server. The Gateway normally obtains DNS Server addresses through DHCP, but you can replace them if necessary. Your cable provider should provide this information.

Secondary DNS Server IP – Enter the IP address of the secondary DNS server. The Gateway normally obtains DNS Server addresses through DHCP, but you can replace them if necessary. Your cable provider should provide this information.

Tertiary DNS Server IP – Enter the IP address of the tertiary DNS server. The Gateway normally obtains DNS Server addresses through DHCP, but you can replace them if necessary. Your cable provider should provide this information.

DNS Relay:

Enable DNS Relay – Check this box to enable DNS Relay.

When DNS Relay is enabled, the Gateway acts as a DNS server, sends requests from connected devices to the configured public DNS servers, and caches the information for later access. When DNS relay is disabled, connected devices retrieve domain name/IP address information directly from the configured DNS servers.

NAT:

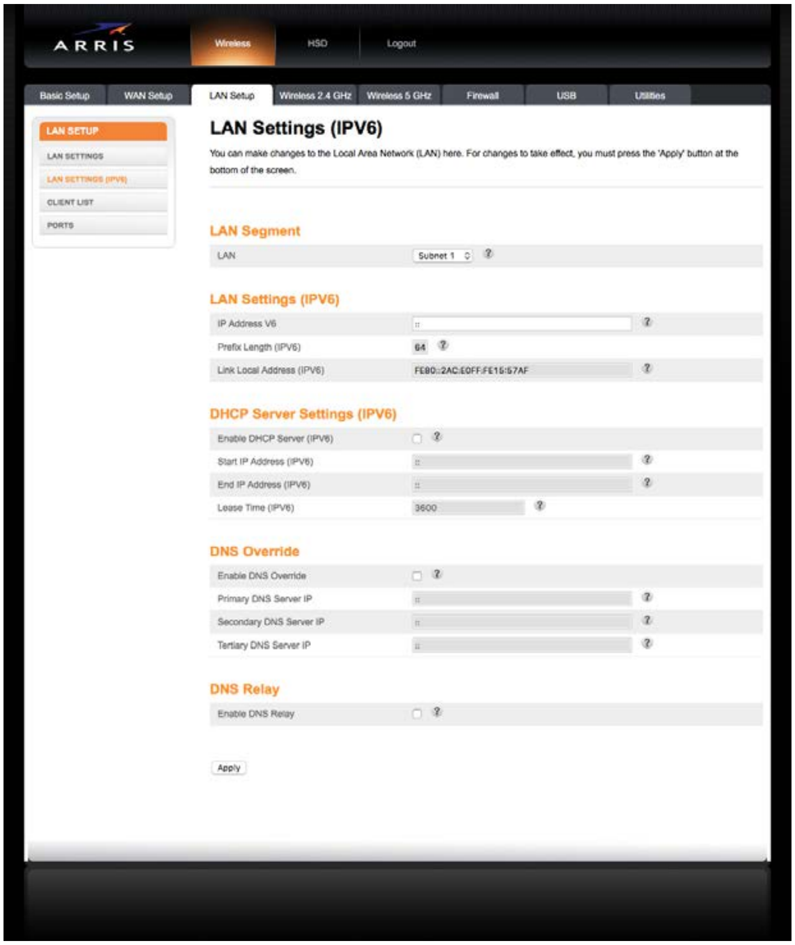
NAT Mode – Select the NAT Mode:

- Bridged – Data passes through the Gateway directly without any routing.
- Routed with NAT – The Gateway routes packets, and all the outgoing packets have Network Address Translation (NAT) applied.
- Routed without NAT – The Gateway routes packets without applying NAT.

UPnP:

Enable UPnP – Check this box to enable UPnP (Universal Plug and Play) on the Gateway.

LAN Setup – LAN Settings (IPV6)



LAN Settings (IPV6)

You can make changes to the Local Area Network (LAN) here. For changes to take effect, you must press the 'Apply' button at the bottom of the screen.

LAN Segment

LAN	Subnet 1

LAN Settings (IPV6)

IP Address V6	::
Prefix Length (IPV6)	64
Link Local Address (IPV6)	FE80::2AC:E0FF:FE15:57AF

DHCP Server Settings (IPV6)

Enable DHCP Server (IPV6)	□
Start IP Address (IPV6)	::
End IP Address (IPV6)	::
Lease Time (IPV6)	3600

DNS Override

Enable DNS Override	□
Primary DNS Server IP	::
Secondary DNS Server IP	::
Tertiary DNS Server IP	::

DNS Relay

Enable DNS Relay	□

This screen configures LAN side support for IPV6. You can make changes to the Local Area Network (LAN) configuration here. For changes to take effect, you must click the **Apply** button.

LAN Segment: (Technician Level Only)

LAN – Selects the LAN index or identifier for each individual LAN on your network.

Note: You can optionally set up the system so that there is more than one LAN in your network. This is most useful for commercial applications not home use. All of the "LAN Setup" and "Wireless Setup" configuration parameters can be set independently for each individual LAN.

LAN Settings (IPV6):

IP Address (IPV6) – The IPV6 address of your LAN. An IPV6 address has eight groups of four hexadecimal digits (0-9, a-f). The groups are separated by colons (:) e.g. 2001:0db8:85a3:0000:0000:8a2e:0370:7334. A double colon (::) is shorthand for an address or group of all zeros.

Prefix Length V6 – The number of bits in an IPv6 address that specify its network. The remaining bits specify a local address.

Link Local Address (IPV6) – IPV6 address that can be used only on this network.

DHCP Server Settings (IPV6):

Enable DHCP Server (IPV6) – Check this box to enable the use of a V6 Dynamic Host Configuration Protocol (DHCP) Server on your network.

DHCP is a set of rules used by devices such as a computer, router, or network adapter to allow the device to request and obtain an IP address from a server which maintains a list of addresses available for use.

The DHCP server ensures that all IP addresses are unique, e.g., no IP address is assigned to a second device while the first device's assignment is valid (its lease has not expired).

Without DHCP, the IP addresses must be entered manually at each computer in an organization and a new IP address must be entered each time a computer moves to a new location on the network.

Start IP Address (IPV6) – Enter the starting address in the range of IPV6 addresses that the DHCP Server can assign to a network device.

End IP Address (IPV6) – Enter the ending address in the range of IPV6 addresses that the DHCP Server can assign to a network device.

Lease Time V6 – Enter the lease time in seconds before the assigned IPV6 address expires. (After the lease time is up, the Gateway automatically assigns the device a new dynamic IP address.)

DHCP uses the concept of a "lease" or amount of time that a given IP address is valid for a computer or other network device. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. Using very short leases, DHCP can dynamically reconfigure networks where there are more computers than available IP addresses, such as educational environments.

DNS Override:

Enable DNS Override – Check this box to enable Domain Name System (DNS) Override.

Primary DNS Server IP – Enter the IP address of the primary DNS server. The Gateway normally obtains DNS Server addresses through DHCP, but you can replace them if necessary. Your cable provider should provide this information.

Secondary DNS Server IP – Enter the IP address of the secondary DNS server. The Gateway normally obtains DNS Server addresses through DHCP, but you can replace them if necessary. Your cable provider should provide this information.

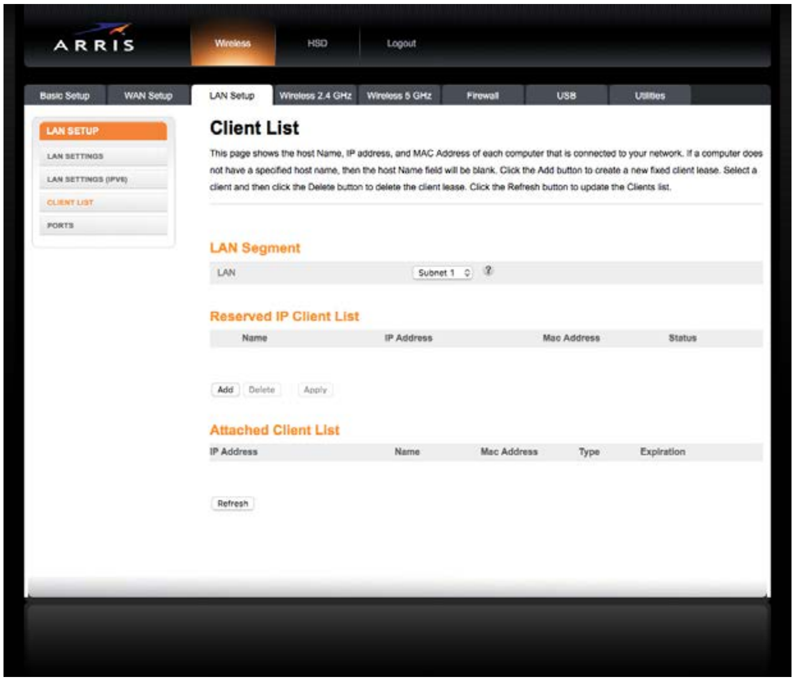
Tertiary DNS Server IP – Enter the IP address of the tertiary DNS server. The Gateway normally obtains DNS Server addresses through DHCP, but you can replace them if necessary. Your cable provider should provide this information.

DNS Relay:

Enable DNS Relay – Check this box to enable DNS Relay.

When DNS Relay is enabled, the Gateway acts as a DNS server, sends requests from connected devices to the configured public DNS servers, and caches the information for later access. When DNS relay is disabled, connected devices retrieve domain name/IP address information directly from the configured DNS servers.

LAN Setup – Client List



Client List

This page shows the host Name, IP address, and MAC Address of each computer that is connected to your network. If a computer does not have a specified host name, then the host Name field will be blank. Click the Add button to create a new fixed client lease. Select a client and then click the Delete button to delete the client lease. Click the Refresh button to update the Clients list.

LAN Segment

LAN: Subnet 1

Reserved IP Client List

Name	IP Address	Mac Address	Status

Attached Client List

IP Address	Name	Mac Address	Type	Expiration

This page shows the host Name, IP address, and MAC Address of each computer that is connected to your network. If a computer does not have a specified host name, then the host Name field is blank.

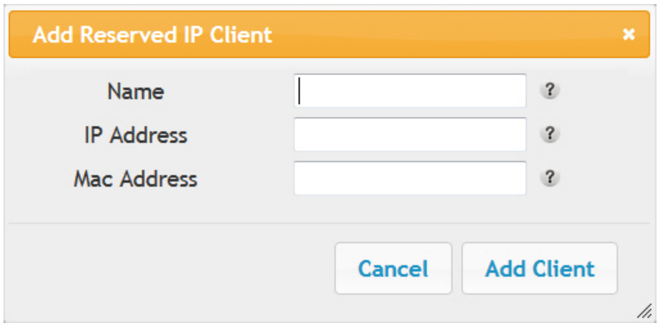
LAN Segment: (Technician Level Only)

LAN – Selects the LAN index or identifier for each individual LAN on your network.

Note: You can optionally set up the system so that there is more than one LAN in your network. This is most useful for commercial applications, not home use. All of the "LAN Setup" and "Wireless Setup" configuration parameters can be set independently for each individual LAN.

Reserved IP Client List:

Click the **Add** button to create a new fixed client lease.



Name – Enter a name for the client.

IP Address – Enter the client’s IP address.

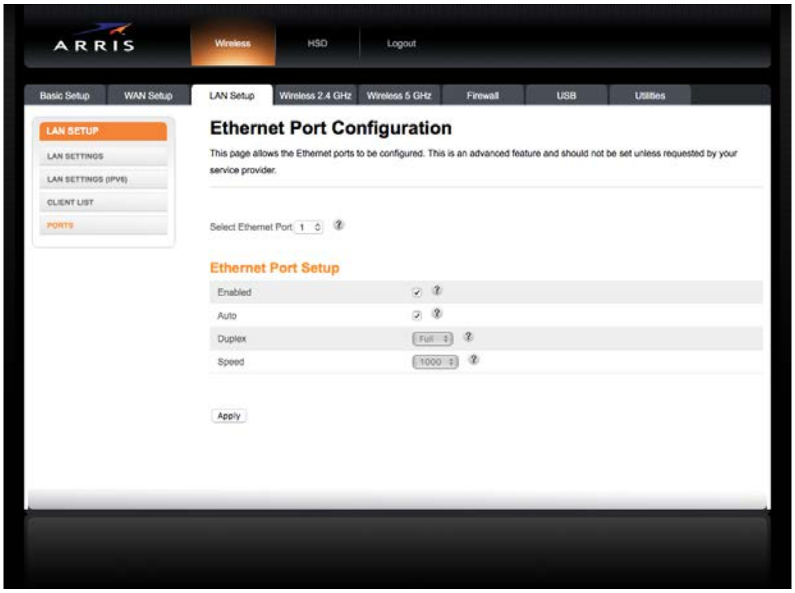
MAC Address – Enter the client’s MAC address.

Select a client and then click the **Delete** button to delete the client lease.

Attached Client List:

Click the **Refresh** button to update the client list.

LAN Setup – Ports



Ethernet Port Configuration

This page allows the Ethernet ports to be configured. This is an advanced feature and should not be set unless requested by your service provider.

Select Ethernet Port 1

Ethernet Port Setup

Enabled	☑
Auto	☑
Duplex	Full
Speed	1000

This page allows you to configure the Ethernet ports. This is an advanced feature; avoid changing these settings unless requested by your cable provider.

Select Ethernet Port – Select the Ethernet port to be configured.

Ethernet Port Setup: (Technician Level Only)

Enabled – Check this box to enable the selected port. Leave this checked unless instructed by support.

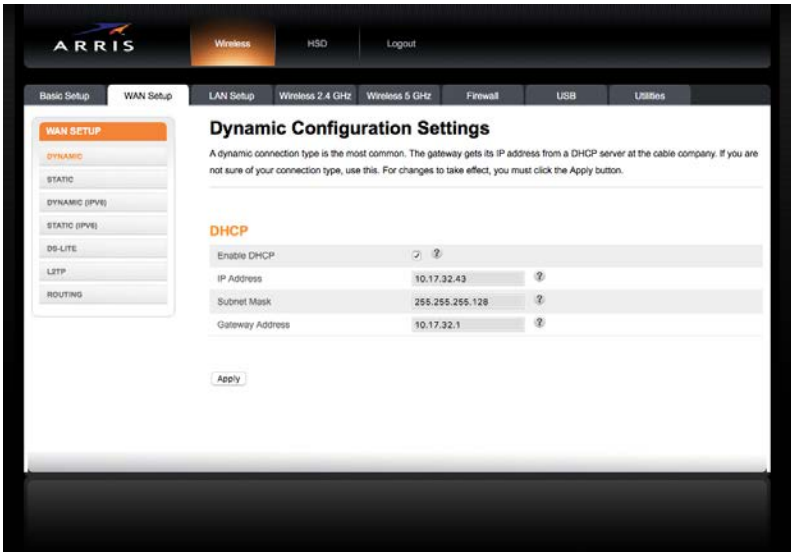
Auto – Check this box to enable automatic configuration. When enabled, the port automatically sets its duplex mode and speed. In most cases, this should be left enabled.

Duplex – If Auto is not enabled, select the communication mode for the port. Can be set to Full Duplex or Half Duplex.

Speed – If Auto is not enabled, select the speed for the port. Can be set to 10 Mbps, 100 Mbps, or 1,000 Mbps.

WAN Setup

WAN Setup – Dynamic Configuration Settings



Dynamic Configuration Settings

A dynamic connection type is the most common. The gateway gets its IP address from a DHCP server at the cable company. If you are not sure of your connection type, use this. For changes to take effect, you must click the Apply button.

DHCP

Enable DHCP	☑
IP Address	10.17.32.43
Subnet Mask	255.255.255.128
Gateway Address	10.17.32.1

A dynamic connection type is the most common. The router gets its IP address from a DHCP server at the cable company. If you are not sure of your connection type, use this type. For changes to take effect, click the **Apply** button.

Dynamic Configuration:

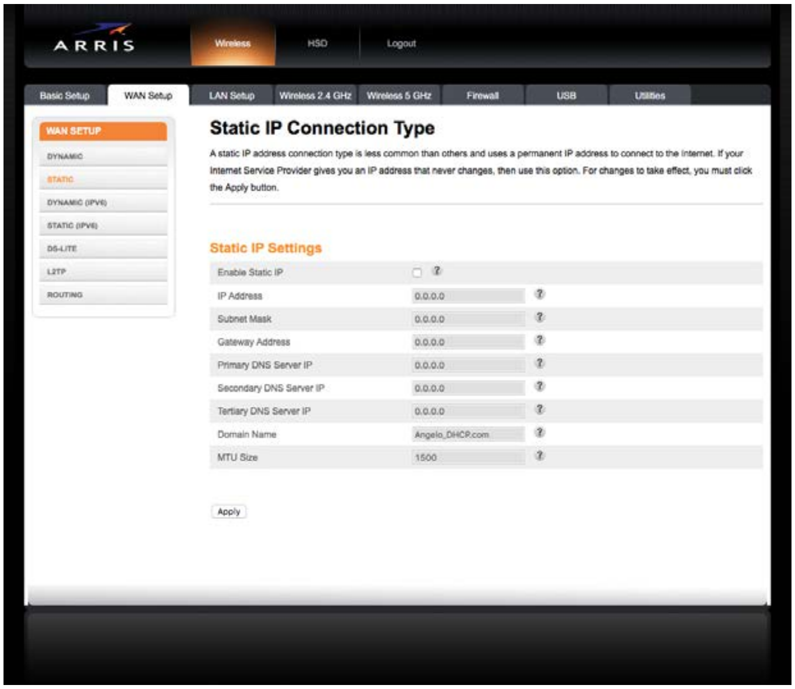
Enable DHCP – Check this box to enable a DHCP connection for your system.

IP Address – This field displays the IP address.

Subnet Mask – This field displays the subnet mask.

Gateway Address – This field displays the gateway address.

WAN Setup – Static IP Connection Type



Static IP Connection Type

A static IP address connection type is less common than others and uses a permanent IP address to connect to the Internet. If your Internet Service Provider gives you an IP address that never changes, then use this option. For changes to take effect, you must click the Apply button.

Static IP Settings

Enable Static IP	□
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway Address	0.0.0.0
Primary DNS Server IP	0.0.0.0
Secondary DNS Server IP	0.0.0.0
Tertiary DNS Server IP	0.0.0.0
Domain Name	Angelo_DHCP.com
MTU Size	1500

Apply

A static IP address connection type is less common than others and uses a permanent IP address to connect to the Internet. If your Internet Service Provider gives you an IP address that never changes, then use this option. For changes to take effect, click the **Apply** button.

Static IP Settings:

Enable Static IP - Check this box to enable a static IP address connection for your system.

IP Address – Enter the IP address assigned by your ISP or static IP operation.

Subnet Mask – Enter the subnet mask assigned for your device by your ISP or static IP operation.

Gateway Address – Enter the gateway address assigned for your device by your cable provider for static IP operation.

Primary DNS Server IP – Enter the IP address of the primary DNS server. Your cable provider furnishes this information.

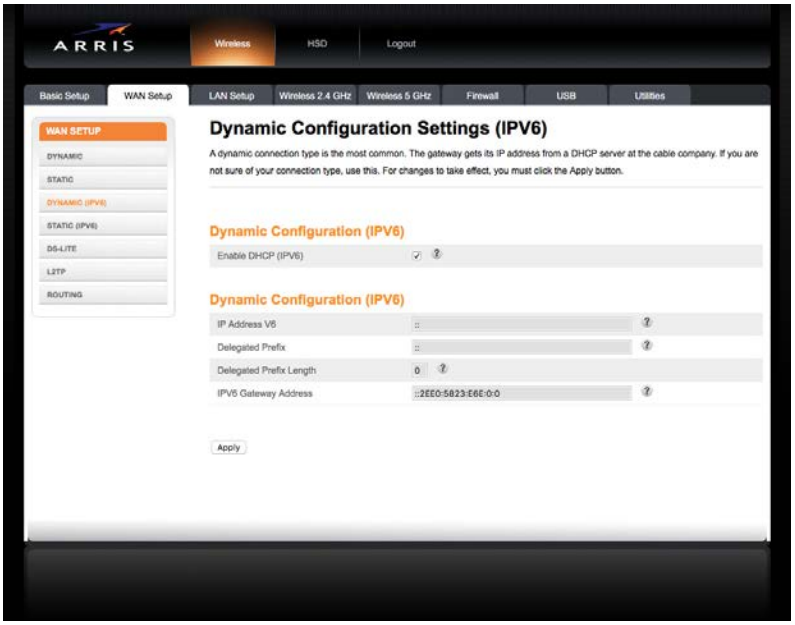
Secondary DNS Server IP – Enter the IP address of the secondary DNS server. Your cable provider furnishes this information.

Tertiary DNS Server IP – Enter the IP address of the tertiary DNS server. Your cable provider furnishes this information.

Domain Name – The domain name for your client devices. If your cable provider has not given you a domain name to use, you can enter your own here.

MTU Size – This field displays the size of the maximum transmission unit (MTU) for the network connection. The default value is 1500. Advanced option – do not change unless instructed by your Service Provider.

WAN Setup – Dynamic Configuration Settings (IPV6)



Dynamic Configuration Settings (IPV6)

A dynamic connection type is the most common. The gateway gets its IP address from a DHCP server at the cable company. If you are not sure of your connection type, use this. For changes to take effect, you must click the Apply button.

Dynamic Configuration (IPV6)

Enable DHCP (IPV6) ☑

Dynamic Configuration (IPV6)

IP Address V6 ::

Delegated Prefix ::

Delegated Prefix Length 0

IPV6 Gateway Address ::2EE0:5823:E6E:0:0

This screen enables a DHCPv6 configured IPV6 stack. A dynamic connection type is the most common.

The router gets its IP address from a DHCP server at the cable company. If you are not sure of your connection type, use this type. For changes to take effect, you must click the **Apply** button.

Dynamic Configuration (IPV6):

Enable DHCP (IPV6) – Check this box to enable a DHCP (IPV6) connection for your system.

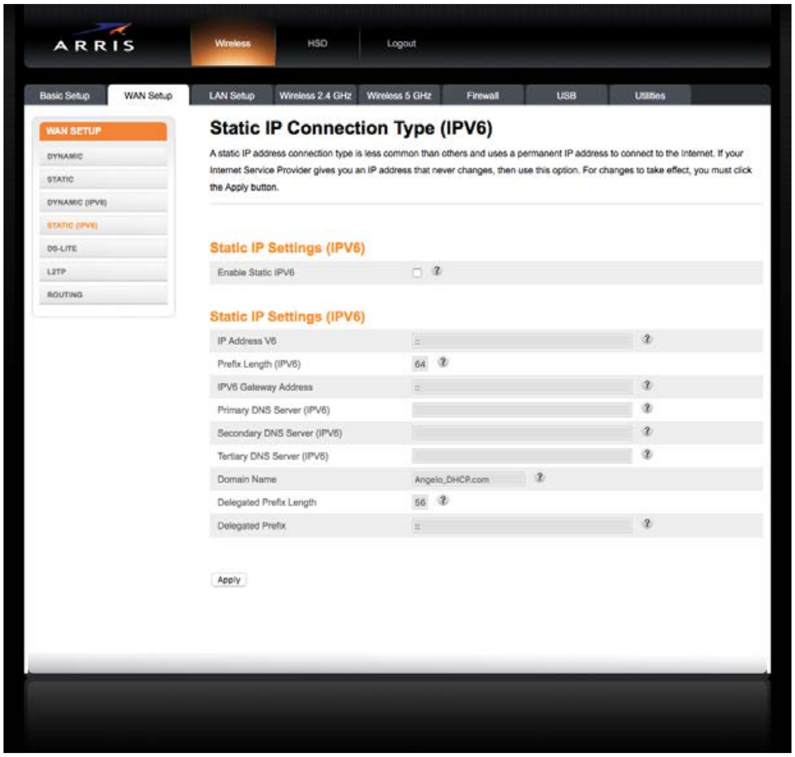
IP Address V6 – The IPV6 address automatically assigned by the MSO. An IPV6 address has eight groups of four hexadecimal digits (0-9, a-f). The groups are separated by colons (:) e.g. 2001:0db8:85a3:0000:0000:8a2e:0370:7334. A double colon (::) is shorthand for an address of all zeros.

Delegated Prefix – The assigned IPV6 prefix to be used by addresses allocated in the local network.

Delegated Prefix Length – The assigned IPV6 prefix length.

IPV6 Gateway Address – The gateway address.

WAN Setup – Static IP Connection Type (IPV6)



Static IP Connection Type (IPV6)

A static IP address connection type is less common than others and uses a permanent IP address to connect to the Internet. If your Internet Service Provider gives you an IP address that never changes, then use this option. For changes to take effect, you must click the Apply button.

Static IP Settings (IPV6)

Enable Static IPV6	□ ?

Static IP Settings (IPV6)

IP Address V6	:: ?
Prefix Length (IPV6)	64 ?
IPV6 Gateway Address	:: ?
Primary DNS Server (IPV6)	?
Secondary DNS Server (IPV6)	?
Tertiary DNS Server (IPV6)	?
Domain Name	Angelo_DHCP.com ?
Delegated Prefix Length	56 ?
Delegated Prefix	:: ?

Apply

This screen enables a statically configured IPV6 stack. A static IP address connection type is less common than others and uses a permanent IP address to connect to the Internet. If your Internet Service Provider gives you an IP address that never changes, then use this option. For changes to take effect, you must click the **Apply** button.

Static IP Settings (IPV6):

Enable Static IPV6 - Check this box to enable a static IPV6 address connection for your system.

IP Address V6 – Enter the IPV6 address assigned by your ISP or static IP operation. An IPV6 address has eight groups of four hexadecimal digits (0-9, a-f). The groups are separated by colons (:) e.g. 2001:0db8:85a3:0000:0000:8a2e:0370:7334. A double colon (::) is shorthand for an address of all zeros.

Prefix Length (IPV6) – The length of the network portion of this address.

IPV6 Gateway Address – Enter the gateway address assigned for your device by your ISP or static IP operation.

Primary DNS Server (IPV6) – Enter the IPV6 address of the primary DNS server. The Gateway normally obtains DNS Server addresses through DHCP, but you can replace them if necessary.

Secondary DNS Server (IPV6) – Enter the IPV6 address of the secondary DNS server. The Gateway normally obtains DNS Server addresses through DHCP, but you can replace them if necessary.

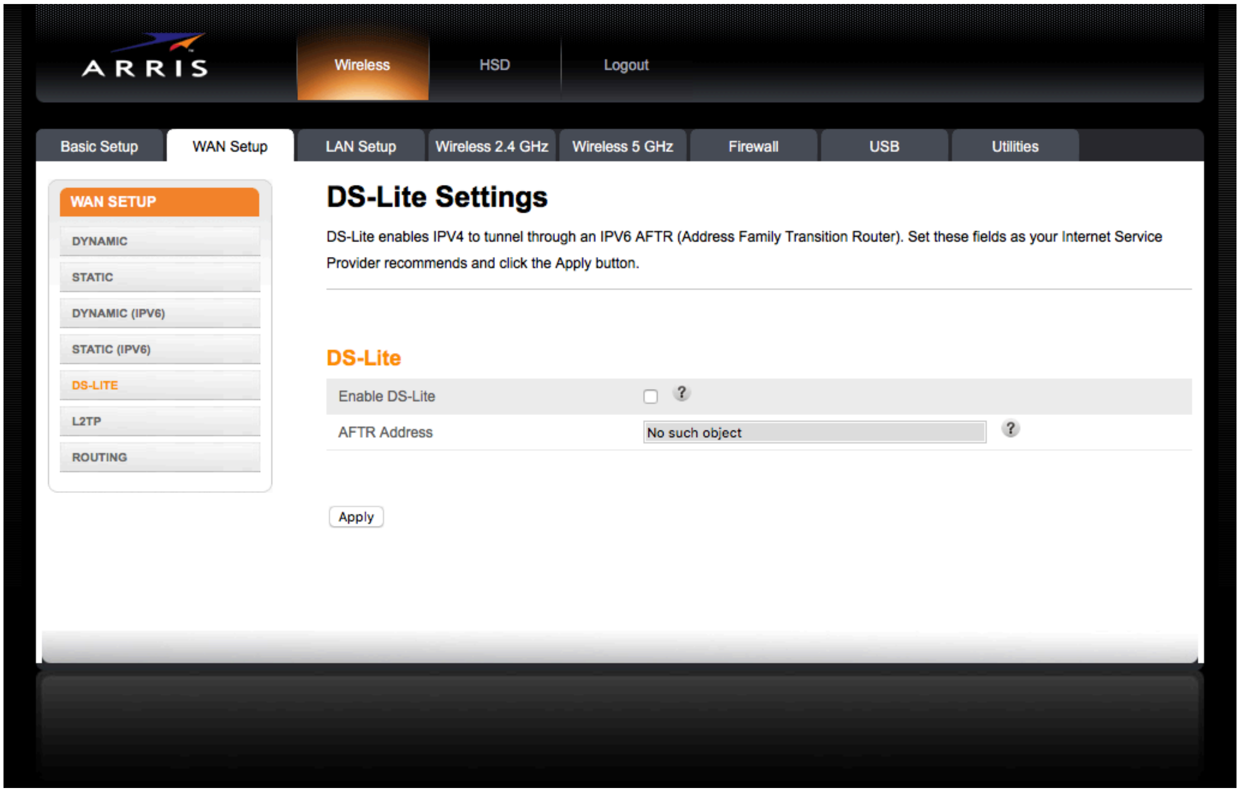
Domain Name – The domain name for your client devices. If your cable provider has not given you a domain name to use, you can enter your own here.

Delegated Prefix Length – The length of the network portion of the IPV6 addresses to be allocated to local clients.

Delegated Prefix – The network portion of the IPV6 addresses to be allocated to local clients.

WAN Setup - DS-Lite Settings

Note: This screen is available only on certain Gateway models.



DS-Lite Settings

DS-Lite enables IPV4 to tunnel through an IPV6 AFTR (Address Family Transition Router). Set these fields as your Internet Service Provider recommends and click the Apply button.

DS-Lite

Enable DS-Lite □ ?

AFTR Address: No such object ?

Gateway models that support DS-Lite can use IPv4 addresses on an IPv6 network. Enter the information provided by your cable operator as described below, and click **Apply**.

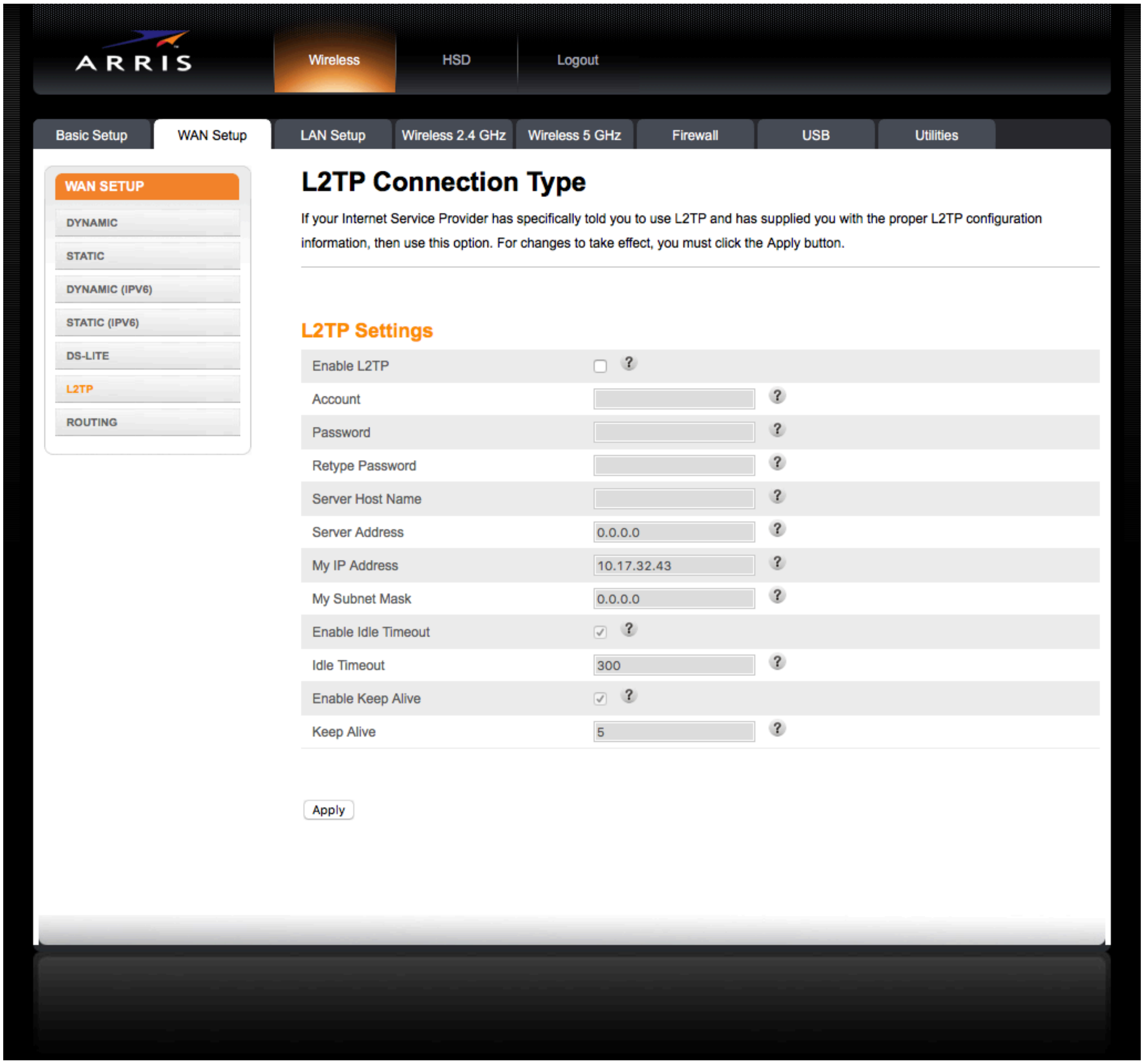
DS-Lite:

Enable DS-Lite – check this box to enable DS-Lite on your Gateway.

AFTR Address – enter the IPv6 address of the Address Family Transition Router (AFTR) in this field.

WAN Setup - L2TP

Note: This screen is available only on certain Gateway models.



L2TP Connection Type

If your Internet Service Provider has specifically told you to use L2TP and has supplied you with the proper L2TP configuration information, then use this option. For changes to take effect, you must click the Apply button.

L2TP Settings

Enable L2TP	□
Account	
Password	
Retype Password	
Server Host Name	
Server Address	0.0.0.0
My IP Address	10.17.32.43
My Subnet Mask	0.0.0.0
Enable Idle Timeout	☑
Idle Timeout	300
Enable Keep Alive	☑
Keep Alive	5

If your cable operator uses L2TP and provides configuration, enter that information in this screen and click **Apply**.

L2TP Settings:

Enable L2TP – Check this box to enable L2TP on this Gateway.

Account – Enter the account ID provided by your cable operator.

Password – Enter the password provided by your cable operator.

Retype Password – Retype the password to confirm proper entry.

Server Host Name – Enter the name of the server.

My IP Address – Enter the IP address provided by your cable company.

My Subnet Mask – Enter the subnet mask provided by your cable company.

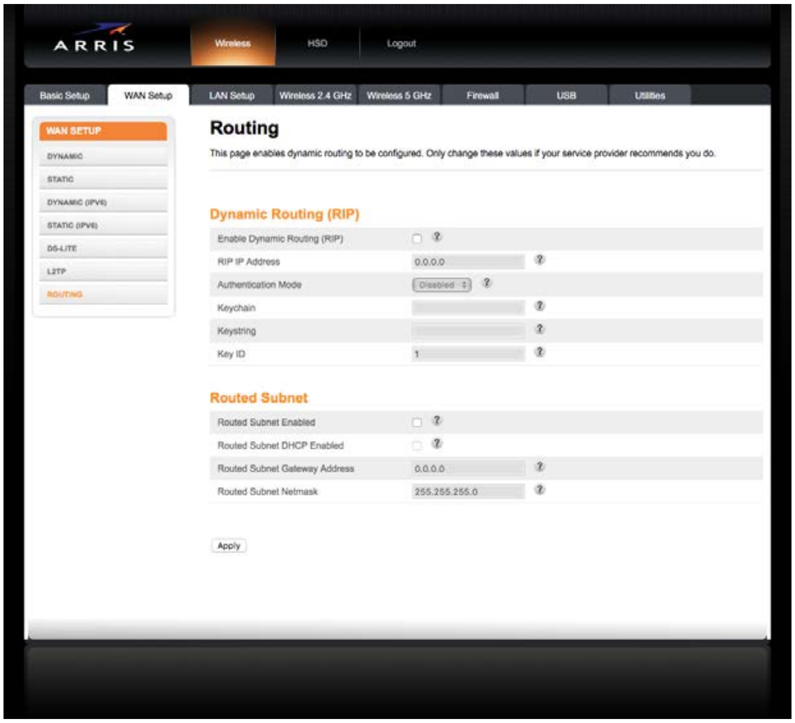
Enable Idle Timeout – Check this box to enable idle timeout.

Idle Timeout – The time, in seconds, the connection can remain idle before the Gateway disconnects.

Enable Keep Alive – Check this box to enable keep-alive.

Keep Alive – The time, in seconds, the Gateway checks the connection and attempts to re-connect if it is down.

WAN Setup – Routing (Technician Level Only)



Routing

This page enables dynamic routing to be configured. Only change these values if your service provider recommends you do.

Dynamic Routing (RIP)

Enable Dynamic Routing (RIP)	□
RIP IP Address	0.0.0.0
Authentication Mode	Disabled
Keychain	
Keystring	
Key ID	1

Routed Subnet

Routed Subnet Enabled	□
Routed Subnet DHCP Enabled	□
Routed Subnet Gateway Address	0.0.0.0
Routed Subnet Netmask	255.255.255.0

This screen allows dynamic routing to be enabled and configured. Only change these values if your service provider recommends that you do so.

Dynamic Routing (RIP):

Enable Dynamic Routing (RIP) – Check this box to enable Dynamic Routing on your system.

RIP IP Address – Enter the RIP IP address.

Authentication Mode – Select Disabled, Text, or MD5 as appropriate for your network.

Keychain – For MD5, enter the keychain name.

Keystring – For Text/MD5, enter the keystring name.

Key ID – For MD5, enter the RIP authentication key ID.

Routed Subnet:

Routed Subnet Enabled – Check this box to route the selected subnet. When checked, the Gateway advertises the RIP routed subnet network IP address with the next hop as the CM IP address.

Routed Subnet DHCP Enabled – Check this box to provide DHCP to devices on this network. When checked, the Gateway starts a public DHCP server for the routed subnet. If disabled, all LAN-based CPE devices need to use public static IP addresses.

Routed Subnet Gateway Address – Enter the gateway IP address for the routable subnet—that is, the address of the router that handles traffic between this subnet and the rest of the Internet.

Routed Subnet Netmask – Enter the subnet mask used for the routed subnet.

WAN Setup – Configuring Dynamic Routing (RIP) – (Technician Level Only)

Enabling Dynamic Routing or RIP (Router Information Protocol) allows your router to operate in a network environment with other routers. This is primarily used for office environments or multiple dwelling units where a network with existing routers already exists. Only enable Dynamic Routing if your service provider recommends that you do so.

Requirements

To successfully configure RIP, you must have:

- A Routed Subnet Netmask and Routed Subnet Gateway Address assigned by your service provider.
- A static IP address for all devices on your local network, or a separate DHCP server to assign addresses.

To enable Dynamic Routing:

1. Access and log into the configuration interface.
2. Click the **WAN Setup** tab.
3. Click **Routing** in the side menu to display the routing screen.
4. Click the **Enable Dynamic Routing (RIP)** checkbox.

Note: See *WAN Setup* for specific instructions on setting the various dynamic routing configuration parameters.

5. After setting the necessary configuration parameters, click the **Apply** button at the bottom of the screen.

WAN Setup – Configuring Dynamic Routing (RIPng) – (Technician Level Only)

Note: Not available on all models.

Enabling Dynamic Routing for IPV6 or RIPng (Router Information Protocol next generation) allows your router to operate in a network environment with other routers. This is primarily used for office environments or multiple dwelling units where a network with existing routers already exists. Only enable Dynamic Routing if your service provider recommends that you do so.

Requirements

To successfully configure RIPng, you must have:

- A static IP address assigned by our service provider.
- You must either assign a static IP address to all devices on your local network or use a DHCP server to assign addresses.

To enable Dynamic Routing for IPV6:

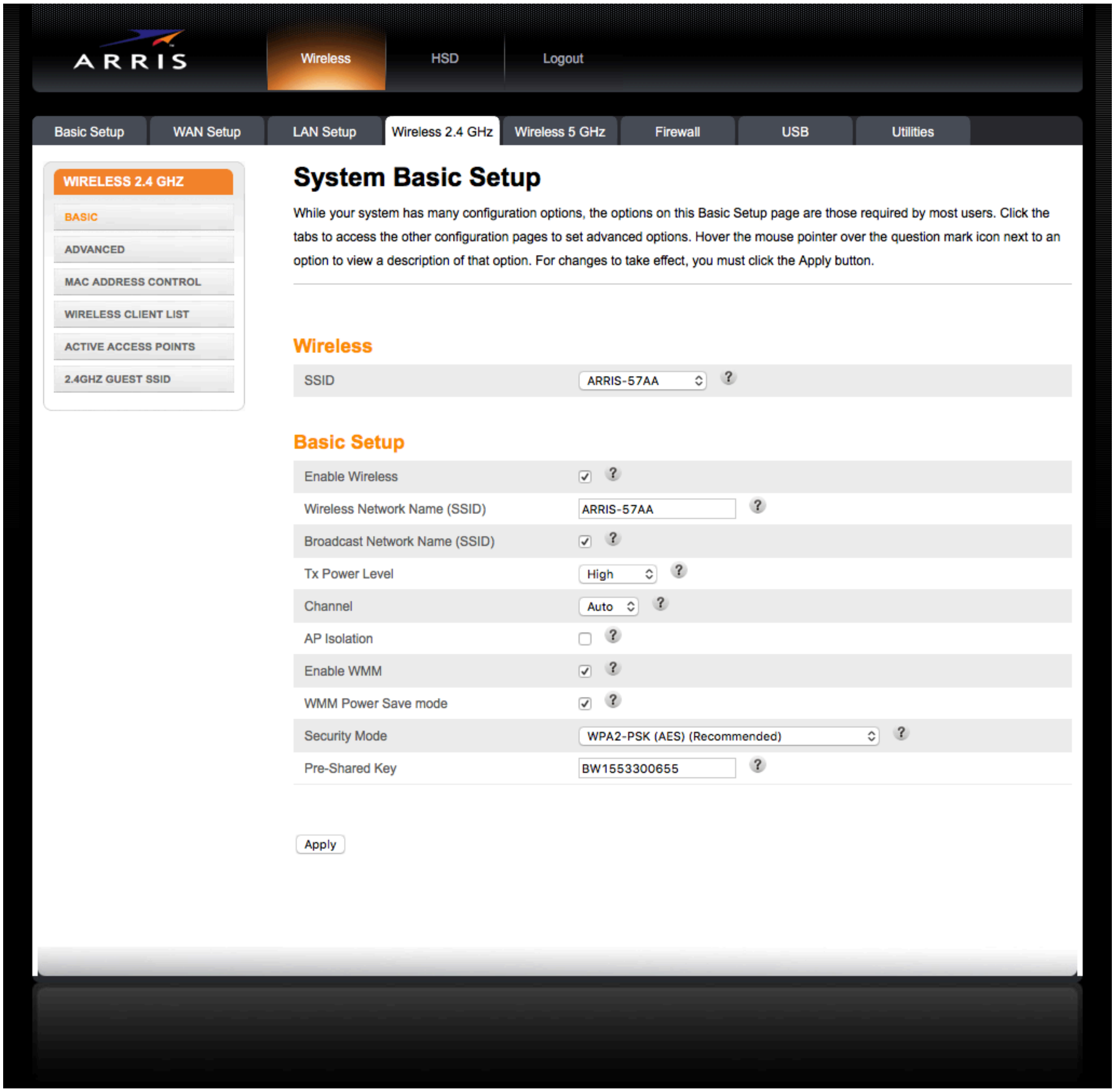
1. Access and log into the configuration interface.
2. Click the **WAN Setup** tab.
3. Click **Routing (RIPng)** in the side menu to display the RIPng configuration screen.
4. Click the **Enable Dynamic Routing** checkbox.

Note: See *WAN Setup – Routing (Technician Level Only)* for specific instructions on setting the various dynamic routing configuration parameters.

5. After setting the necessary configuration parameters, click the **Apply** button at the bottom of the screen.

Wireless Setup

Wireless 2.4 GHz – System Basic Setup



System Basic Setup

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

Wireless

SSID	ARRIS-57AA

Basic Setup

Enable Wireless	☑
Wireless Network Name (SSID)	ARRIS-57AA
Broadcast Network Name (SSID)	☑
Tx Power Level	High
Channel	Auto
AP Isolation	□
Enable WMM	☑
WMM Power Save mode	☑
Security Mode	WPA2-PSK (AES) (Recommended)
Pre-Shared Key	BW1553300655

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

Wireless: (Technician Level Only)

SSID – Sets the SSID for each individual LAN on your network.

Note: If this option is enabled, you can create a separate Wi-Fi LAN for guests or other uses. If used, you can set up all of the "LAN Setup" and "Wireless Setup" parameters independently for each LAN.

Basic Setup:

Enable Wireless – Check this box to enable the wireless network on your system.

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

Broadcast Network Name (SSID) – Check this box to allow the SSID to be broadcast by the router. If enabled, your SSID could be obtained allowing unauthorized access to your network. If you would like others not to see your access point, uncheck the checkbox to hide the SSID.

Tx Power Level – Sets the transmit power level, which is the output power level of the wireless radio. Can be set to High, Medium, or Low.

Channel – Sets a communications channel for your router. The default setting is "Auto", in which the router selects a channel with the least amount of interference to use. For 2.4 GHz, if you manually select a channel, the best channels are 1, 6, and 11, since these channels do not overlap. If another unit is operating in the area, choose a channel that is farthest away from the channel that unit uses. For example, if one is using channel 11, set yours to channel 1. For 5 GHz, choose a channel that is farthest away from the channel used by any other unit operating in the area. If you experience interference or poor performance on a particular channel, try a different channel.

AP Isolation – Check this box to enable AP isolation. When enabled, each of your wireless clients is in its own virtual network and cannot communicate directly with one another. This may be useful if you have many guests using your network.

Enable WMM – Check this box to enable Wi-Fi Multimedia (WMM) functionality. Enabling WMM can help control latency and jitter when transmitting multimedia content over a wireless connection.

This quality of service mechanism uses four access categories, which in order of priority are: voice, video, best effort, and background. This ensures that applications with low tolerance for latency and jitter are treated with higher priority than less-sensitive data applications. WMM sets different wait times for the four categories in order to provide priority network access for applications that are less tolerant of packet delays.

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.

Security Mode – Sets the security mode for your router. Can be set to:

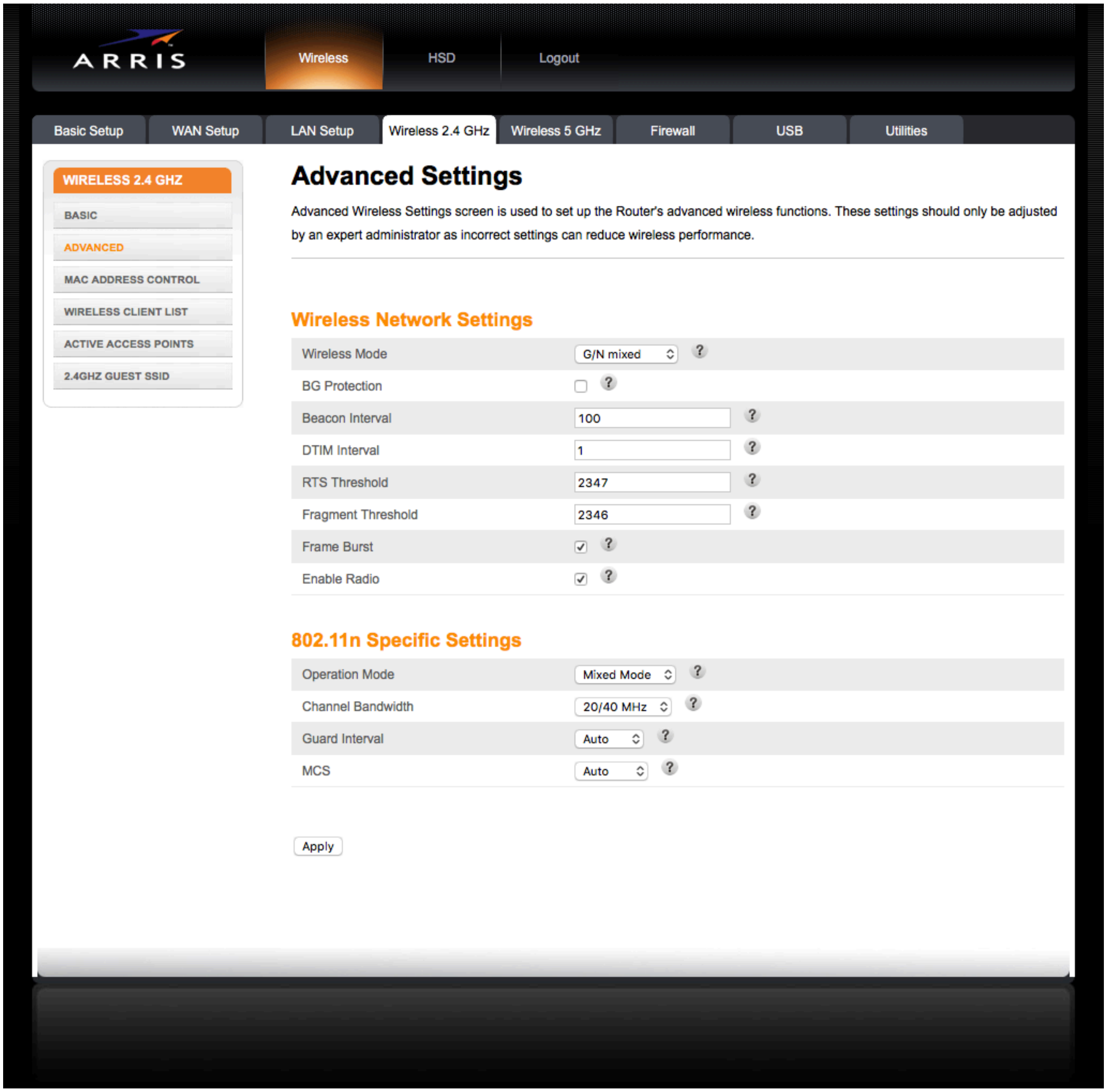
- OPEN (no security)
- WEP (64/128) (Wired Equivalency Privacy – 64/128) (poor security)

- WPA/WPA2-PSK (TKIP/AES) (Wi-Fi Protected Access/Wi-Fi Protected Access 2 – Pre-Shared Key – TKIP/AES encryption) (most compatible)
- WPA2-PSK (AES) (Wi-Fi Protected Access 2 – Pre-Shared Key – AES encryption) (recommended)
- WPA Enterprise
- WPA2 Enterprise.

802.11n performance is only available in Open mode, or WPA2 with AES encryption mode.

Pre-Shared Key – Sets your WPA Pre-Shared Key. This text string is used to generate a unique set of encryption keys for your network. Enter a text string in this field. The key can be either ASCII (text) or Hex (hexadecimal). An ASCII text key can be from 8 to 63 characters long. Valid characters are numbers "0" through "9" and letters "a" through "z", and any printable ASCII characters. A hexadecimal key must be 64 characters long. Valid characters are numbers "0" through "9" and letters "a" through "f".

Wireless 2.4 GHz – Advanced Settings



Advanced Settings

Advanced Wireless Settings screen is used to set up the Router's advanced wireless functions. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.

Wireless Network Settings

Wireless Mode	G/N mixed
BG Protection	☐
Beacon Interval	100
DTIM Interval	1
RTS Threshold	2347
Fragment Threshold	2346
Frame Burst	☑
Enable Radio	☑

802.11n Specific Settings

Operation Mode	Mixed Mode
Channel Bandwidth	20/40 MHz
Guard Interval	Auto
MCS	Auto

The Advanced Settings page sets up the router’s advanced wireless functions. These settings should only be adjusted by an expert administrator since incorrect settings can reduce wireless performance. For changes to take effect, you must click the **Apply** button.

Wireless Network Settings:

> **Wireless Mode** – Sets the wireless mode. Options are: B/G mixed, B only, G only, N only, G/N mixed, and B/G/N mixed. Select the proper mode to support all of the wireless devices that connect to your router. 802.11b supports bandwidth up to 11 Mb/s. 802.11g supports bandwidth up to 54 Mb/s. 802.11n supports bandwidth up to 300 Mb/s.

BG Protection – Sets the BG protection mode. Options are OFF or AUTO. Default is OFF (checkbox unchecked).

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 OFF (unchecked) for maximum performance.

Note: 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 (OFF). The Gateway auto-detects 802.11b devices and sets the feature accordingly when the BG protection checkbox is checked (AUTO).

Beacon Interval – Sets the time interval between beacon transmissions, in milliseconds. The router uses these transmissions to synchronize the wireless network and its client devices. For best compatibility, leave the Beacon Interval at the default 100ms setting. The allowable setting range is from 20 to 1024ms.

DTIM Interval – Sets the DTIM (Delivery Traffic Indication Message) Interval. The DTIM Interval informs the wireless client devices of the next available window for listening to broadcast and multicast messages. When the router sends a DTIM beacon the client devices hear the beacon and then listen for the messages. For best compatibility, leave the DTIM Interval at the default 1ms setting. The allowable range is from 1 to 255 ms.

RTS Threshold – Sets the packet size limit. When the threshold is passed, the ready to send/clear to send (RTS/CTS) function is invoked. The default setting is 2347 bytes. The allowable setting range is from 1 to 2347 bytes.

Fragment Threshold – Sets the fragmentation threshold. This threshold should be set to equal the maximum Ethernet frame size allowable on the link including overhead. Setting a lower threshold can damage data throughput since large frames could be fragmented and/or collisions could occur. The default setting is 2346. The allowable setting range is from 256 to 2346 bytes.

Frame Burst – Check this box to enable Frame Burst on your network. Frame Bursting is a transmission technique that increases the throughput of point-to-point 802.11a, b, or g links by reducing the overhead associated with the wireless transmissions. This results in the ability to support higher data throughput in mixed and uniform networks. It can, however, result in unfair allocation of airtime where there are a mix of client devices on the network, of which only some support Frame-Bursting.

WMM Power Save Mode – Check this box to enable WMM Power Save Mode. WMM Power Save delivery is a more efficient power management method than legacy 802.11 power save polling.

Enable Radio (Technician level only) – Check this box to enable or disable the Wi-fi radio.

802.11n Specific Settings:

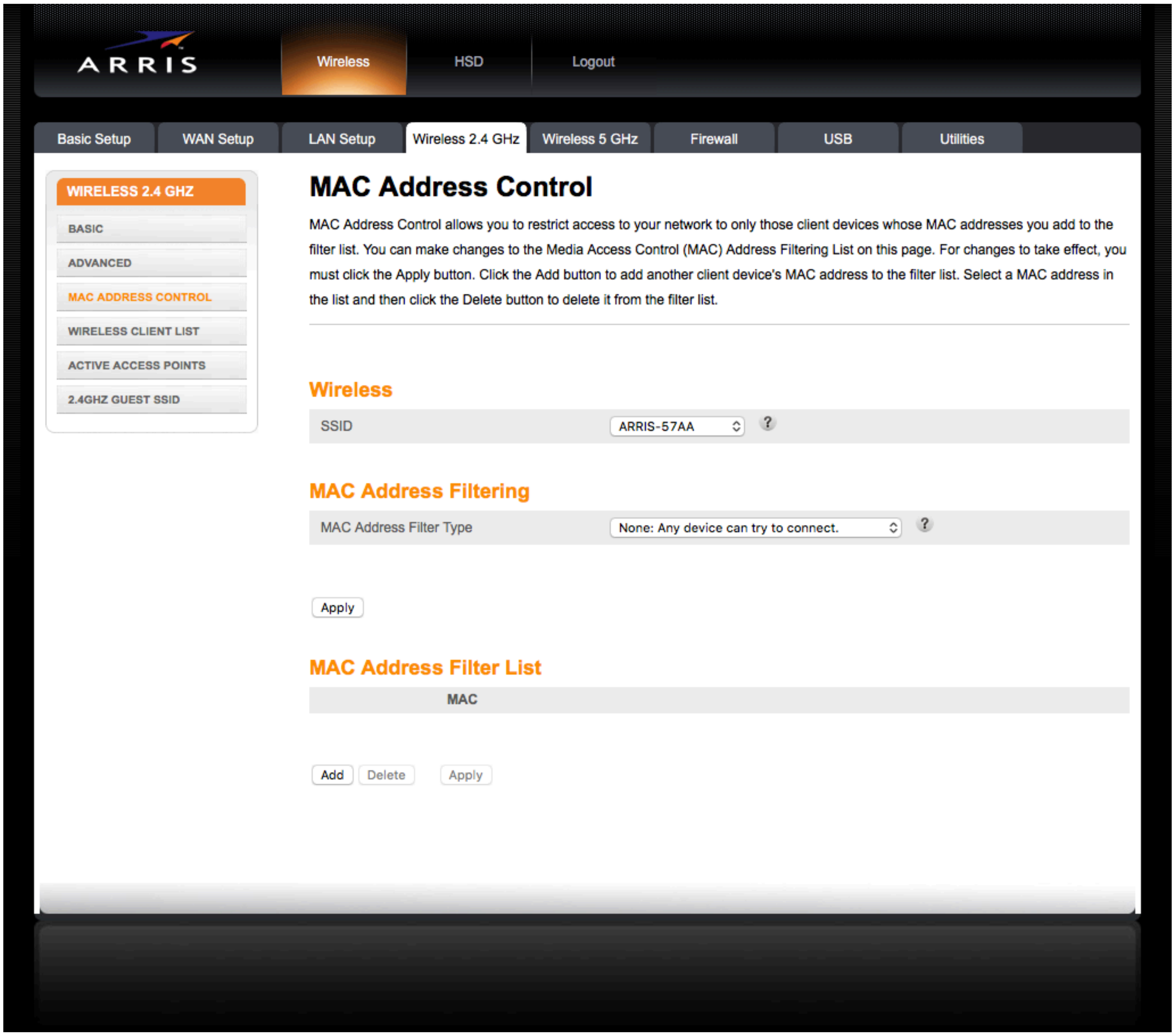
Operation Mode – Sets the 802.11n Operation Mode. Options are Mixed Mode or Greenfield. The default, Mixed Mode, is for networks with a mix of 802.11a/b/g/n client devices. The optional Greenfield mode improves efficiency of networks using only 802.11n devices by eliminating support for the 802.11a/b/g client devices.

Channel Bandwidth – Sets the 802.11n Channel Bandwidth. Options are 20 MHz or 20/40 MHz. The default setting is 20/40 MHz. If your wireless network is in a very clean RF environment, setting the Channel Bandwidth to 20/40 increases throughput by "bonding" two channels. However, if there are any other wireless routers or access points within range of the Gateway, it allocates 20 MHz bandwidth regardless of this setting. This is a Wi-fi Alliance requirement. (You can verify the channel bandwidth by using the previously mentioned wireless network scanning software, MetaGeek's inSSIDer.)

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).

MCS – Sets the 802.11n Modulation and Coding Scheme to be used. Options are 1 through 23, Legacy, and AUTO. The default is AUTO. The 802.11n standard defines a total of 77 MCS. Each MCS specifies a certain modulation type (BPSK, QPSK, 64-QAM), coding rate (1/2, 3/4), guard interval (800 or 400ns), and number of spatial streams. Support for MCS 0-15 is mandatory for 802.11n access points while support for MCS 0-7 is mandatory for 802.11n clients.

Wireless 2.4 GHz – MAC Address Control



MAC Address Control

MAC Address Control allows you to restrict access to your network to only those client devices whose MAC addresses you add to the filter list. You can make changes to the Media Access Control (MAC) Address Filtering List on this page. For changes to take effect, you must click the Apply button. Click the Add button to add another client device's MAC address to the filter list. Select a MAC address in the list and then click the Delete button to delete it from the filter list.

Wireless

SSID: ARRIS-57AA

MAC Address Filtering

MAC Address Filter Type: None: Any device can try to connect.

MAC Address Filter List

MAC

MAC Address Control allows you to restrict access to your network to only those client devices whose MAC addresses you add to the filter list. You can make changes to the Media Access Control (MAC) Address Filtering List on this page. For changes to take effect, you must click the Apply button.

Wireless: (Technician Level only)

SSID – Sets the SSID for each individual LAN on your network.

Note: You can optionally set up the system so that there is more than one LAN in your network. This is most useful for commercial applications not home use. All of the "LAN Setup" and "Wireless Setup" configuration parameters can be set independently for each individual LAN.

MAC Address Control allows you to restrict access to your network to only those client devices whose MAC addresses you add to the filter list. You can make changes to the Media Access Control (MAC) Address Filtering List on this page. For changes to take effect, you must click the **Apply** button.

Wireless: (Technician Level only)

SSID – Sets the SSID for each individual LAN on your network.

Note: If this option is enabled, you can create a separate Wi-Fi LAN for guests or other uses. If used, you can set up all of the "LAN Setup" and "Wireless Setup" parameters independently for each LAN.

MAC Address Filtering:

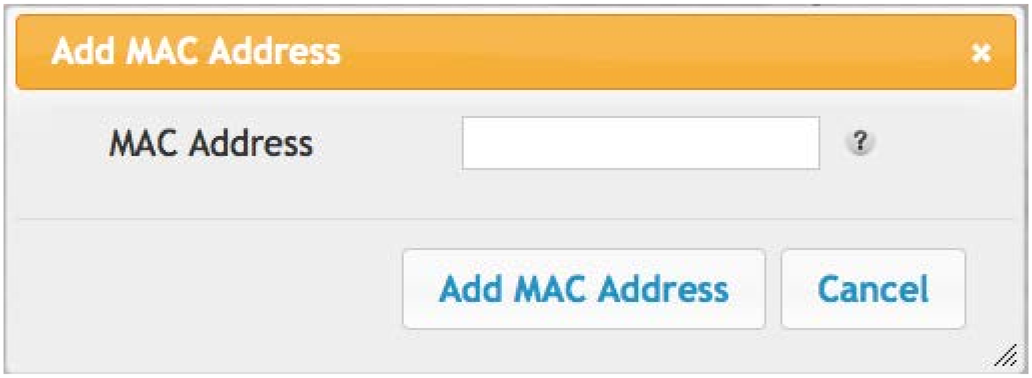
MAC Address Filter Type – Sets the MAC address filter type:

- None – Allows any device to try to connect.
- Whitelist – Allows only listed devices to connect.
- Blacklist – Allows any device not listed to connect. Note that the correct access keys must still be entered if required.

Click **Apply** to immediately apply the chosen filter type.

MAC Address Filter List:

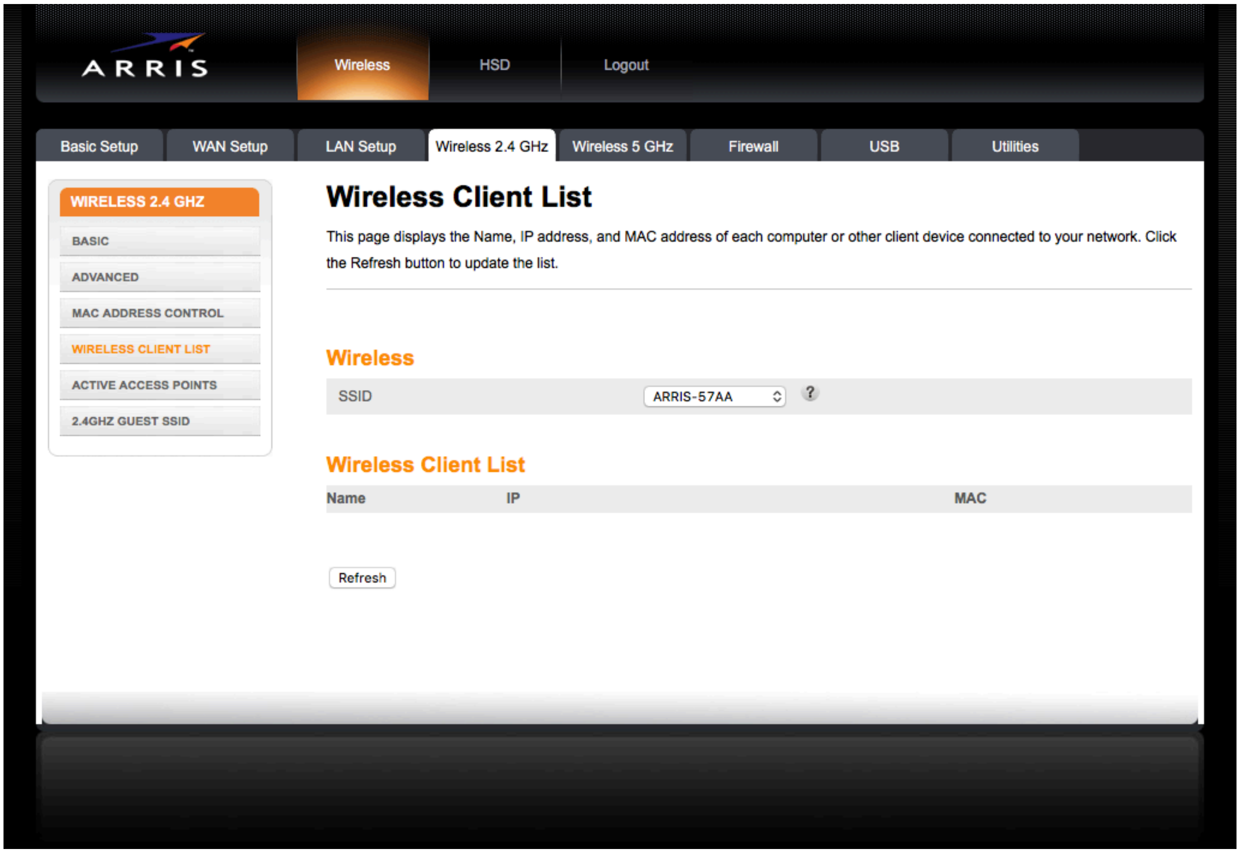
Click the **Add** button to add another client device’s MAC address to the filter list.



MAC Address – Enter the MAC address of the wireless client device.

Select a MAC address in the list and then click the **Delete** button to delete it from the filter list.

Wireless 2.4 GHz – Wireless Client List



Wireless Client List

This page displays the Name, IP address, and MAC address of each computer or other client device connected to your network. Click the Refresh button to update the list.

Wireless

SSID ARRIS-57AA

Wireless Client List

Name	IP	MAC

This page displays the Name, IP address, and MAC address of each computer or other client device connected to your network. Click the **Refresh** button to update the list.

Wireless: (Technician Level Only)

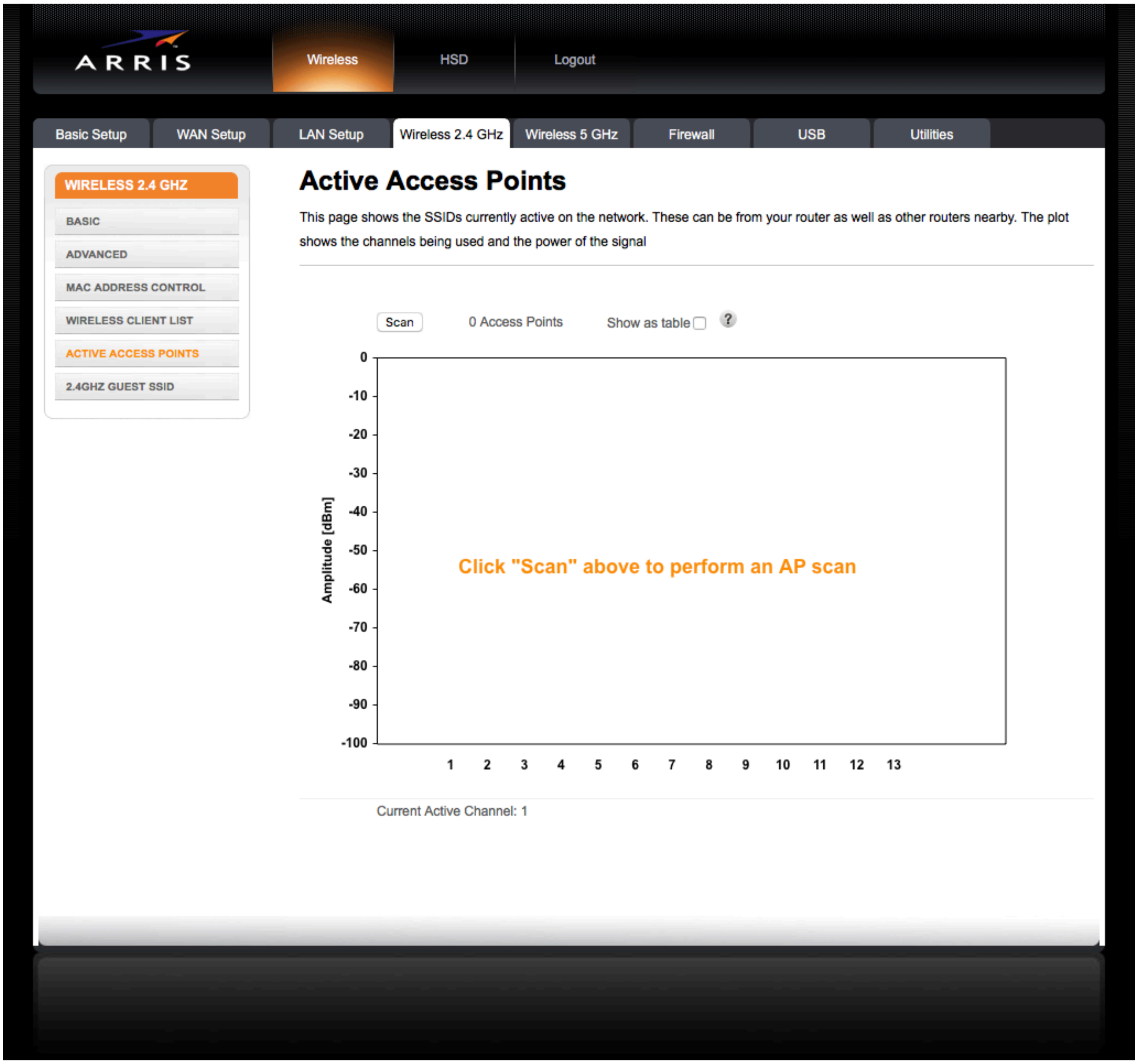
SSID – Sets the SSID for each individual LAN on your network.

Note: If this option is enabled, you can create a separate Wi-Fi LAN for guests or other uses. If used, you can set up all of the "LAN Setup" and "Wireless Setup" parameters independently for each LAN.

Wireless Client List:

Click the **Refresh** button to update the wireless client list.

Wireless 2.4 GHz - Active Access Points



Active Access Points

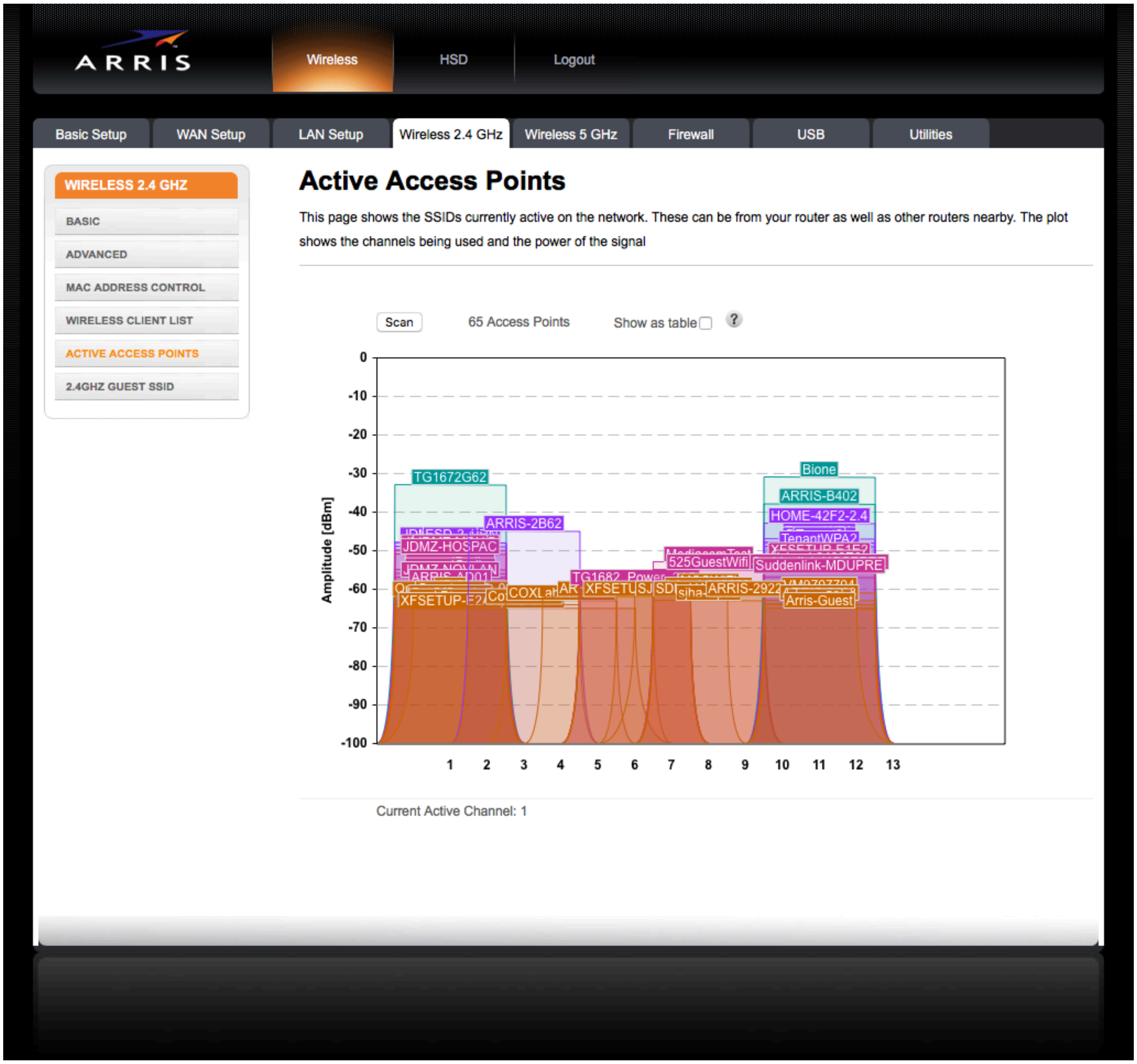
This page shows the SSIDs currently active on the network. These can be from your router as well as other routers nearby. The plot shows the channels being used and the power of the signal

0 Access Points

Click "Scan" above to perform an AP scan

Current Active Channel: 1

This screen lets you scan the local 2.4 GHz wifi spectrum for other access points (routers). This can be useful to diagnose interference issues. Click the **Scan** button to see a graphic display of other local access points:

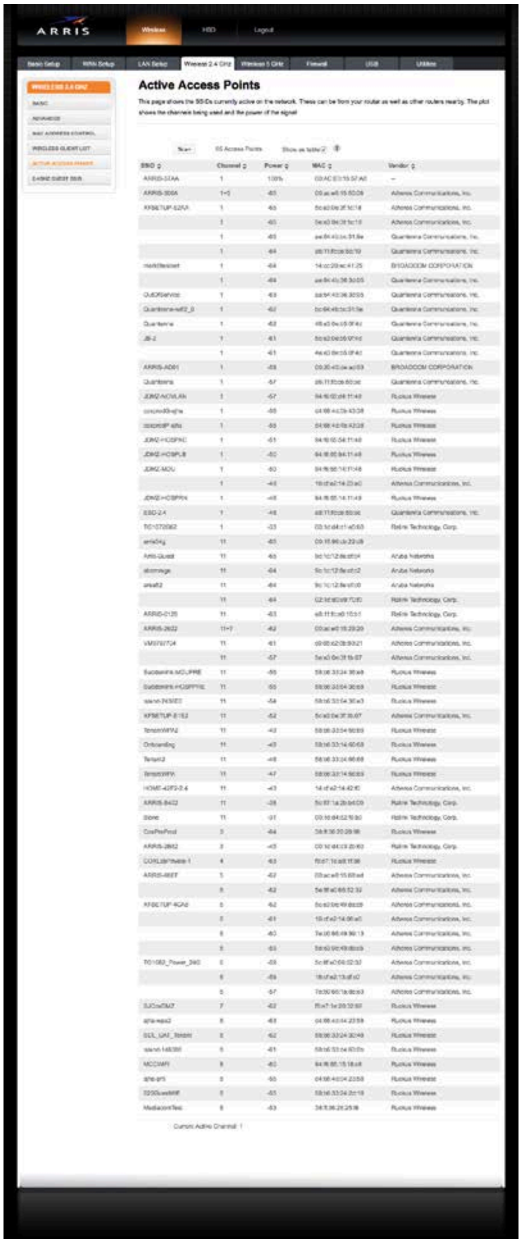


Active Access Points

This page shows the SSIDs currently active on the network. These can be from your router as well as other routers nearby. The plot shows the channels being used and the power of the signal

Current Active Channel: 1

Click the **Show as table** checkbox to display the results in table format, as shown below. This is useful in a location where there are a large number of access points, as in the example above.



Active Access Points

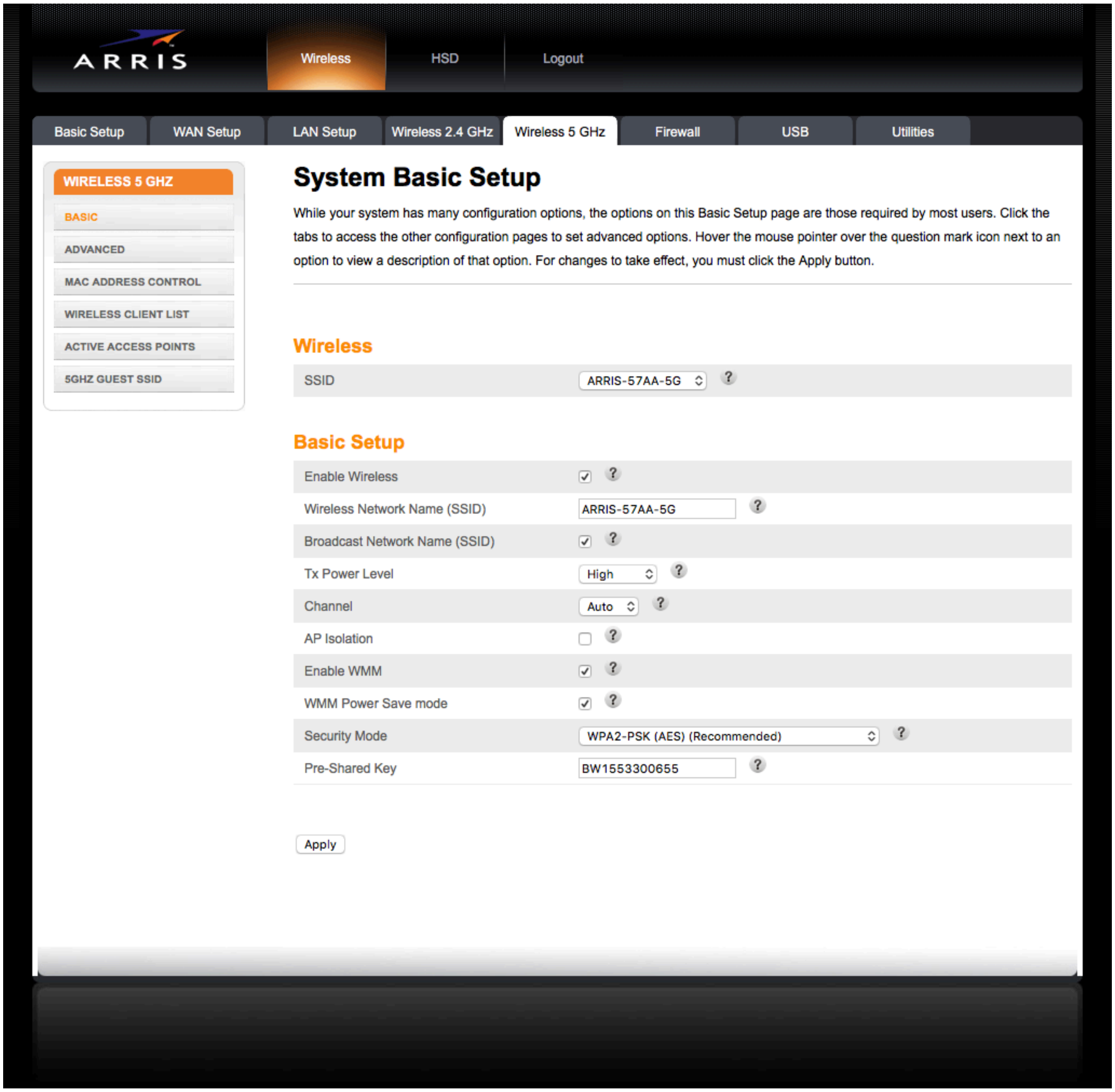
This page shows the SSIDs currently active on the network. These can be from your router as well as other routers nearby. The plot shows the channels being used and the power of the signal

66 Access Points   Show as table ☑

SSID ⇕	Channel ⇕	Power ⇕	MAC ⇕	Vendor ⇕
ARRIS-37AA	1	100%	00:AC:E3:15:57:A0	--
ARRIS-300A	1+5	-65	00:ac:e0:15:60:08	Atheros Communications, Inc.
KFSETUP-52FA	1	-65	5c:a3:0e:3f:1c:18	Atheros Communications, Inc.
	1	-65	5e:a3:0e:3f:1c:18	Atheros Communications, Inc.
	1	-65	ae:84:41:04:31:8e	Quantenna Communications, Inc.
	1	-64	a6:11:8b:c6:60:10	Quantenna Communications, Inc.
markBerabet	1	-64	14:cc:20:ec:41:25	BROADCOM CORPORATION
	1	-64	ae:84:41:36:30:05	Quantenna Communications, Inc.
OutOfService	1	-63	aa:84:43:36:30:55	Quantenna Communications, Inc.
Quantenna-wifi2_0	1	-62	bc:84:4b:bc:31:9e	Quantenna Communications, Inc.
Quantenna	1	-62	4e:a3:0e:05:0f:4c	Quantenna Communications, Inc.
JB-2	1	-61	5c:a2:0e:05:0f:4d	Quantenna Communications, Inc.
	1	-61	4e:a3:0e:05:0f:4c	Quantenna Communications, Inc.
ARRIS-AD01	1	-58	00:30:40:de:ad:03	BROADCOM CORPORATION
Quantenna	1	-57	a6:11:8b:c6:60:ac	Quantenna Communications, Inc.
JDMZ-ACVLAN	1	-57	84:18:02:d8:11:48	Ruckus Wireless
conomd0-wpa	1	-55	c4:08:4a:0b:43:38	Ruckus Wireless
conomdP wpa	1	-55	54:68:4a:0a:42:28	Ruckus Wireless
JDMZ-HCSPAC	1	-51	84:18:02:54:11:48	Ruckus Wireless
JDMZ-HCSPLB	1	-50	84:18:88:84:11:48	Ruckus Wireless
JDMZ-MOU	1	-50	84:18:88:14:11:48	Ruckus Wireless
	1	-46	18:cf:e2:14:23:a0	Atheros Communications, Inc.
JDMZ-HCSPRN	1	-48	84:18:88:14:11:48	Ruckus Wireless
ESD-2.4	1	-46	a8:11:8b:c6:60:ac	Quantenna Communications, Inc.
TC1072062	1	-33	00:1d:d4:c1:a0:63	Ralink Technology, Corp.
arris54g	11	-65	00:15:96:cb:22:c8	
Arris-Guest	11	-65	9c:1c:12:8e:d0:c4	Aruba Networks
alcomega	11	-64	9c:1c:12:8e:d0:c2	Aruba Networks
arisaft2	11	-64	9c:1c:12:8e:d0:c0	Aruba Networks
	11	-64	02:1d:d0:e9:70:f0	Ralink Technology, Corp.
ARRIS-0125	11	-63	a8:11:fc:a0:10:c1	Ralink Technology, Corp.
ARRIS-2622	11+7	-62	00:ac:e0:15:29:20	Atheros Communications, Inc.
VM070724	11	-61	c0:05:c2:0b:90:21	Atheros Communications, Inc.
	11	-57	5e:a3:0e:3f:1b:07	Atheros Communications, Inc.
Suddenlink-MOUPRE	11	-55	58:b6:33:24:30:a8	Ruckus Wireless
Suddenlink-HCSPPYE	11	-55	58:b6:33:04:30:68	Ruckus Wireless
island-2N3IE	11	-54	58:b6:33:04:30:a3	Ruckus Wireless
KFSETUP-E1E2	11	-52	5c:a3:0e:3f:1b:07	Atheros Communications, Inc.
TenantWiFi2	11	-43	58:b6:33:54:90:b9	Ruckus Wireless
Onboarding	11	-43	58:b6:33:14:60:68	Ruckus Wireless
Tenant2	11	-48	58:b6:33:24:90:68	Ruckus Wireless
TenantWiFi	11	-47	58:b6:33:14:90:b9	Ruckus Wireless
HOME-42F0-2.4	11	-43	14:cf:e2:14:42:f0	Atheros Communications, Inc.
ARRIS-8422	11	-38	5c:87:1a:2b:b4:00	Ralink Technology, Corp.
Store	11	-31	00:1d:d4:52:1b:b0	Ralink Technology, Corp.
CoxPreProd	3	-64	38:ff:36:20:28:98	Ruckus Wireless
ARRIS-2862	3	-45	00:1d:d4:c3:20:63	Ralink Technology, Corp.
CORLabPrivate-1	4	-63	f0:b7:1e:a8:1f:98	Ruckus Wireless
ARRIS-4EEF	5	-67	00:ac:e0:15:6f:ed	Atheros Communications, Inc.
	5	-62	5e:8f:a0:66:52:32	Atheros Communications, Inc.
KFSETUP-4CA6	5	-62	5c:a3:0e:49:da:c6	Atheros Communications, Inc.
	5	-61	18:cf:e2:14:06:a0	Atheros Communications, Inc.
	5	-60	7e:d0:66:48:90:13	Atheros Communications, Inc.
	5	-63	5e:a3:0e:49:da:c6	Atheros Communications, Inc.
TC1062_Power_340	5	-58	5c:8f:a0:66:52:32	Atheros Communications, Inc.
	5	-59	18:cf:e2:13:df:c0	Atheros Communications, Inc.
	5	-57	7e:00:66:1a:de:63	Atheros Communications, Inc.
SJCoxDMZ	7	-62	f0:a7:1e:20:30:60	Ruckus Wireless
apfa-wpa2	8	-63	04:08:4a:04:23:58	Ruckus Wireless
SDL_UAT_Tenant	8	-62	58:b6:33:24:30:48	Ruckus Wireless
island-14838	8	-61	58:b6:33:04:90:0a	Ruckus Wireless
MCCWIFI	8	-60	84:18:88:15:18:a8	Ruckus Wireless
apfa-psk	8	-55	04:08:4a:04:23:58	Ruckus Wireless
3230GuestWiFi	8	-55	58:b6:33:24:2c:18	Ruckus Wireless
MediacomTest	8	-63	38:ff:36:28:25:18	Ruckus Wireless

Current Active Channel: 1

Wireless 5 GHz – System Basic Setup



System Basic Setup

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

Wireless

SSID	ARRIS-57AA-5G

Basic Setup

Enable Wireless	☑
Wireless Network Name (SSID)	ARRIS-57AA-5G
Broadcast Network Name (SSID)	☑
Tx Power Level	High
Channel	Auto
AP Isolation	☐
Enable WMM	☑
WMM Power Save mode	☑
Security Mode	WPA2-PSK (AES) (Recommended)
Pre-Shared Key	BW1553300655

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

Wireless: (Technician Level Only)

SSID – Sets the SSID for each individual LAN on your network.

Note: If this option is enabled, you can create a separate Wi-Fi LAN for guests or other uses. If used, you can set up all of the "LAN Setup" and "Wireless Setup" parameters independently for each LAN.

Basic Setup:

Enable Wireless – Check this box to enable the wireless network on your system.

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

Broadcast Network Name (SSID) – Check this box to allow the SSID to be broadcast by the router. If enabled, your SSID could be obtained allowing unauthorized access to your network. If you would like others not to see your access point, uncheck the checkbox to hide the SSID.

Tx Power Level – Sets the transmit power level, which is the output power level of the wireless radio. Can be set to High, Medium, or Low.

Channel – Sets a communications channel for your router. The default setting is "Auto", in which the router selects a channel with the least amount of interference to use. If you manually select a channel and another unit is operating in the area, choose a channel that is farthest away from the channel that unit uses. If you experience interference or poor performance on a particular channel, try a different channel.

AP Isolation – Check this box to enable AP isolation. When enabled, each of your wireless clients is in its own virtual network and cannot communicate directly with one another. This may be useful if you have many guests using your network.

Enable WMM – Check this box to enable Wi-Fi Multimedia (WMM) functionality. Enabling WMM can help control latency and jitter when transmitting multimedia content over a wireless connection.

This quality of service mechanism uses four access categories, which in order of priority are: voice, video, best effort, and background. This ensures that applications with low tolerance for latency and jitter are treated with higher priority than less-sensitive data applications. WMM sets different wait times for the four categories in order to provide priority network access for applications that are less tolerant of packet delays.

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.

Security Mode – Sets the security mode for your router. Can be set to:

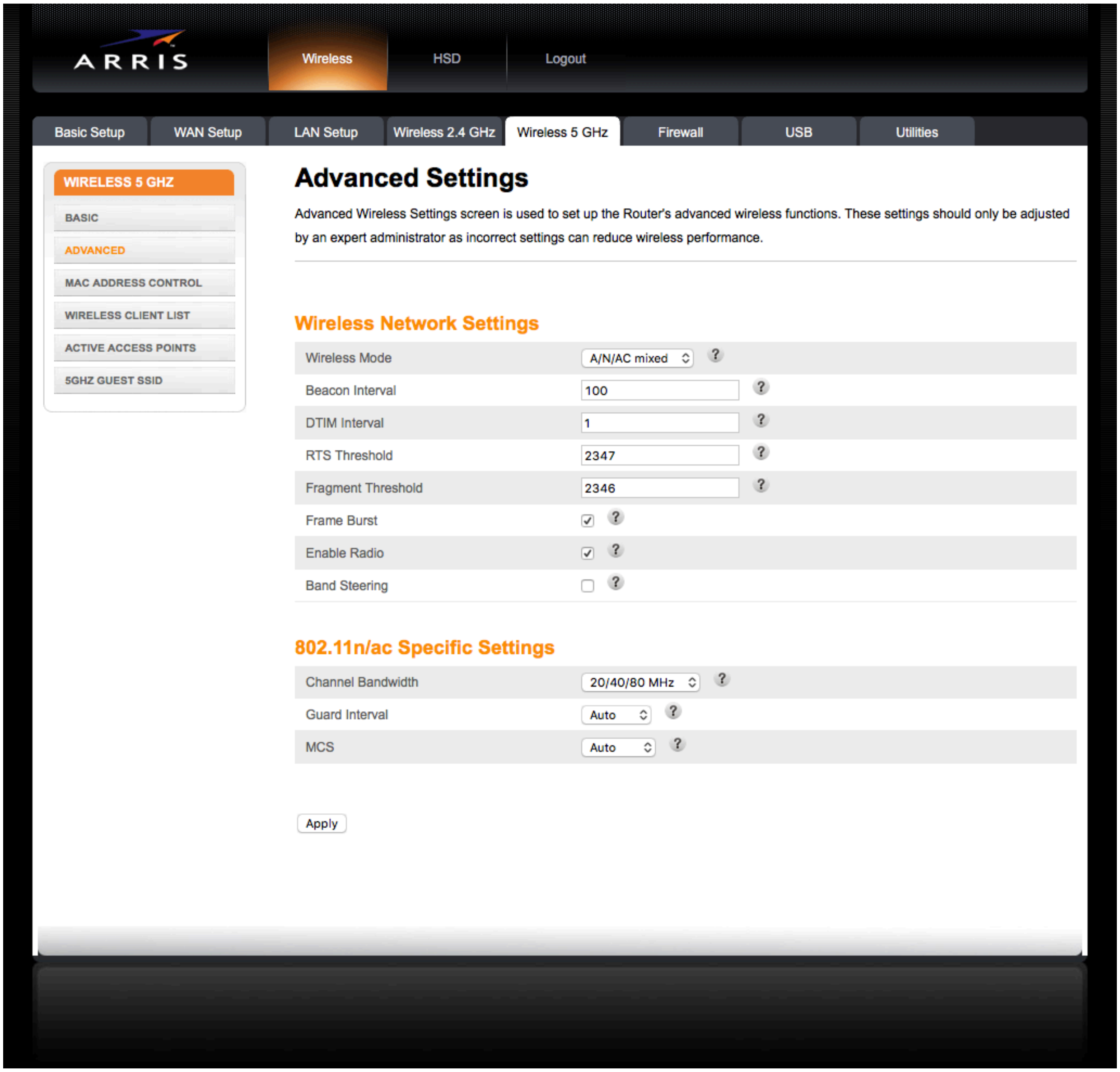
- OPEN (no security)
- WEP (64/128) (Wired Equivalency Privacy – 64/128) (poor security)
- WPA/WPA2-PSK (TKIP/AES) (Wi-Fi Protected Access/Wi-Fi Protected Access 2 – Pre-Shared Key – TKIP/AES encryption) (most compatible)

- WPA2-PSK (AES) (Wi-Fi Protected Access 2 – Pre-Shared Key – AES encryption) (recommended)
- WPA Enterprise
- WPA2 Enterprise.

802.11n performance is only available in Open mode, or WPA2 with AES encryption mode.

Pre-Shared Key – Sets your WPA Pre-Shared Key. This text string is used to generate a unique set of encryption keys for your network. Enter a text string in this field. The key can be either ASCII (text) or Hex (hexadecimal). An ASCII text key can be from 8 to 63 characters long. Valid characters are numbers "0" through "9" and letters "a" through "z", and any printable ASCII characters. A hexadecimal key must be 64 characters long. Valid characters are numbers "0" through "9" and letters "a" through "f".

Wireless 5 GHz – Advanced Settings



Advanced Settings

Advanced Wireless Settings screen is used to set up the Router's advanced wireless functions. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.

Wireless Network Settings

Wireless Mode	A/N/AC mixed
Beacon Interval	100
DTIM Interval	1
RTS Threshold	2347
Fragment Threshold	2346
Frame Burst	☑
Enable Radio	☑
Band Steering	□

802.11n/ac Specific Settings

Channel Bandwidth	20/40/80 MHz
Guard Interval	Auto
MCS	Auto

The Advanced Settings page is used to set up the router's advanced wireless functions. These settings should only be adjusted by an expert administrator since incorrect settings can reduce wireless performance. For changes to take effect, you must click the **Apply** button.

Wireless Network Settings:

> **Wireless Mode** – Sets the wireless mode. Options are: A/N mixed, A only, N only, AC only, N/AC mixed, and A/N/AC mixed. Select the proper mode to support all of the wireless devices that connect to your router.
>
> **Beacon Interval** – Sets the time interval between beacon transmissions, in milliseconds. The router uses these transmissions to synchronize the wireless network and its client devices. For best compatibility, leave the Beacon Interval at the default 100ms setting.

The allowable setting range is from 20 to 1024ms.

DTIM Interval – Sets the DTIM (Delivery Traffic Indication Message) Interval. The DTIM Interval informs the wireless client devices of the next available window for listening to broadcast and multicast messages. When the router sends a DTIM beacon the client devices hear the beacon and then listen for the messages. For best compatibility, leave the DTIM Interval at the default 1ms setting. The allowable range is from 1 to 255 ms.

RTS Threshold – Sets the packet size limit. When the threshold is passed, the ready to send/clear to send (RTS/CTS) function is invoked. The default setting is 2347 bytes. The allowable setting range is from 1 to 2347 bytes.

Fragment Threshold – Sets the fragmentation threshold. This threshold should be set to equal the maximum Ethernet frame size allowable on the link including overhead. Setting a lower threshold can damage data throughput since large frames could be fragmented and/or collisions could occur. The default setting is 2346. The allowable setting range is from 256 to 2346 bytes.

Frame Burst – Check this box to enable Frame Burst on your network. Frame Bursting is a transmission technique that increases the throughput of point-to-point 802.11a, b, or g links by reducing the overhead associated with the wireless transmissions. This results in the ability to support higher data throughput in mixed and uniform networks. It can, however, result in unfair allocation of airtime where there are a mix of client devices on the network, of which only some support Frame-Bursting.

WMM Power Save Mode – Check this box to enable WMM Power Save Mode. WMM Power Save delivery is a more efficient power management method than legacy 802.11 power save polling.

Enable Radio (Technician level only) – Check this box to enable or disable the Wi-fi radio.

Band Steering – Check this box to enable Band Steering. The SSID and passphrase for both the 2.4 GHz and 5.0 GHz networks must be identical for Band Steering to operate.

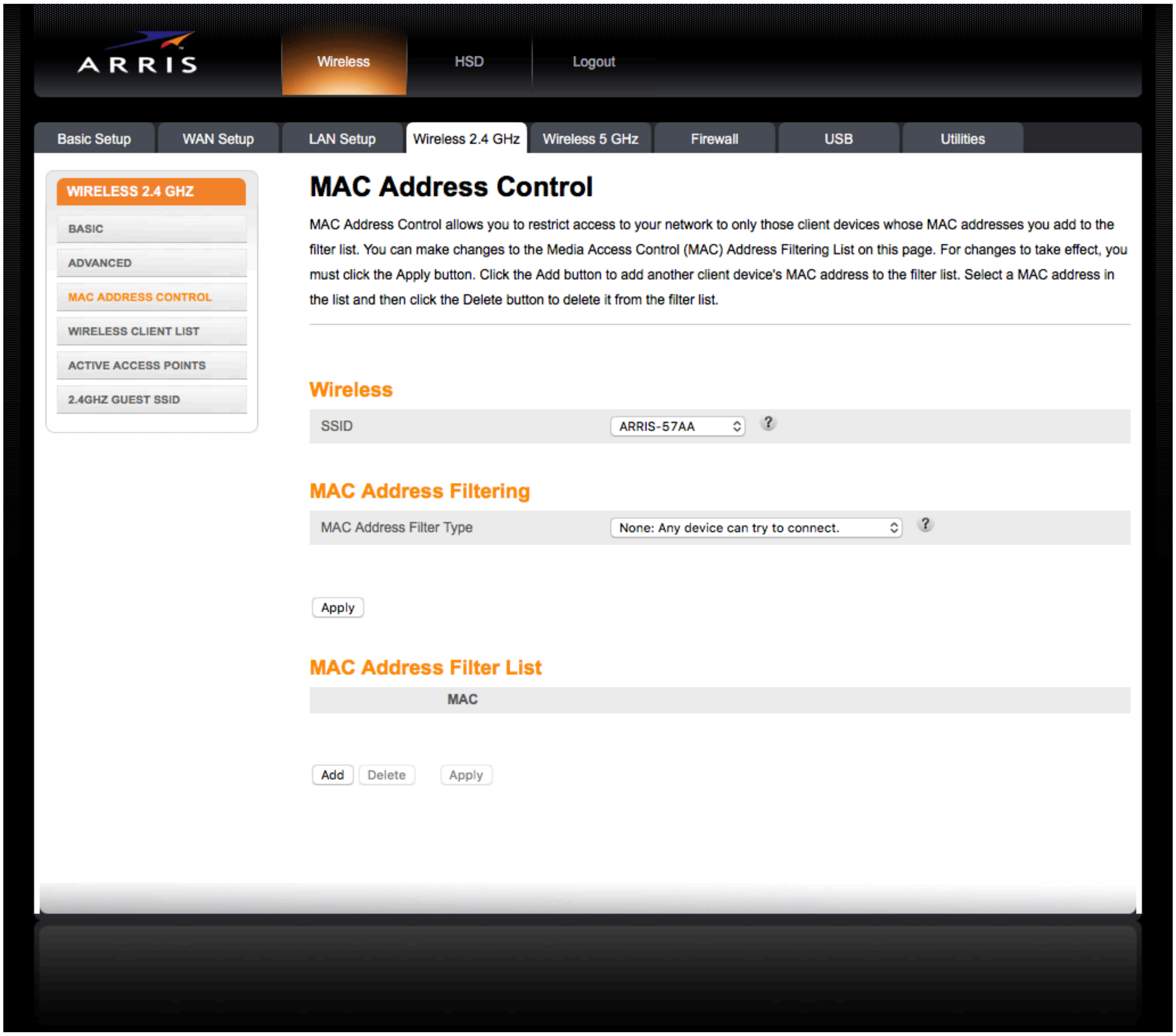
802.11n Specific Settings:

Channel Bandwidth – Sets the 802.11n Channel Bandwidth. Options are 20 MHz or 20/40 MHz. The default setting is 20/40 MHz. If your wireless network is in a very clean RF environment, setting the Channel Bandwidth to 20/40 increases throughput by "bonding" two channels. However, if there are any other wireless routers or access points within range of the Gateway, it allocates 20 MHz bandwidth regardless of this setting. This is a Wi-fi Alliance requirement. (You can verify the channel bandwidth by using the previously mentioned wireless network scanning software, MetaGeek's inSSIDer.)

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).

MCS – Sets the 802.11n Modulation and Coding Scheme to be used. Options are 1 through 23, Legacy, and AUTO. The default is AUTO. The 802.11n standard defines a total of 77 MCS. Each MCS specifies a certain modulation type (BPSK, QPSK, 64-QAM), coding rate (1/2, 3/4), guard interval (800 or 400ns), and number of spatial streams. Support for MCS 0-15 is mandatory for 802.11n access points while support for MCS 0-7 is mandatory for 802.11n clients.

Wireless 5 GHz – MAC Address Control



MAC Address Control

MAC Address Control allows you to restrict access to your network to only those client devices whose MAC addresses you add to the filter list. You can make changes to the Media Access Control (MAC) Address Filtering List on this page. For changes to take effect, you must click the Apply button. Click the Add button to add another client device's MAC address to the filter list. Select a MAC address in the list and then click the Delete button to delete it from the filter list.

Wireless

SSID	ARRIS-57AA

MAC Address Filtering

MAC Address Filter Type	None: Any device can try to connect.

MAC Address Filter List

MAC

MAC Address Control allows you to restrict access to your network to only those client devices whose MAC addresses you add to the filter list. You can make changes to the Media Access Control (MAC) Address Filtering List on this page. For changes to take effect, you must click the **Apply** button.

Wireless: (Technician Level only)

SSID – Sets the SSID for each individual LAN on your network.

Note: If this option is enabled, you can create a separate Wi-Fi LAN for guests or other uses. If used, you can set up all of the "LAN Setup" and "Wireless Setup" parameters independently for each LAN.

MAC Address Filtering:

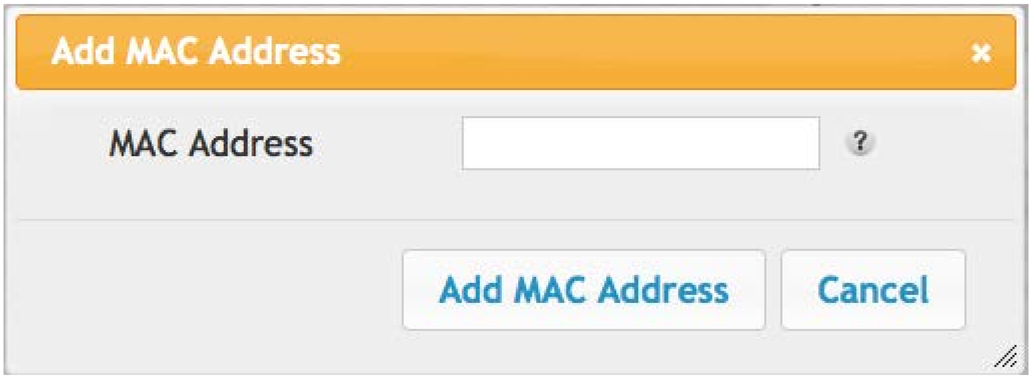
MAC Address Filter Type – Sets the MAC address filter type:

- None – Allows any device to try to connect.
- Whitelist – Allows only listed devices to connect.
- Blacklist – Allows any device not listed to connect. Note that the correct access keys must still be entered if required.

Click **Apply** to immediately apply the chosen filter type.

MAC Address Filter List:

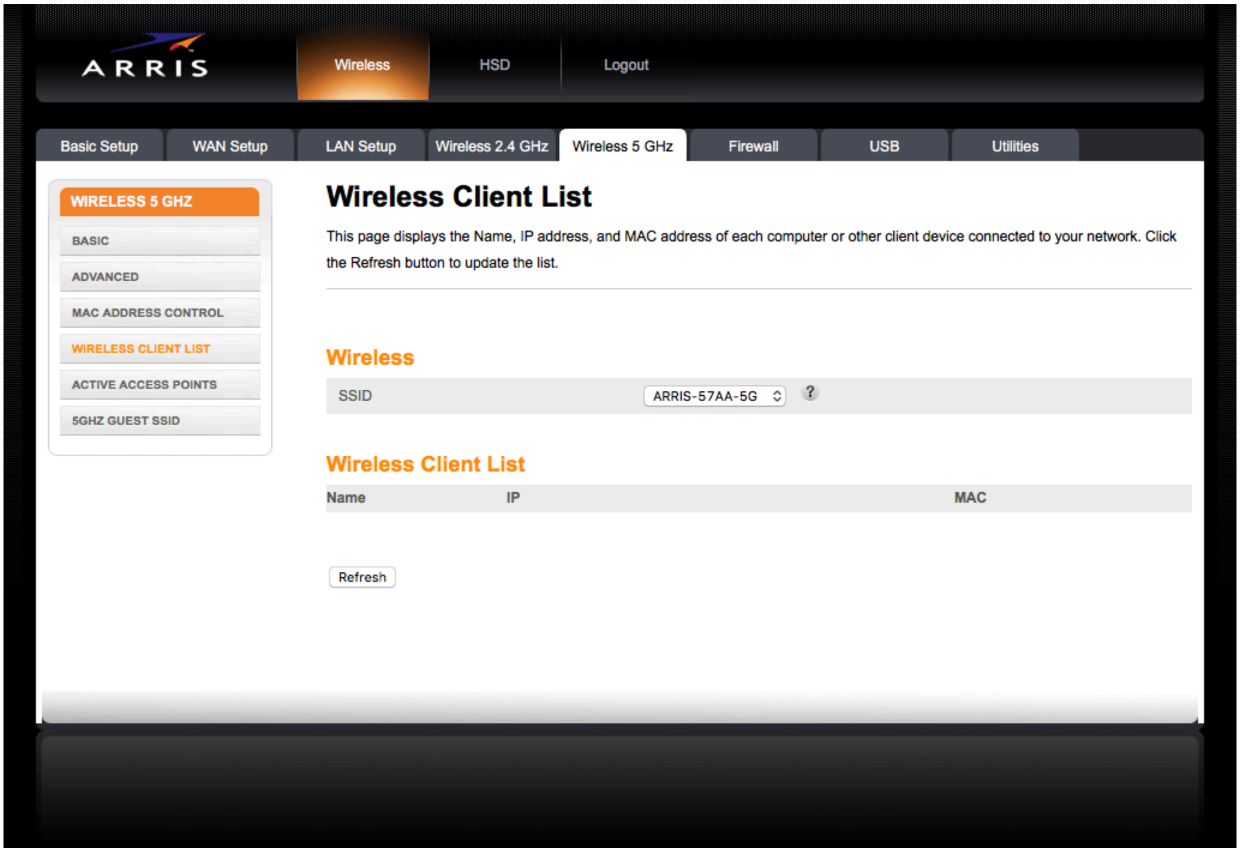
Click the **Add** button to add another client device's MAC address to the filter list.



MAC Address – Enter the MAC address of the wireless client device.

Select a MAC address in the list and then click the **Delete** button to delete it from the filter list.

Wireless 5 GHz – Wireless Client List



Wireless Client List

This page displays the Name, IP address, and MAC address of each computer or other client device connected to your network. Click the Refresh button to update the list.

Wireless

SSID: ARRIS-57AA-5G

Wireless Client List

Name	IP	MAC

This page displays the Name, IP address, and MAC address of each computer or other client device connected to your network. Click the **Refresh** button to update the list.

Wireless: (Technician Level Only)

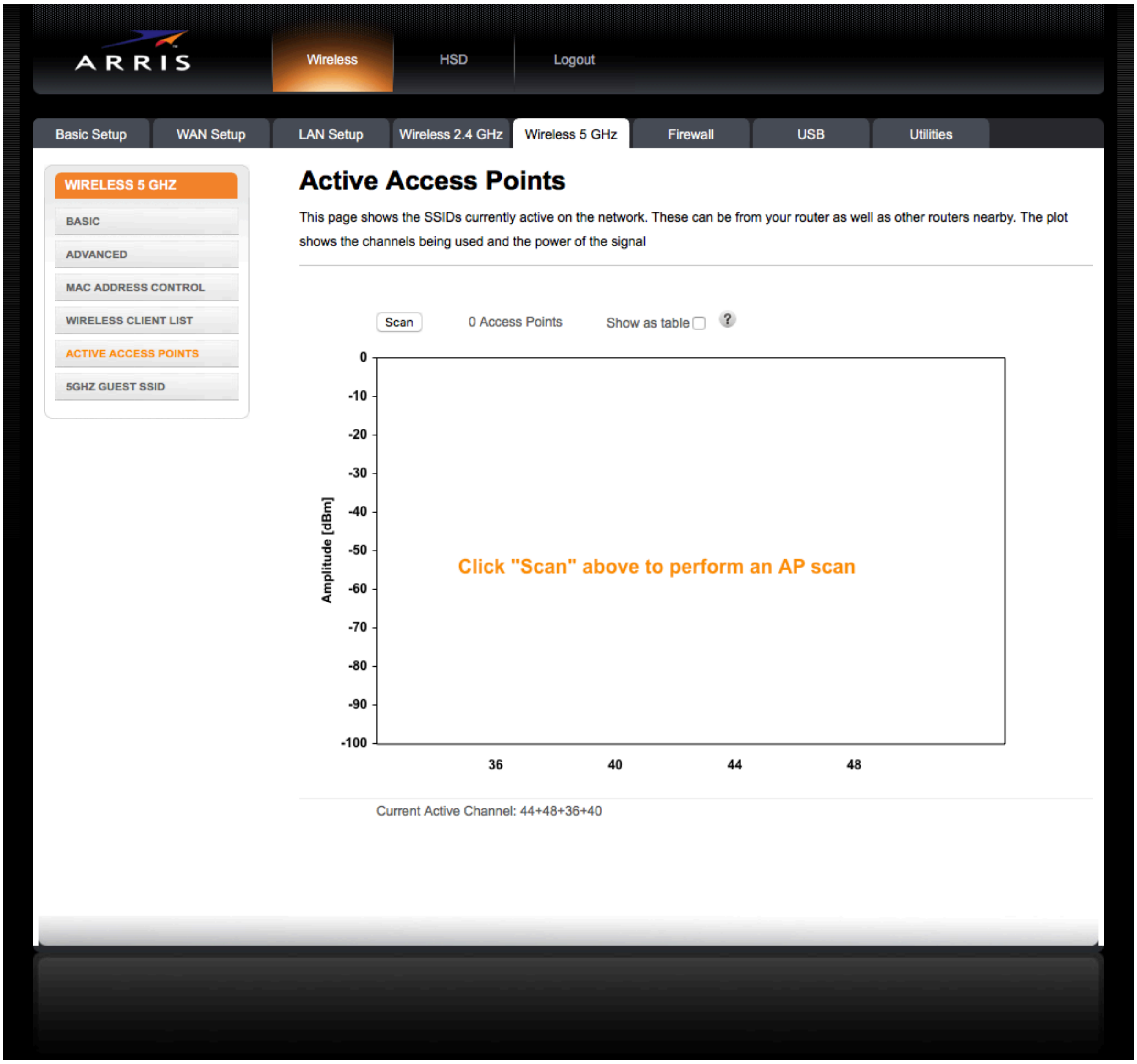
SSID – Sets the SSID for each individual LAN on your network.

Note: If this option is enabled, you can create a separate Wi-Fi LAN for guests or other uses. If used, you can set up all of the "LAN Setup" and "Wireless Setup" parameters independently for each LAN.

Wireless Client List:

Click the **Refresh** button to update the wireless client list.

Wireless 5 GHz - Active Access Points

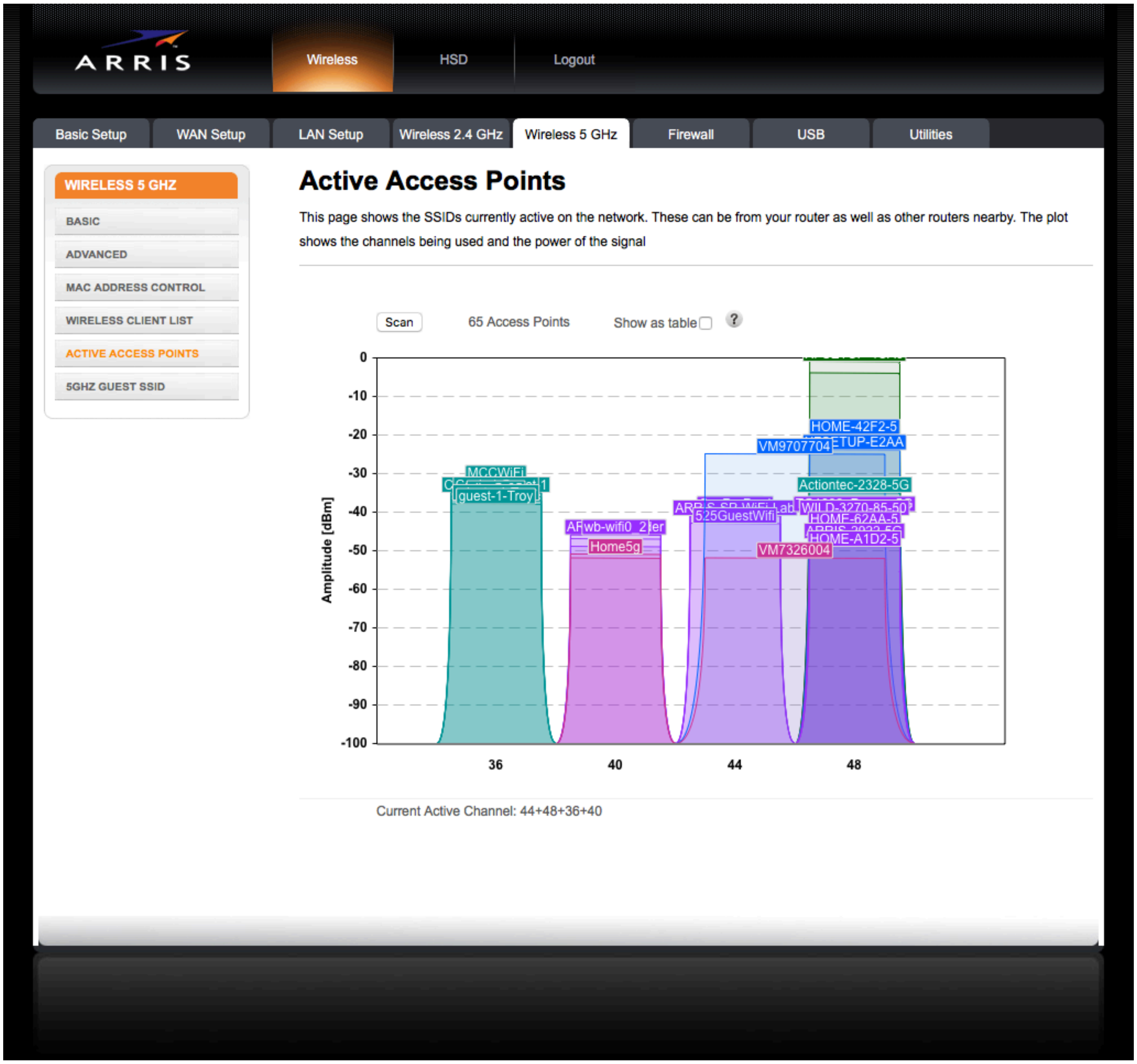


Active Access Points

This page shows the SSIDs currently active on the network. These can be from your router as well as other routers nearby. The plot shows the channels being used and the power of the signal

Current Active Channel: 44+48+36+40

This screen lets you scan the local 5 GHz wifi spectrum for other access points (routers). This can be useful to diagnose interference issues. Click the **Scan** button to see a graphic display of other local access points:



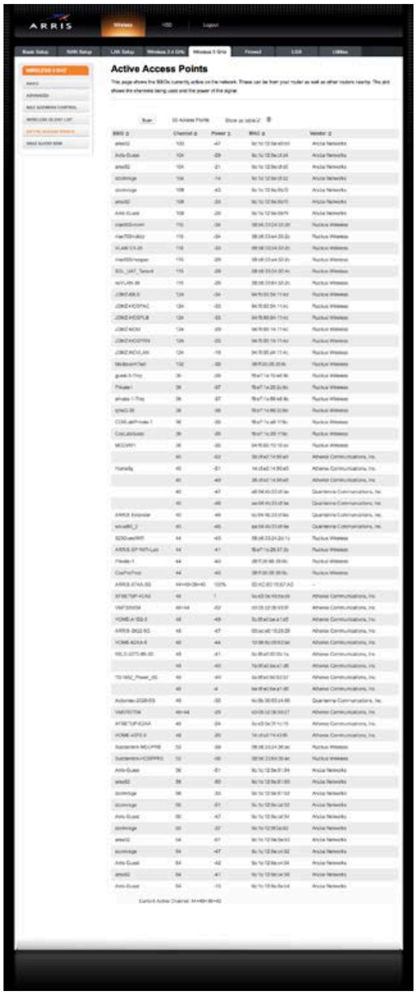
Active Access Points

This page shows the SSIDs currently active on the network. These can be from your router as well as other routers nearby. The plot shows the channels being used and the power of the signal

65 Access Points

Current Active Channel: 44+48+36+40

Click the **Show as table** checkbox to display the results in table format, as shown below. This is useful in a location where there are a large number of access points, as in the example above.

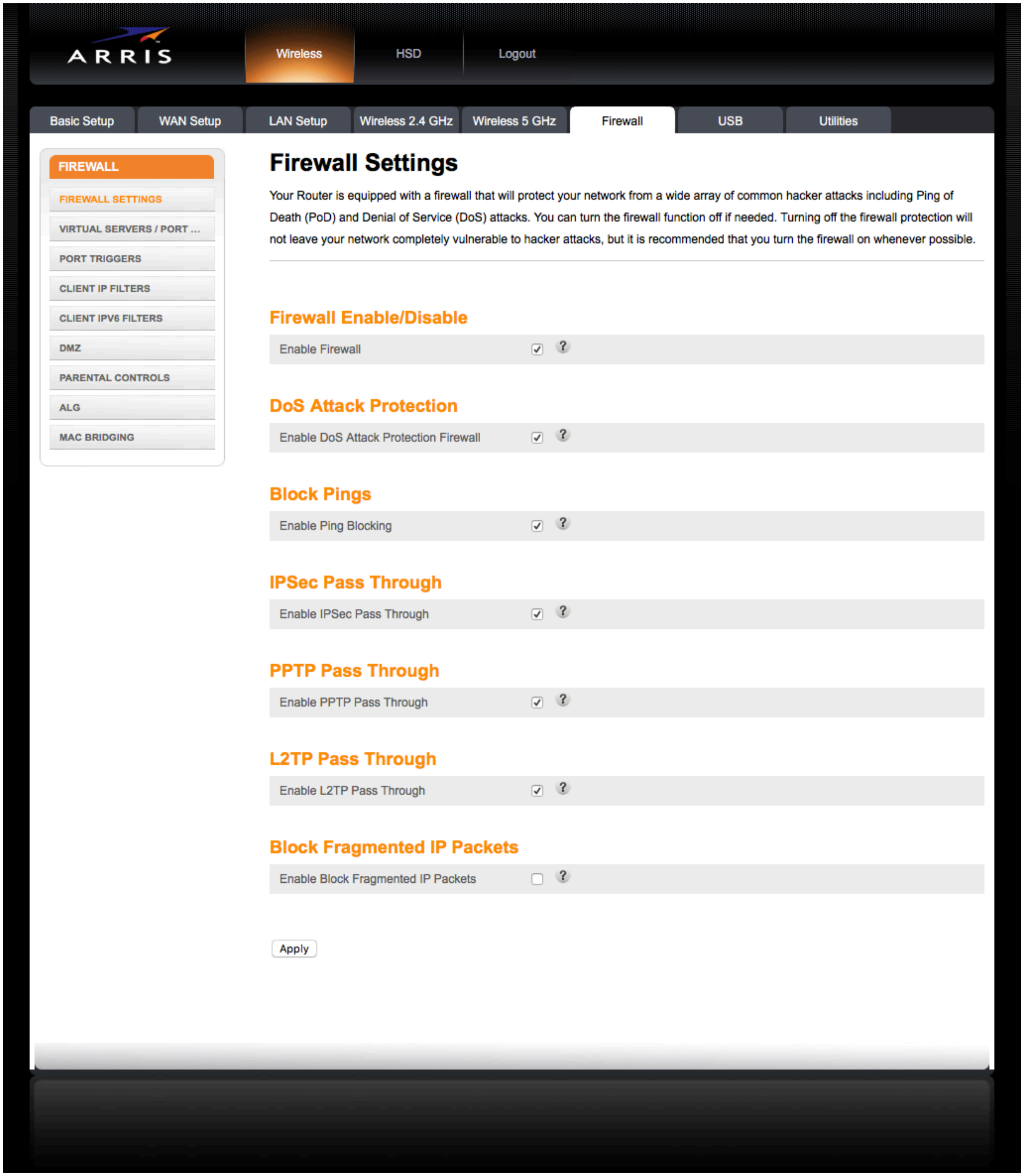


Active Access Points

SSID	Channel	Power	MAC	Vendor

Firewall

Firewall – Firewall Settings



Firewall Settings

Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including Ping of Death (PoD) and Denial of Service (DoS) attacks. You can turn the firewall function off if needed. Turning off the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you turn the firewall on whenever possible.

Firewall Enable/Disable

Enable Firewall ☑ ?

DoS Attack Protection

Enable DoS Attack Protection Firewall ☑ ?

Block Pings

Enable Ping Blocking ☑ ?

IPSec Pass Through

Enable IPSec Pass Through ☑ ?

PPTP Pass Through

Enable PPTP Pass Through ☑ ?

L2TP Pass Through

Enable L2TP Pass Through ☑ ?

Block Fragmented IP Packets

Enable Block Fragmented IP Packets □ ?

Your router is equipped with a firewall that protects your network from a wide array of common hacker attacks, including Ping of Death (PoD) and Denial of Service (DoS) attacks. You can also configure VPN pass-through to enable VPN tunneling using IPSec, PPTP, or L2TP protocols to pass through the router’s firewall so that you can connect to a Virtual Private Network at your office, for example.

You can disable the firewall function if needed. Turning off the firewall protection does not leave your network completely vulnerable to hacker attacks, but you should enable the firewall whenever possible. For changes to take effect, click the **Apply** button.

Firewall Enable/Disable:

Enable Firewall – Check this box to enable the firewall on your system.

DoS Attack Protection:

Enable DoS Attack Protection Firewall – Check this box to enable DoS attack protection.

Block Pings:

Enable Block Pings – Check this box to enable ping blocking.

IPSec Pass Through:

Enable IPSec Pass Through – Check this box to enable IPSec (Internet Protocol Security) pass through. This allows IPSec tunnels to pass through the firewall.

PPTP Pass Through:

Enable PPTP Pass Through – Check this box to enable PPTP (Point-to-Point Tunneling Protocol) pass through. This allows PPTP tunnels to pass through the firewall.

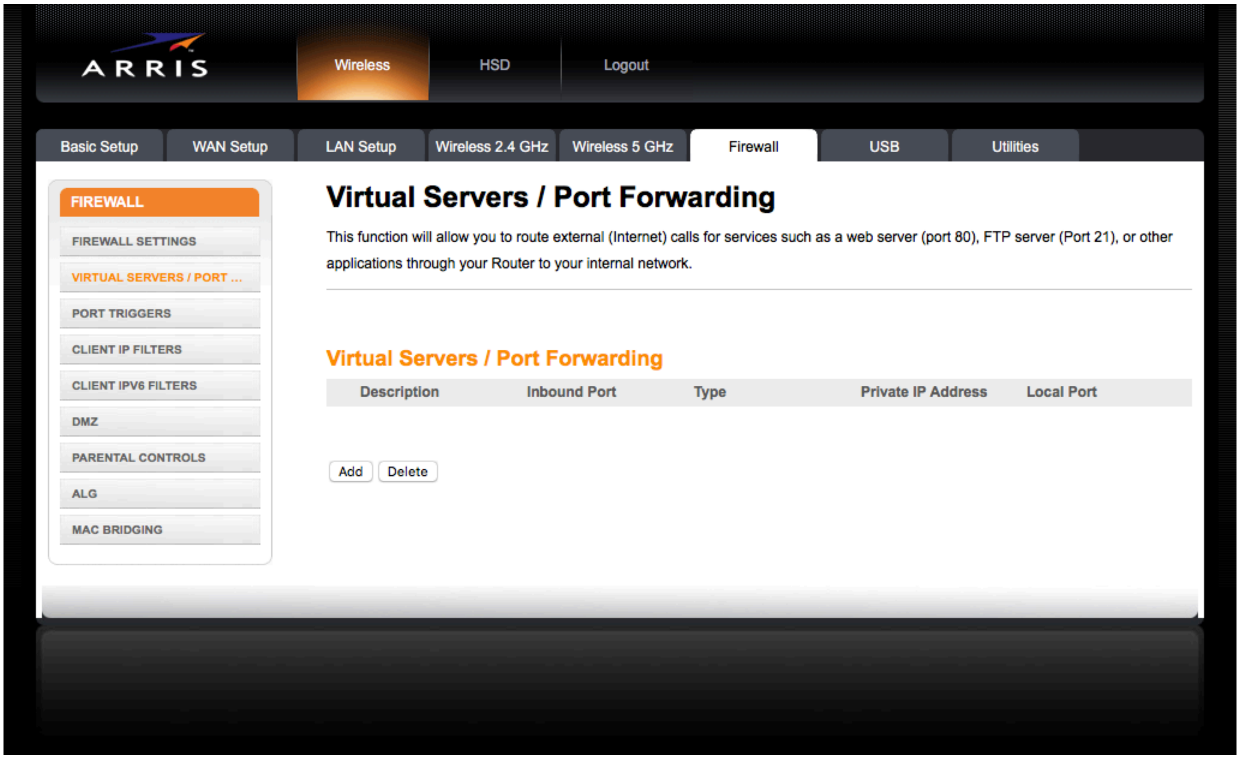
L2TP Pass Through:

Enable L2TP Pass Through – Check this box to enable L2TP (Layer 2 Tunneling Protocol) pass through. This allows L2TP tunnels to pass through the firewall.

Block Fragmented IP Packets:

Enable Block Fragmented IP Packets – Check this box to enable fragmented IP packet blocking.

Firewall – Virtual Servers / Port Forwarding



Virtual Servers / Port Forwarding

This function will allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications through your Router to your internal network.

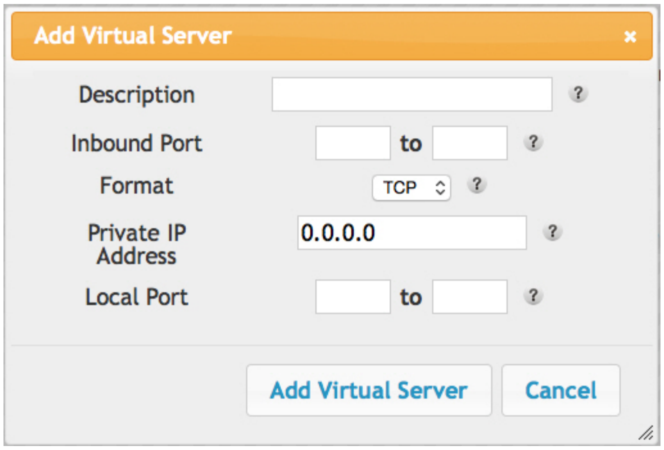
Virtual Servers / Port Forwarding

Description	Inbound Port	Type	Private IP Address	Local Port

The port forwarding function forwards inbound traffic from the Internet to a specified single device on your network. Examples include allowing access to a web server on your network, peer-to-peer file sharing, some gaming and videoconferencing applications, and others. This function allows you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications through your router to your internal network.

Click the Add button to add a virtual server. Select a virtual server from the list and click the Delete button to delete a virtual server.

Virtual Servers:



Description

Inbound Port to

Format TCP

Private IP Address 0.0.0.0

Local Port to

Description – Enter a name for the virtual server.

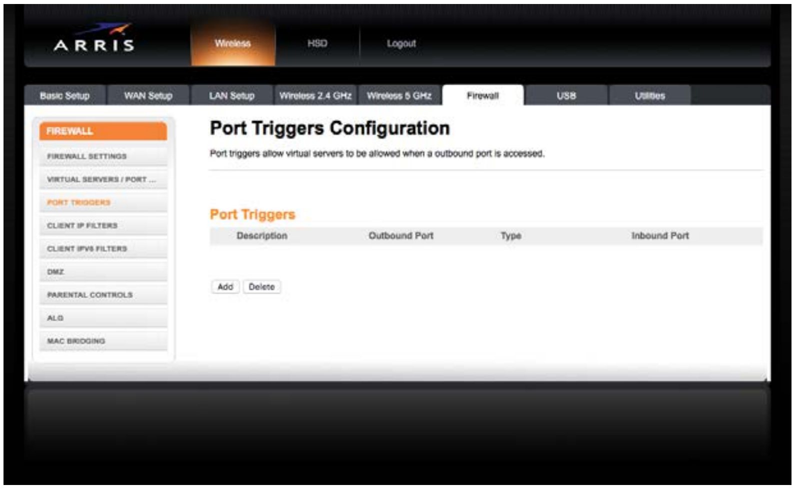
Inbound Port – Enter the inbound port range for the virtual server. It should be the same range as the local port.

Format – Sets the format for the port. Options are TCP, UDP, or BOTH.

Private IP Address – Enter the IP address of the machine on the LAN that you want the connections to go to.

Local Port – Enter the local port range for the virtual server. It should be the same range as the inbound port.

Firewall – Port Triggers Configuration



Port Triggers Configuration

Port triggers allow virtual servers to be allowed when a outbound port is accessed.

Port Triggers

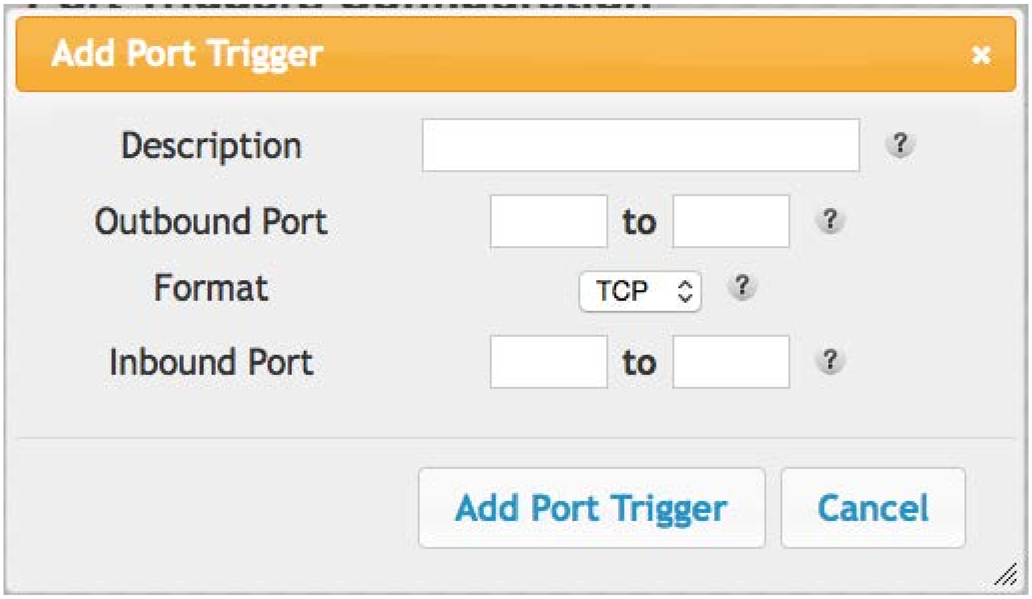
Description	Outbound Port	Type	Inbound Port

Port triggering lets you set the router to watch outgoing traffic for specific port numbers, remember the IP address of the sending computer, and then route the data back to the sending computer when the requested data returns. This is typically used for online gaming and online chat applications.

Port triggers allow virtual servers to be allowed when an outbound port is accessed.

Click the **Add** button to add a port trigger. Select a port trigger from the list and click the **Delete** button to delete a port trigger.

Port Triggers:



Description

Outbound Port to

Format TCP

Inbound Port to

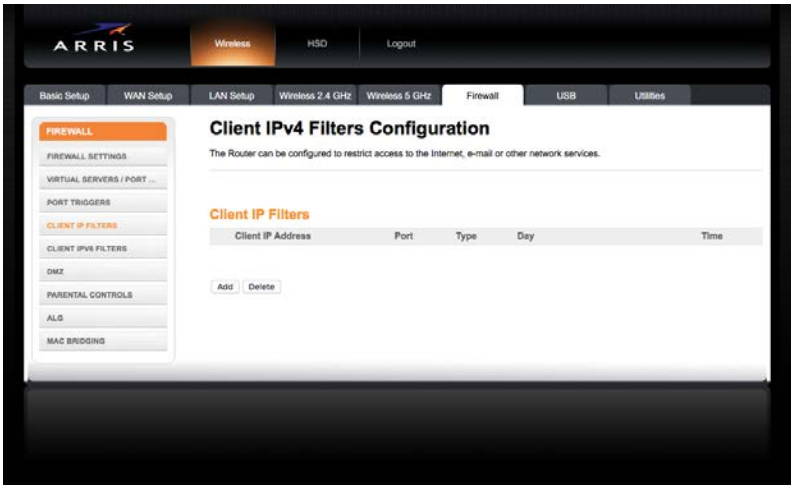
Description – Enter a name for the port trigger.

Outbound Port – Enter the outbound port range for the port trigger. It should be the same range as the inbound port.

Format – Sets the format for the port. Options are TCP, UDP, or BOTH.

Inbound Port – Enter the inbound port range for the port trigger. It should be the same range as the outbound port.

Firewall – Client IP Filters Configuration



Client IPv4 Filters Configuration

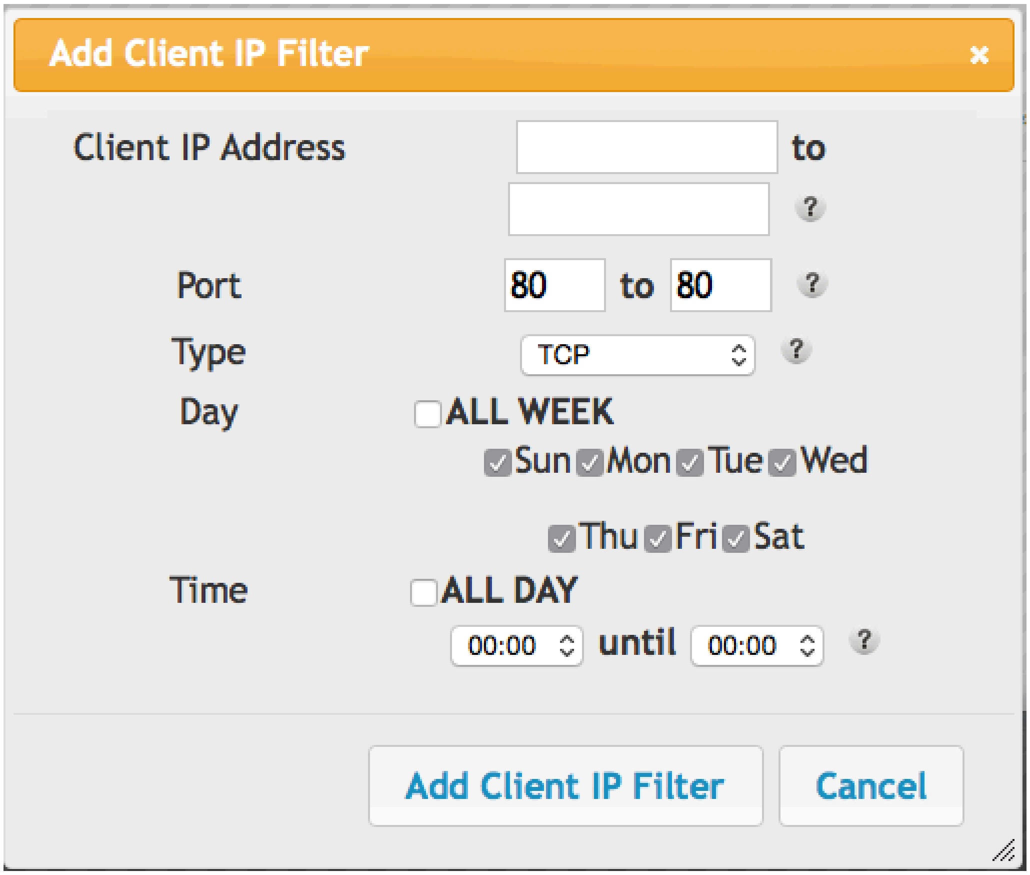
The Router can be configured to restrict access to the Internet, e-mail or other network services.

Client IP Filters

Client IP Address	Port	Type	Day	Time

The router can be configured to restrict access to the Internet, email, or other network services at specific days and times.

Client IP Filters:



Client IP Address to

Port 80 to 80

Type TCP

Day □ ALL WEEK

☑Sun ☑Mon ☑Tue ☑Wed

☑Thu ☑Fri ☑Sat

Time □ ALL DAY

00:00 until 00:00

Client IP Address – Enter the client IP address or range to filter.

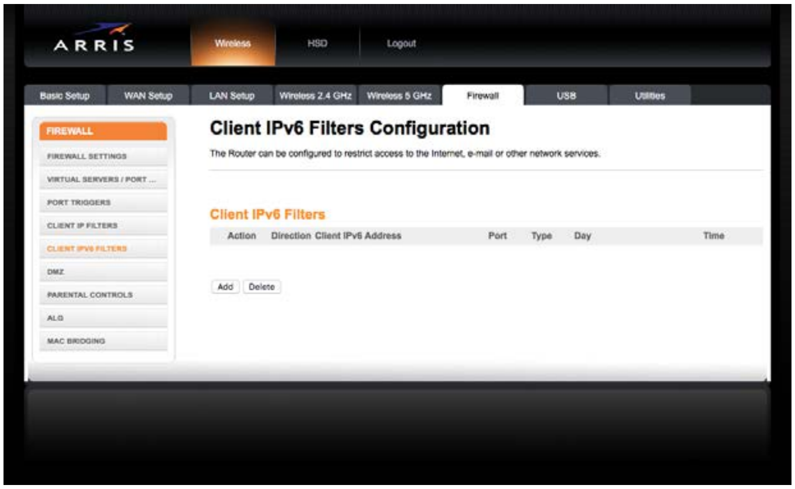
Port – Enter the outbound traffic port number range, starting and ending.

Type – Sets the port type. Options are TCP, UDP, or BOTH.

Day – Click the check boxes for the days you want access allowed, or click the All Week checkbox for all week.

Time – Sets the start time and end time for the allowed access during the specified days (24-hour clock). 00:00 to 24:00 indicates all day, or click the checkbox for All Day.

Firewall – Client IP Filters (IPV6) Configuration



Client IPv6 Filters Configuration

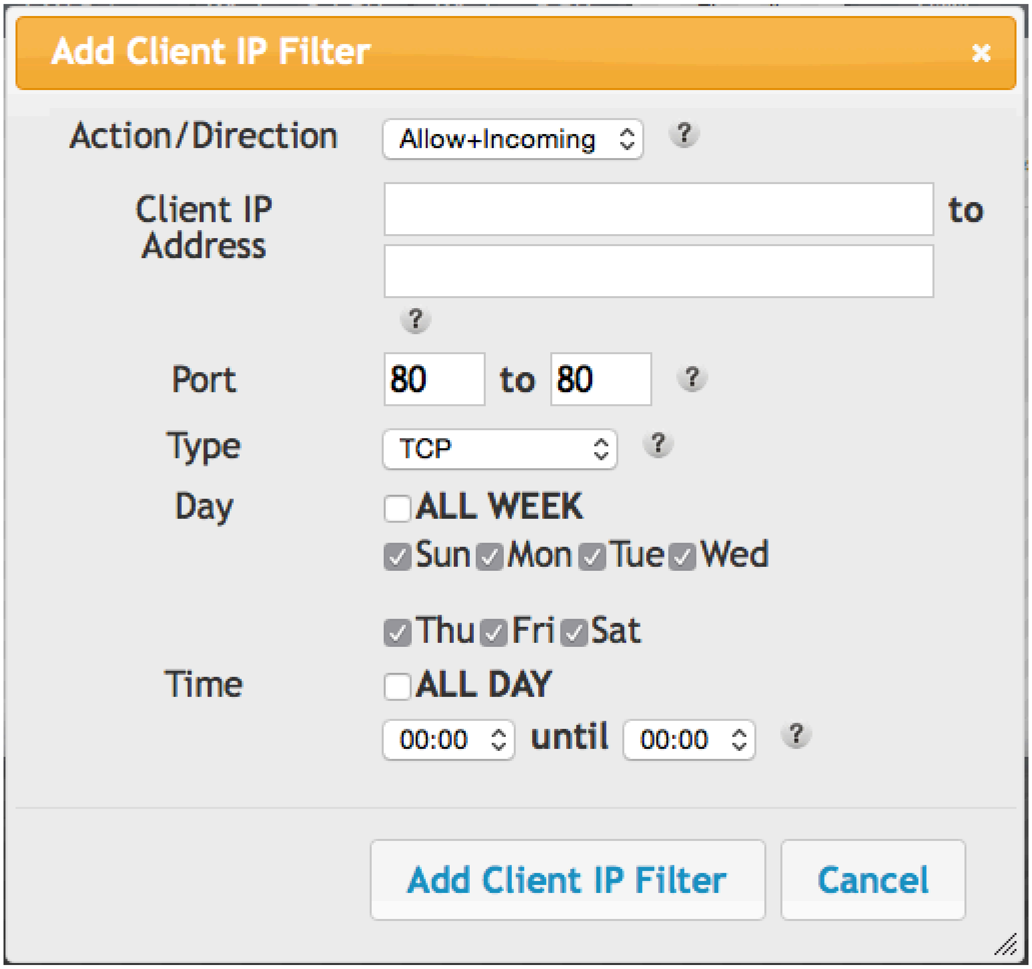
The Router can be configured to restrict access to the Internet, e-mail or other network services.

Client IPv6 Filters

Action	Direction	Client IPv6 Address	Port	Type	Day	Time

The router can be configured to restrict access to the Internet, email, or other network services. This screen adds and deletes filters for IPV6.

Client IP Filters:



Add Client IP Filter

Action/Direction: Allow+Incoming

Client IP Address: ______ to ______

Port: 80 to 80

Type: TCP

Day: □ ALL WEEK
☑ Sun ☑ Mon ☑ Tue ☑ Wed
☑ Thu ☑ Fri ☑ Sat

Time: □ ALL DAY
00:00 until 00:00

Action/Direction - By default, the router accepts all IPv6 outgoing traffic and denies all

IPv6 incoming traffic. Select either **Allow+Incoming** or **Deny+Outgoing** to configure exception rules to filter incoming or outgoing traffic.

Client IP Address – Enter the range of IPv6 addresses to filter.

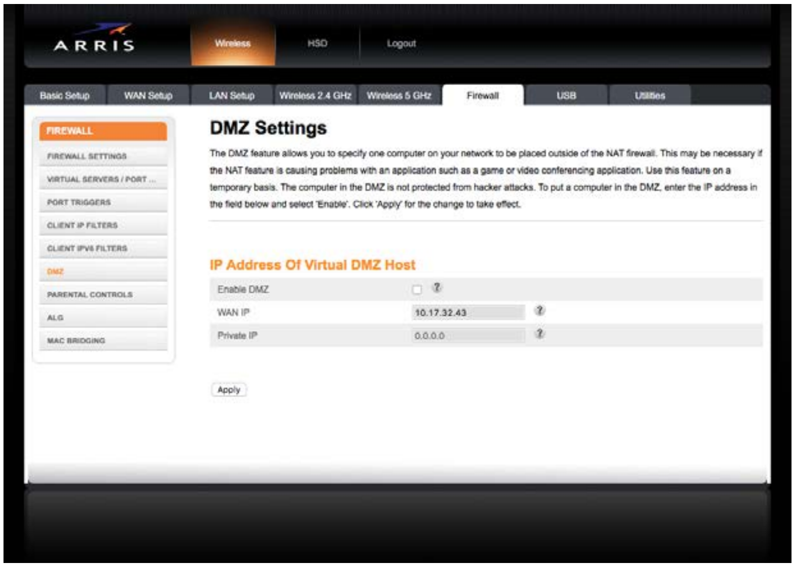
Port – Enter the outbound traffic port number range, starting and ending.

Type – Sets the port type. Options are TCP, UDP, or BOTH.

Day – Click the check boxes for the days you want access allowed, or click the All Week checkbox for all week.

Time – Sets the start time and end time for the allowed access during the specified days (24-hour clock). 00:00 to 24:00 indicates all day, or click the checkbox for All Day.

Firewall – DMZ Settings



DMZ Settings

The DMZ feature allows you to specify one computer on your network to be placed outside of the NAT firewall. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. The computer in the DMZ is not protected from hacker attacks. To put a computer in the DMZ, enter the IP address in the field below and select 'Enable'. Click 'Apply' for the change to take effect.

IP Address Of Virtual DMZ Host

Enable DMZ	□ ?
WAN IP	10.17.32.43 ?
Private IP	0.0.0.0 ?

The DMZ feature allows you to specify one computer on your network to be placed outside of the NAT firewall. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application.

Use this feature only on a temporary basis. The computer in the DMZ is not protected from hacker attacks.

To put a computer in the DMZ, click the **Enable DMZ** checkbox, enter its IP address, and click the **Apply** button.

IP Address Of Virtual DMZ Host:

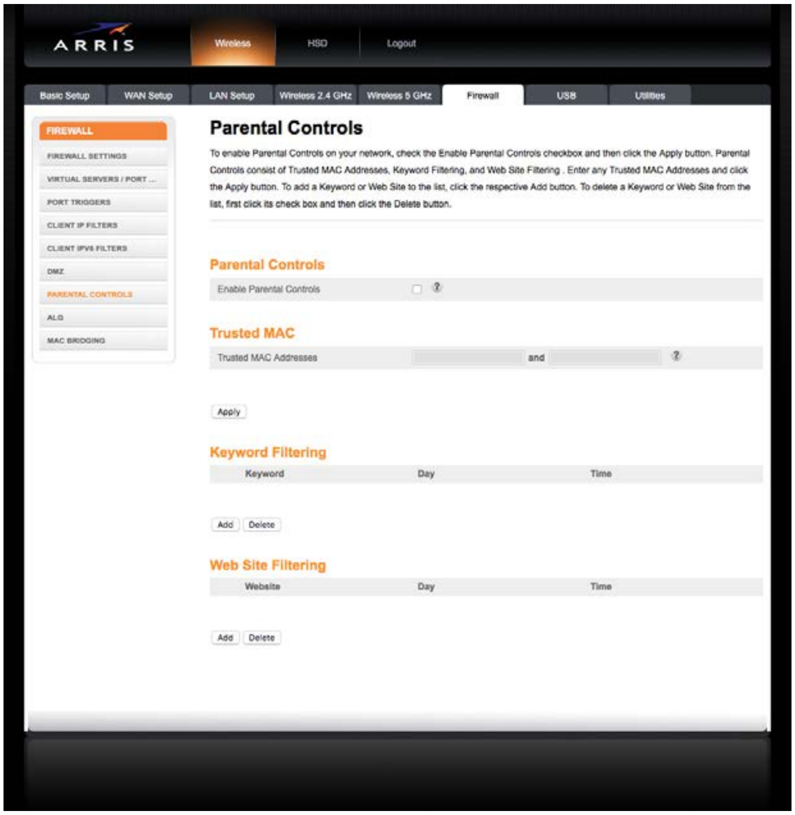
Enable DMZ – Check this box to enable DMZ on your network.

WAN IP – Displays the public IP address.

Private IP – Enter the IP address of the computer to be placed in the DMZ. Be sure that the address is not in the range of addresses delivered by the DHCP server if enabled. After placing the computer in the DMZ, all ports on the computer are open to the

Internet and not protected.

Firewall – Parental Controls



Parental Controls

To enable Parental Controls on your network, check the Enable Parental Controls checkbox and then click the Apply button. Parental Controls consist of Trusted MAC Addresses, Keyword Filtering, and Web Site Filtering . Enter any Trusted MAC Addresses and click the Apply button. To add a Keyword or Web Site to the list, click the respective Add button. To delete a Keyword or Web Site from the list, first click its check box and then click the Delete button.

Parental Controls

Enable Parental Controls □ ?

Trusted MAC

Trusted MAC Addresses ____ and ____ ?

Apply

Keyword Filtering

Keyword	Day	Time

Add Delete

Web Site Filtering

Website	Day	Time

Add Delete

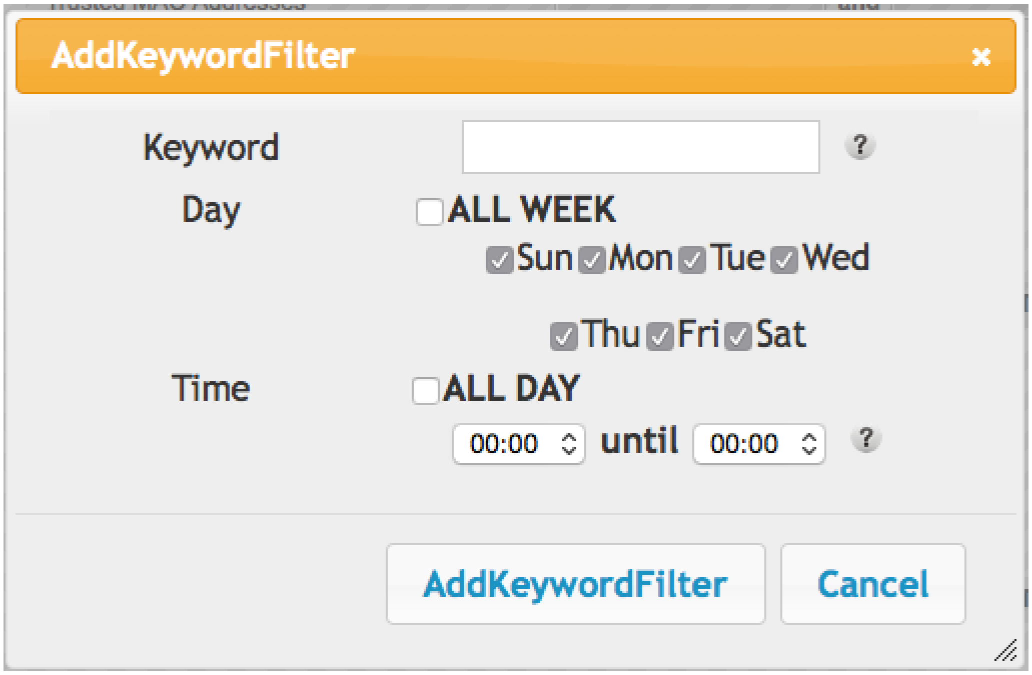
To enable Parental Controls on your network, check the **Enable Parental Controls** checkbox and then click the **Apply** button. Parental Controls consist of Trusted MAC Addresses, Keyword Filtering and Web Site Filtering. Enter any Trusted MAC Addresses and click the **Apply** button.

To add a Keyword or Web Site filter to the list, click the respective **Add** button. To delete a Keyword or Web Site from the list, first click its checkbox and then click the **Delete** button.

Trusted MAC:

Trusted MAC Addresses – Enter the trusted MAC addresses. These MAC addresses are not affected by Parental Control settings. You can add a total of two trusted MAC addresses. If the Trusted MAC Addresses fields are left empty, all source MAC addresses are trusted.

Keyword Filtering:



Keyword

Day □ ALL WEEK
☑ Sun ☑ Mon ☑ Tue ☑ Wed
☑ Thu ☑ Fri ☑ Sat

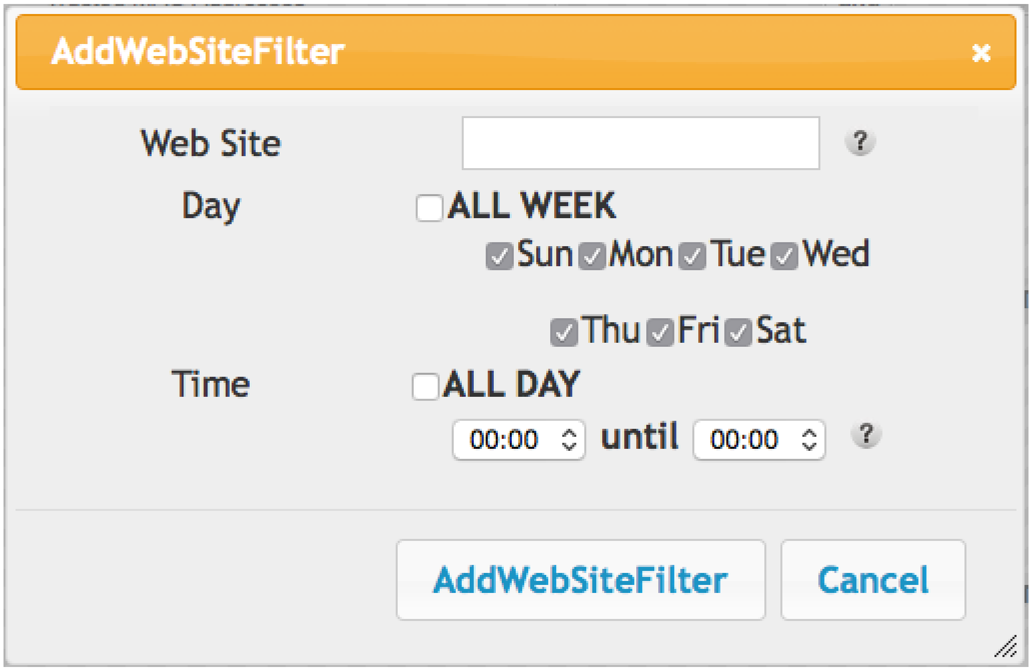
Time □ ALL DAY
00:00 until 00:00

Keyword – Enter a keyword that you want to filter out.

Day – Click the check boxes for the days you want access blocked, or click the All Week checkbox for all week.

Time – Sets the start time and end time for the blocked access during the specified days (24-hour clock). 00:00 to 24:00 indicates all day, or click the checkbox for All Day.

Web Site Filtering:



Web Site

Day □ ALL WEEK
☑ Sun ☑ Mon ☑ Tue ☑ Wed
☑ Thu ☑ Fri ☑ Sat

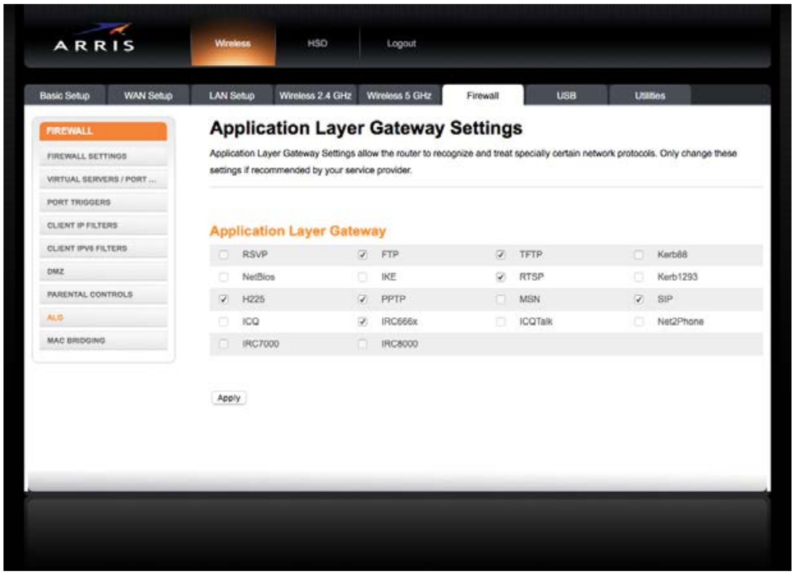
Time □ ALL DAY
00:00 until 00:00

Web Site – Enter the domain name of a web site that you want to filter out.

Day – Click the check boxes for the days you want access blocked, or click the All Week checkbox for all week.

Time – Sets the start time and end time for the blocked access during the specified days (24-hour clock). 00:00 to 24:00 indicates all day, or click the checkbox for All Day.

Firewall – ALG Settings



Application Layer Gateway Settings

Application Layer Gateway Settings allow the router to recognize and treat specially certain network protocols. Only change these settings if recommended by your service provider.

Application Layer Gateway

☐ RSVP	☑ FTP	☑ TFTP	☐ Kerb88
☐ NetBios	☐ IKE	☑ RTSP	☐ Kerb1293
☑ H225	☑ PPTP	☐ MSN	☑ SIP
☐ ICQ	☑ IRC666x	☐ ICQTalk	☐ Net2Phone
☐ IRC7000	☐ IRC8000		

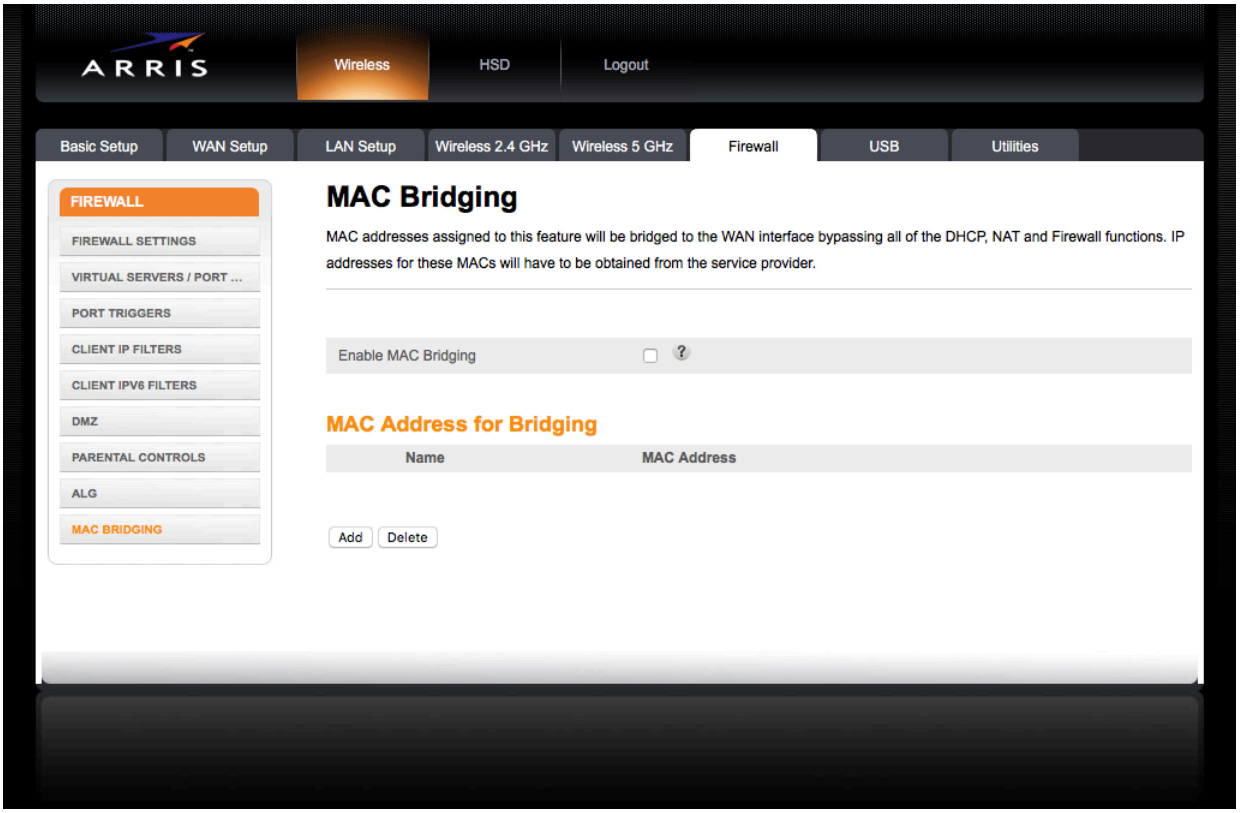
Application layer gateway settings allow the router to recognize and treat certain network protocols specially.

Application Layer Gateway:

Click the checkbox for each network protocol for which you want special handling.

Firewall - MAC Bridging

Note: This screen is not used on all models.



MAC Bridging

MAC addresses assigned to this feature will be bridged to the WAN interface bypassing all of the DHCP, NAT and Firewall functions. IP addresses for these MACs will have to be obtained from the service provider.

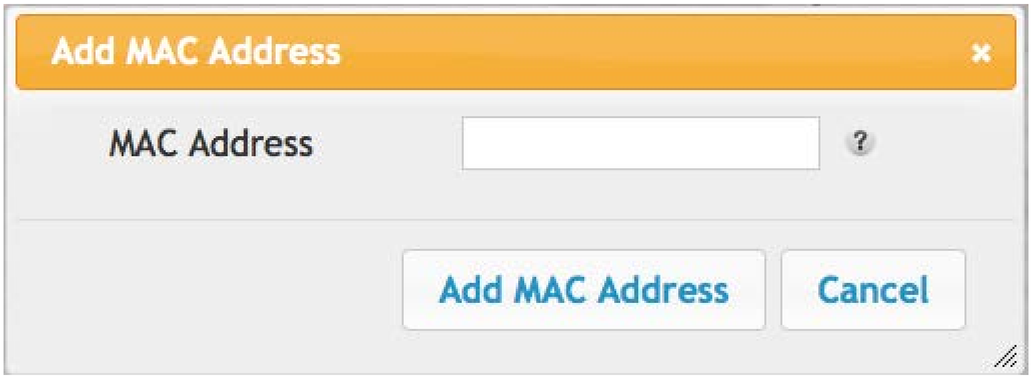
Enable MAC Bridging □ ?

MAC Address for Bridging

Name	MAC Address

Check the Enable MAC Bridging box to enable MAC bridging. The Gateway bridges devices with MAC addresses in the list to the WAN interface, bypassing router functions including DHCP, NAT, and firewall. Devices in this list must acquire IP addresses from the cable provider.

To add a device to the MAC Bridging list, click the **Add** button.



Add MAC Address

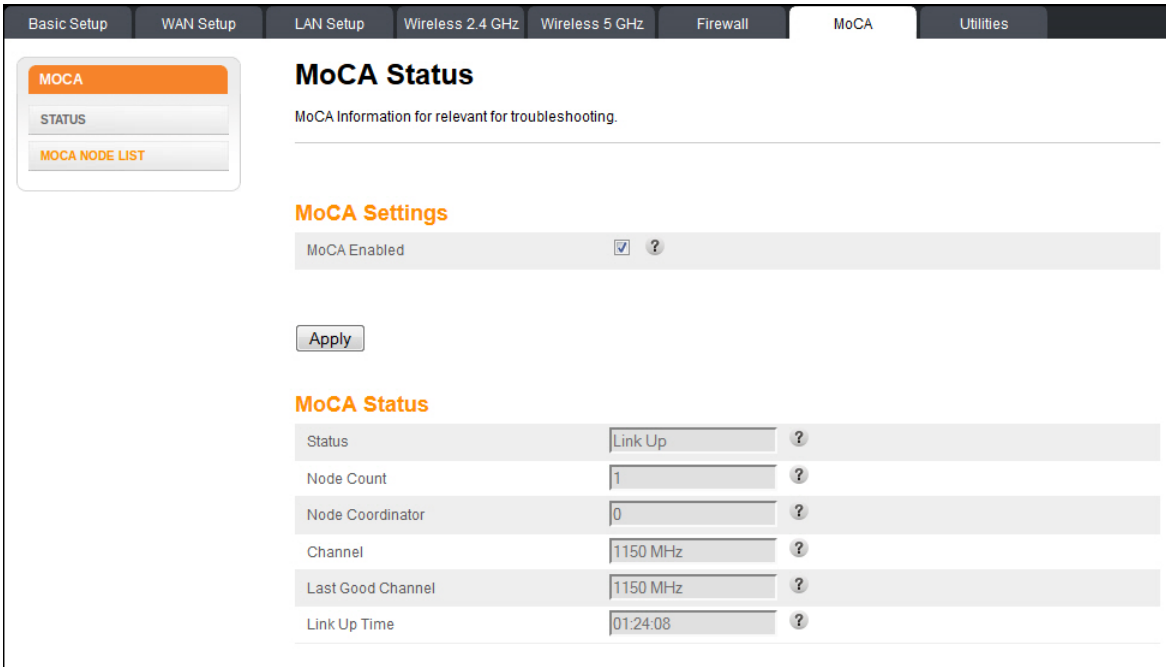
MAC Address

MAC Address – the MAC address of the device to be bridged. Verify that you have entered the address correctly, then click **Add MAC Address**.

To remove a device from the Bridging list, click **Delete**.

MoCA Status

MoCA is available on some Gateway products.



MoCA Status

MoCA Information for relevant for troubleshooting.

MoCA Settings

MoCA Enabled ☑ ?

MoCA Status

Status	Link Up
Node Count	1
Node Coordinator	0
Channel	1150 MHz
Last Good Channel	1150 MHz
Link Up Time	01:24:08

MoCA Settings:

MoCA Enabled – Check this box to enable MoCA on your system.

Note: This parameter may be set to a default by your service provider and not be user configurable.

MoCA Status:

Status – Displays the status of MoCA, either noLink, linkUp, or disable.

Node Count – Displays the number of nodes that this device communicates with in the MoCA network.

Node Coordinator – Displays the node ID of the network coordinator.

Channel – Displays the MoCA channel in MHz this interface is tuned to when part of a MoCA network. When not part of a MoCA network, this value may not indicate the actual tuned channel.

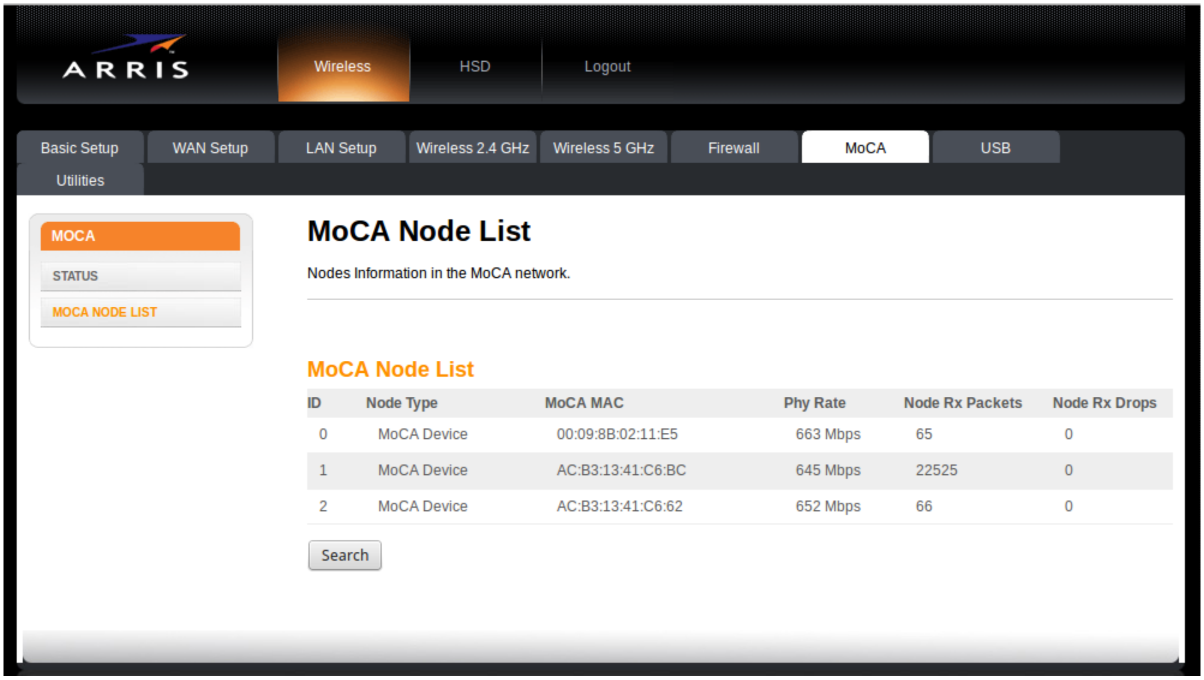
Last Good Channel – Displays the MoCA channel this interface was tuned to when it was last in the linkUp state.

LinkUp Time – Displays the total time in seconds this interface is part of a MoCA network.

MoCA Node List

The devices table lists the ID, node type, MAC address, and performance data (if any is available) of the nodes.

Note: Depending on the number of devices and network status, it may take up to several minutes to display the node list.



MoCA Node List

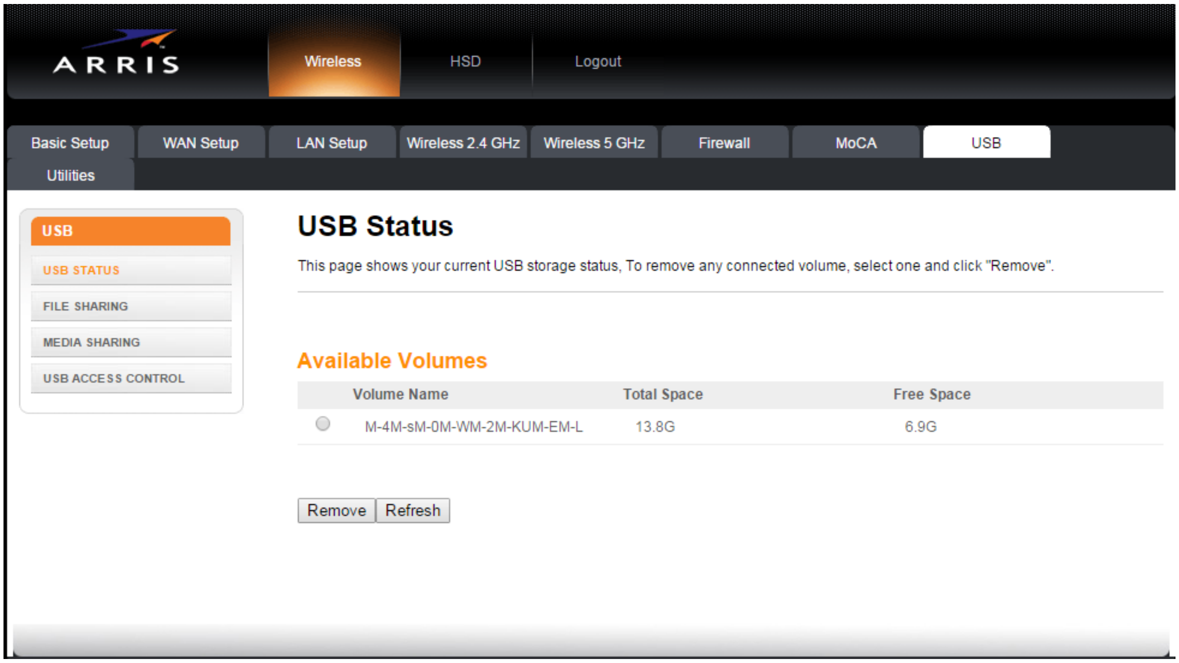
Nodes Information in the MoCA network.

MoCA Node List

ID	Node Type	MoCA MAC	Phy Rate	Node Rx Packets	Node Rx Drops
0	MoCA Device	00:09:8B:02:11:E5	663 Mbps	65	0
1	MoCA Device	AC:B3:13:41:C6:BC	645 Mbps	22525	0
2	MoCA Device	AC:B3:13:41:C6:62	652 Mbps	66	0

USB

USB - USB Status



USB Status

This page shows your current USB storage status, To remove any connected volume, select one and click "Remove".

Available Volumes

	Volume Name	Total Space	Free Space
○	M-4M-sM-0M-WM-2M-KUM-EM-L	13.8G	6.9G

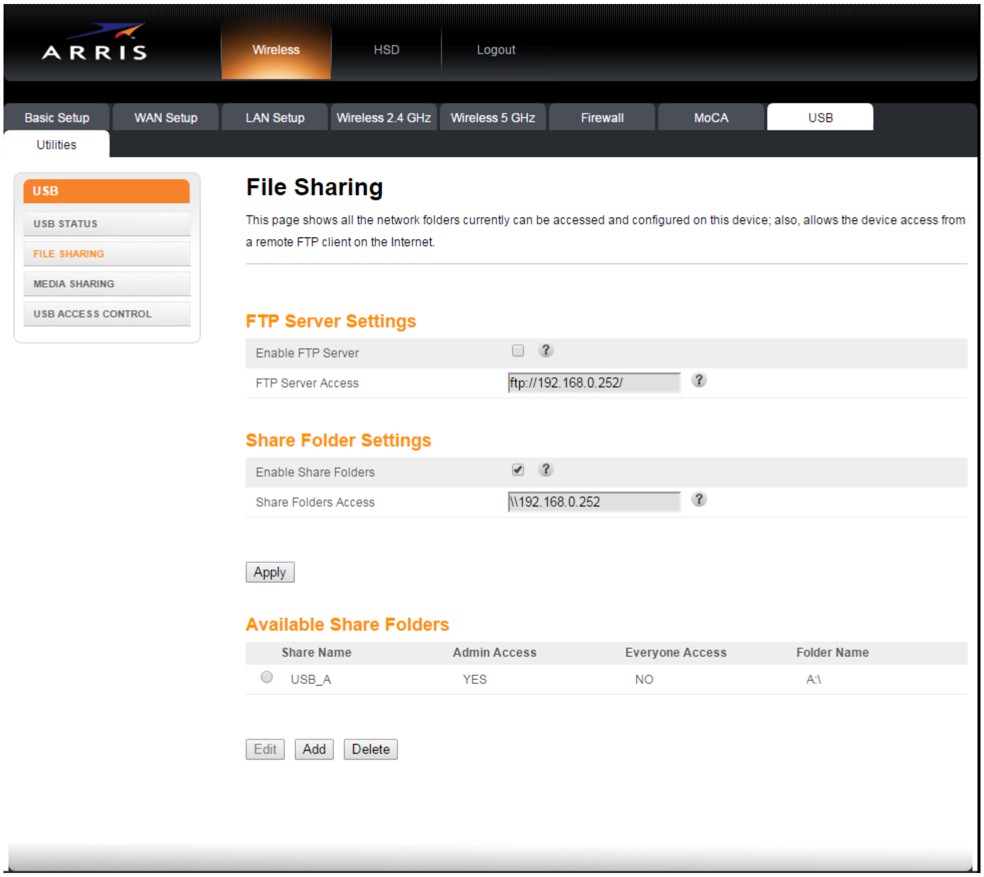
The USB Status screen shows connected hard drives and displays the following information:

- name
- total space on drive
- free space on drive

You can unmount a drive from this screen by clicking the checkbox next to the drive and clicking the **Remove** button.

Click the **Refresh** button to reload the information. You may need this if you attach a drive while displaying this screen.

USB - File Sharing



File Sharing

This page shows all the network folders currently can be accessed and configured on this device; also, allows the device access from a remote FTP client on the Internet.

FTP Server Settings

Enable FTP Server	□
FTP Server Access	ftp://192.168.0.252/

Share Folder Settings

Enable Share Folders	☑
Share Folders Access	\\192.168.0.252

Available Share Folders

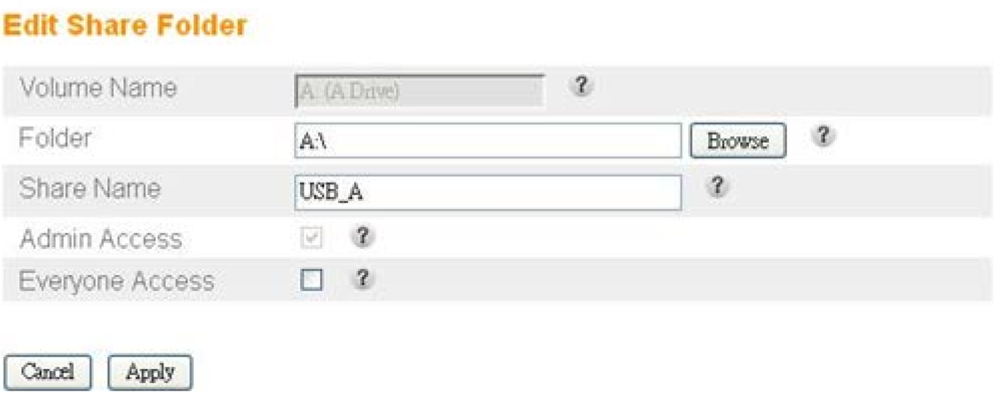
	Share Name	Admin Access	Everyone Access	Folder Name
○	USB_A	YES	NO	A:\

The File Sharing screen controls two types of file sharing for connected USB drives:

- Share Folder Settings—when enabled, the Touchstone Gateway provides a Windows-compatible network folder. The Available Share Folders list shows currently accessible folders, and allows adding or removing folder access as described below.
- FTP Server Settings—when enabled, the Touchstone Gateway provides an FTP server.

Editing a Shared Folder

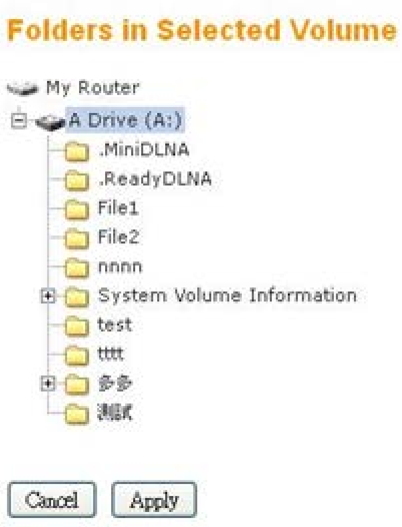
When you click the **Edit** button under Available Share Folders, the following fields appear:



Edit Share Folder

Volume Name	A: (A Drive)
Folder	A:\
Share Name	USB_A
Admin Access	☑
Everyone Access	□

These fields allow setting share names, access, and drives (if two or more drives are chained together). Drives are named beginning with A:\. Click the **Browse** button to display folders in the selected drive:



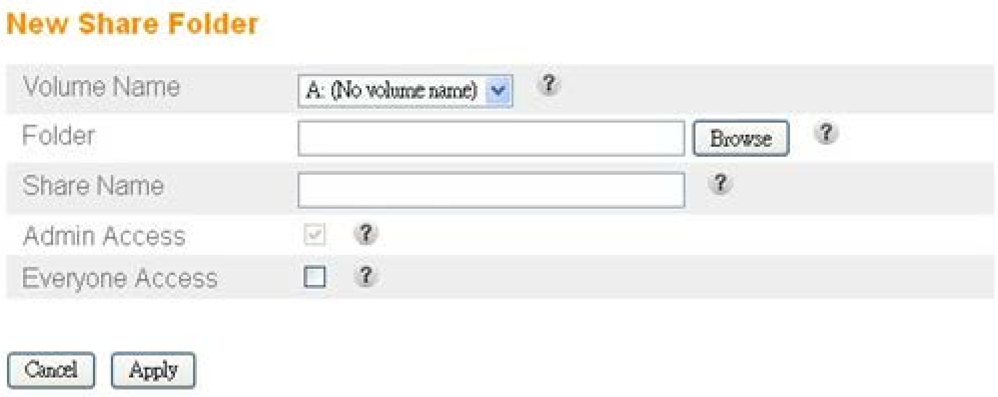
Folders in Selected Volume

- My Router
  - A Drive (A:)
    - .MiniDLNA
    - .ReadyDLNA
    - File1
    - File2
    - nnnn
    - System Volume Information
    - test
    - tttt
    - 多多
    - 測試

Select the folder and click the **Apply** button.

Defining a Shared Folder

When you click the **New** button under Available Share Folders, the following fields appear:

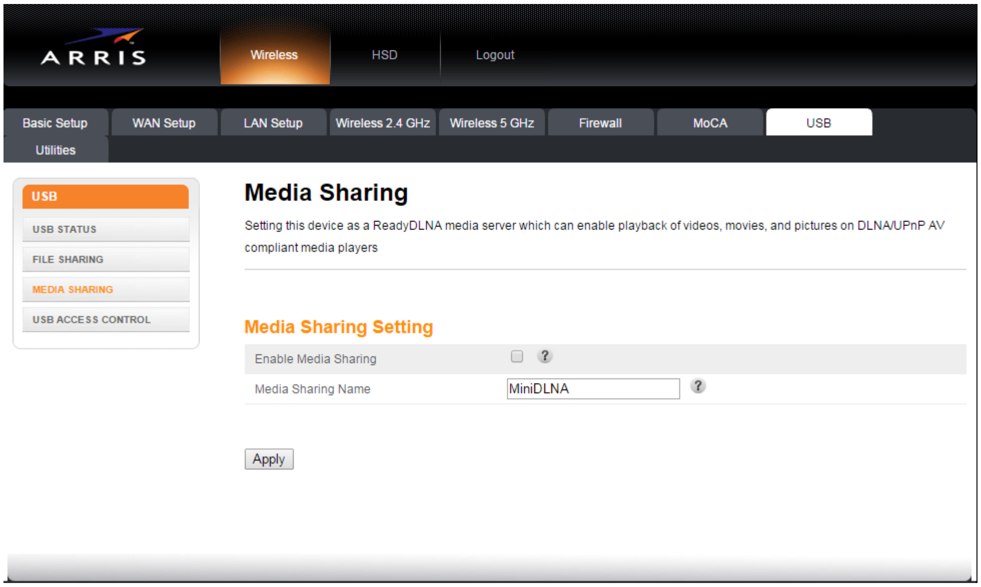


New Share Folder

Volume Name	A: (No volume name)
Folder	
Share Name	
Admin Access	☑
Everyone Access	□

These fields allow defining a new shared folder. Click the **Browse** button to display folders in the selected drive, as shown above.

USB - Media Sharing



Media Sharing

Setting this device as a ReadyDLNA media server which can enable playback of videos, movies, and pictures on DLNA/UPnP AV compliant media players

Media Sharing Setting

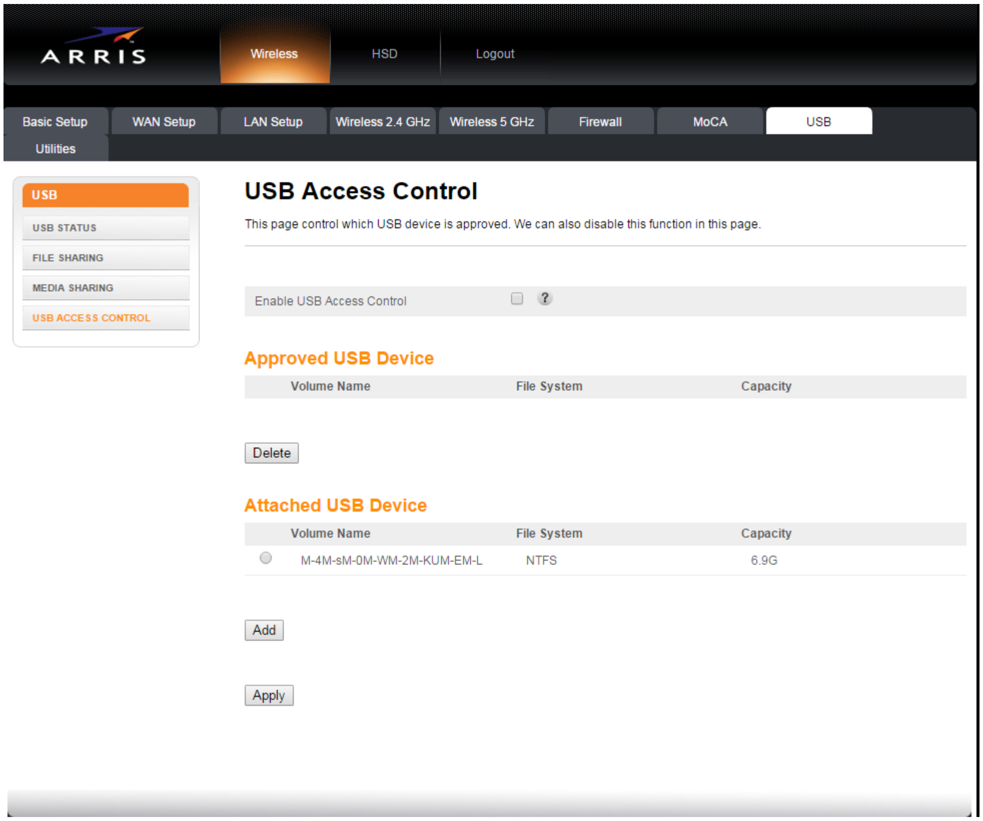
Enable Media Sharing	□ ?
Media Sharing Name	MiniDLNA ?

The Media Sharing screen controls streaming media (such as video or music) from attached USB drives.

When enabled, the Media Sharing Settings show the name of the DLNA share name. DLNA-compatible client devices can access media files on the drive.

Note: only ASCII characters are supported for the Media Sharing Name.

USB - USB Access Control



USB Access Control

This page control which USB device is approved. We can also disable this function in this page.

Enable USB Access Control □ ?

Approved USB Device

Volume Name	File System	Capacity

Attached USB Device

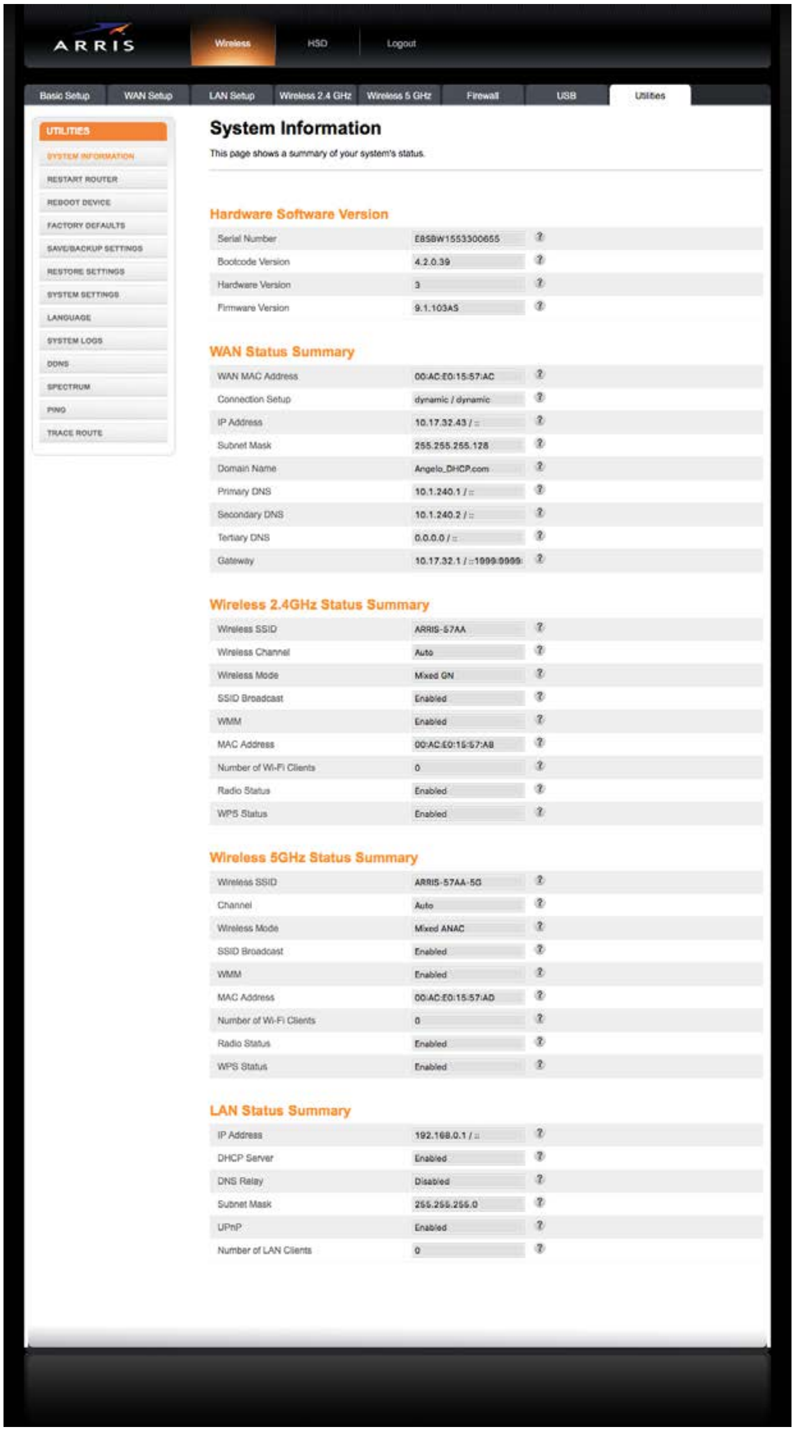
	Volume Name	File System	Capacity
○	M-4M-sM-0M-WM-2M-KUM-EM-L	NTFS	6.9G

The USB Access Control screen provides the following functions when enabled:

- Defines approved devices. USB drives not on this list are not recognized.
- Allows adding and removing approved devices on the list.

Utilities

Utilities – System Information



System Information

This page shows a summary of your system's status.

Hardware Software Version

Serial Number	E8SBW1553300655
Bootcode Version	4.2.0.39
Hardware Version	3
Firmware Version	9.1.103AS

WAN Status Summary

WAN MAC Address	00:AC:E0:15:57:AC
Connection Setup	dynamic / dynamic
IP Address	10.17.32.43 / ::
Subnet Mask	255.255.255.128
Domain Name	Angelo_DHCP.com
Primary DNS	10.1.240.1 / ::
Secondary DNS	10.1.240.2 / ::
Tertiary DNS	0.0.0.0 / ::
Gateway	10.17.32.1 / ::1999:9999:

Wireless 2.4GHz Status Summary

Wireless SSID	ARRIS-57AA
Wireless Channel	Auto
Wireless Mode	Mixed GN
SSID Broadcast	Enabled
WMM	Enabled
MAC Address	00:AC:E0:15:57:A8
Number of Wi-Fi Clients	0
Radio Status	Enabled
WPS Status	Enabled

Wireless 5GHz Status Summary

Wireless SSID	ARRIS-57AA-5G
Channel	Auto
Wireless Mode	Mixed ANAC
SSID Broadcast	Enabled
WMM	Enabled
MAC Address	00:AC:E0:15:57:AD
Number of Wi-Fi Clients	0
Radio Status	Enabled
WPS Status	Enabled

LAN Status Summary

IP Address	192.168.0.1 / ::
DHCP Server	Enabled
DNS Relay	Disabled
Subnet Mask	255.255.255.0
UPnP	Enabled
Number of LAN Clients	0

This page shows a summary of your system's status.

Hardware Software Version:

Serial Number – The Gateway's serial number.

Bootcode Version – The Gateway's bootcode version.

Hardware Version – The Gateway's hardware version.

Firmware Version – The Gateway's firmware version.

WAN Status Summary:

WAN MAC Address – The Gateway's WAN MAC address.

Connection Setup – The WAN connection type: Dynamic or Static.

IP Address – The Gateway's WAN IP address.

Subnet Mask – The Gateway's WAN subnet mask.

Domain Name – The Gateway's domain name.

Primary DNS – The Gateway's Primary DNS IP address.

Secondary DNS – The Gateway's Secondary DNS IP address.

Tertiary DNS – The Gateway's Tertiary DNS IP address.

Gateway – The Gateway's IP address.

Wireless 2.4 GHz Status Summary:

Wireless SSID – The Service Set Identifier (SSID), which is the wireless network name.

Wireless Channel – The 2.4 GHz channel your Gateway is using.

Wireless Mode – The wireless mode: B/G mixed, B only, G only, N only, A only, G/N mixed, A/N mixed, or B/G/N mixed.

SSID Broadcast – The status of the SSID Broadcast function: Enabled or Disabled.

WMM – The status of the Wi-Fi Multimedia (WMM) function: Enabled or Disabled.

MAC Address – The wireless router's MAC Address.

Number of WiFi Clients – The number of 2.4 GHz wireless client devices connected to the Gateway.

Radio Status – The status of the wireless radio: Enabled or Disabled.

WPS Status – The status of the WPS function: Enabled or Disabled.

Wireless 5 GHz Status Summary:

Wireless SSID – The Service Set Identifier (SSID), which is the wireless network name.

Wireless Channel – The 5 GHz channel your Gateway is using.

Wireless Mode – The wireless mode: A/N mixed, A only, N only, AC only, N/AC mixed, or A/N/AC mixed.

SSID Broadcast – The status of the SSID Broadcast function: Enabled or Disabled.

WMM – The Wi-Fi Multimedia (WMM) function: Enabled or Disabled.

MAC Address – The wireless adapter MAC Address.

Number of Wi-fi Clients – The number of 5 GHz wireless client devices connected to the Gateway.

Radio Status – The status of the wireless radio: Enabled or Disabled.

WPS Status – The status of the WPS function: Enabled or Disabled.

LAN Status Summary:

IP Address – The IP Address of your LAN.

DHCP Server – The status of the DHCP Server: Enabled or Disabled.

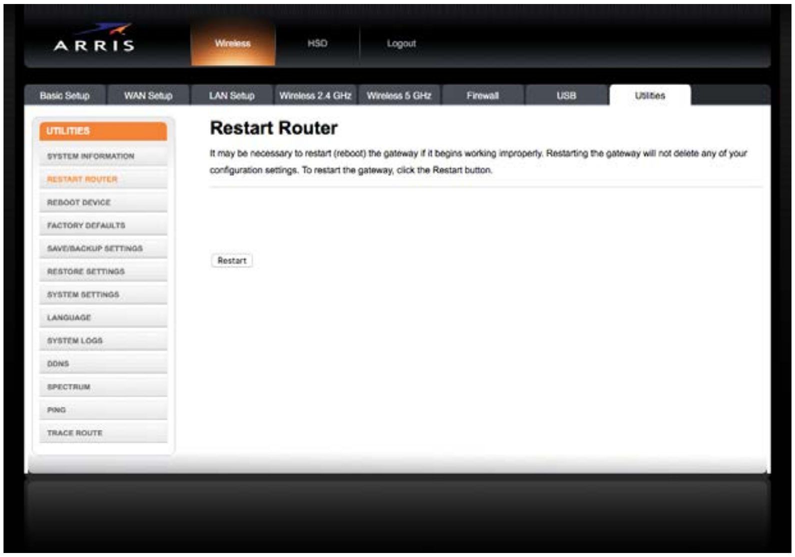
DNS Relay – The status of the DNS Relay function: Enabled or Disabled.

Subnet Mask – The subnet mask of your LAN.

UPnP – The status of the UPnP feature: Enabled or Disabled.

Number of LAN Clients – The number of LAN client devices connected to the Gateway.

Utilities – Restart Router



Restart Router

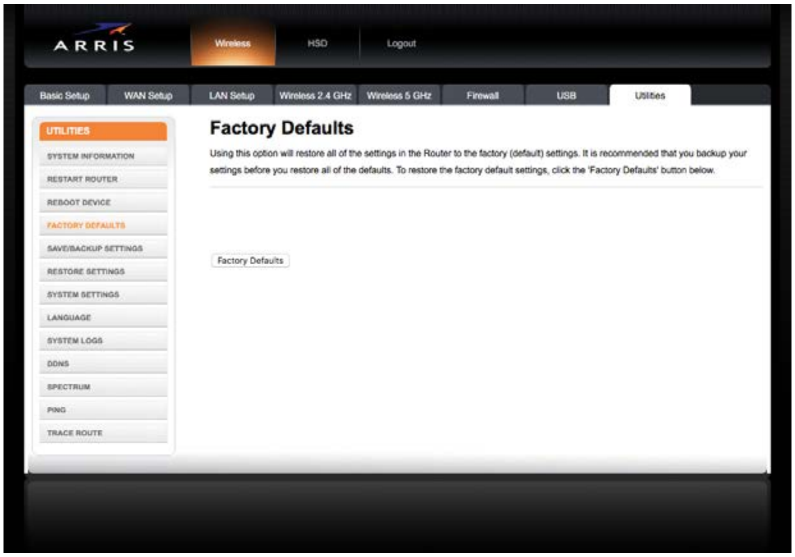
It may be necessary to restart (reboot) the gateway if it begins working improperly. Restarting the gateway will not delete any of your configuration settings. To restart the gateway, click the Restart button.

It may be necessary to restart (reboot) the router if it begins working improperly. Restarting the router does not delete any of your configuration settings.

To restart the router, click the **Restart** button.

Note: A dialog box displays "This will restart your router. Current connections and telephony may be interrupted." Click **OK** to restart now or click **Cancel** to restart later.

Utilities – Factory Defaults



Factory Defaults

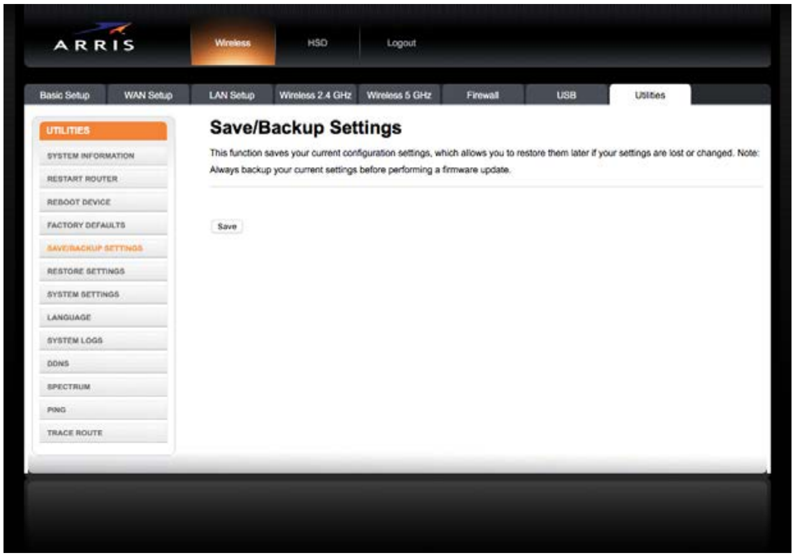
Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults. To restore the factory default settings, click the 'Factory Defaults' button below.

This function restores all of the router's configuration settings to the factory default setting. Before restoring the factory defaults, you should back up your current configuration settings using the Save/Backup Settings page.

Click the **Factory Defaults** button to restore the factory default configuration settings.

Note: A dialog box displays "This will restore your router to its factory state. Any customizations you have made will be lost. Current connections and telephony may be interrupted." Click **OK** to restore now or click **Cancel** to restore later.

Utilities – Save/Backup Settings



Save/Backup Settings

This function saves your current configuration settings, which allows you to restore them later if your settings are lost or changed. Note: Always backup your current settings before performing a firmware update.

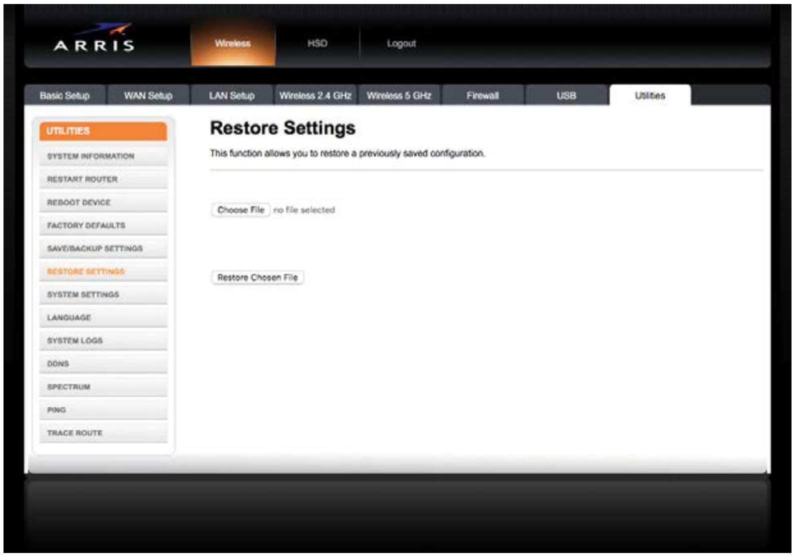
This function saves your current configuration settings, which allows you to restore them later if your settings are lost or changed. Click the **Save** button to backup your current settings.

Note: A dialog box displays "This will take a few minutes. Continue? Click OK to save settings now or click Cancel to save later."

When saving, follow the "file download" and "save as" dialog box instructions for your specific browser to select a location to save the `router.data` backup file.

Important: Always backup your current settings before performing a firmware update.

Utilities – Restore Settings



Restore Settings

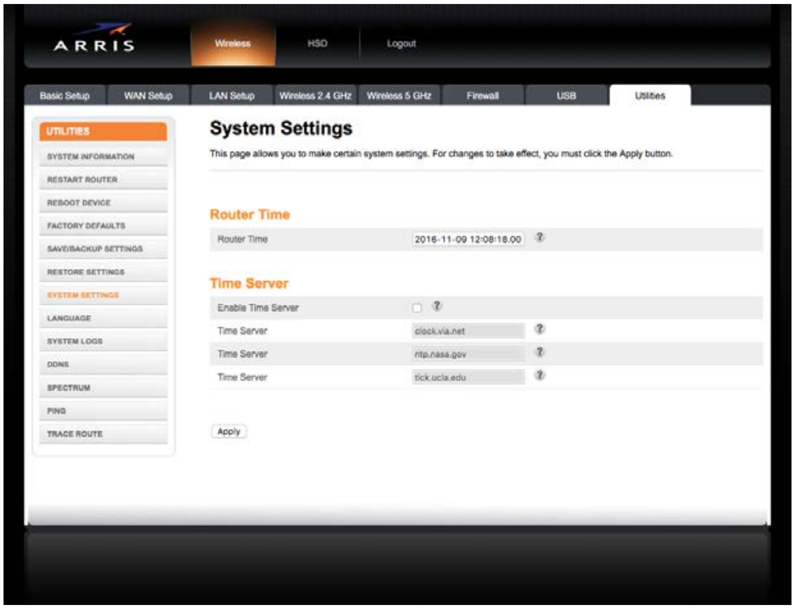
This function allows you to restore a previously saved configuration.

This function allows you to restore a previously saved configuration.

To restore a previous configuration: Use the **Browse** button to locate and select the previously saved backup file. Then click the **Restore Chosen File** button.

Note: A dialog box displays "This will restore your router's saved state. Current connections, recordings, and telephony may be interrupted." Click **OK** to restore now or click **Cancel** to restore later.

Utilities – System Settings



System Settings

This page allows you to make certain system settings. For changes to take effect, you must click the Apply button.

Router Time

Router Time 2016-11-09 12:08:18.00

Time Server

Enable Time Server □

Time Server clock.via.net

Time Server ntp.nasa.gov

Time Server tick.ucla.edu

This page allows you to make certain system settings. For changes to take effect, you must click the **Apply** button.

Router Time:

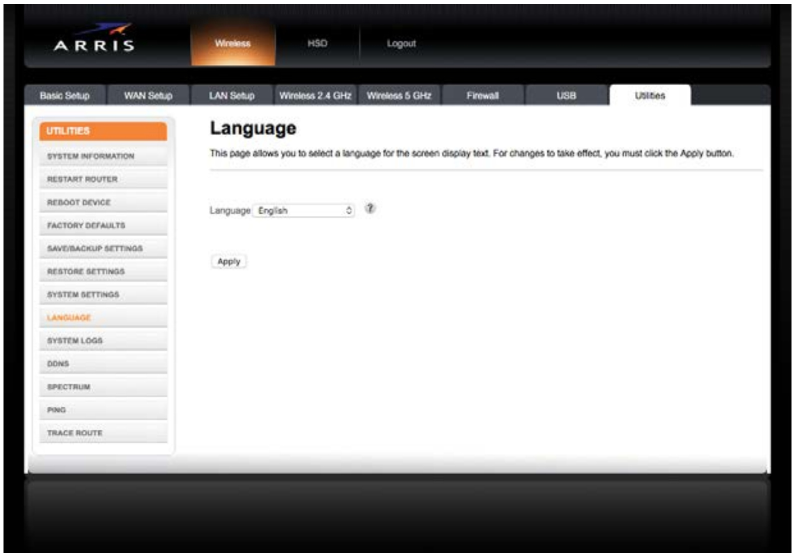
Router Time – Date and time on the router. (yyyy-mm-dd hh:mm:ss.ss)

Time Server:

Enable Time Server – Check this box to set the time via these servers.

Time Server – The host name or IP address of up to three time servers.

Utilities – Language

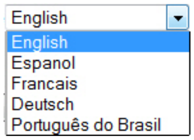


Language

This page allows you to select a language for the screen display text. For changes to take effect, you must click the Apply button.

Language English

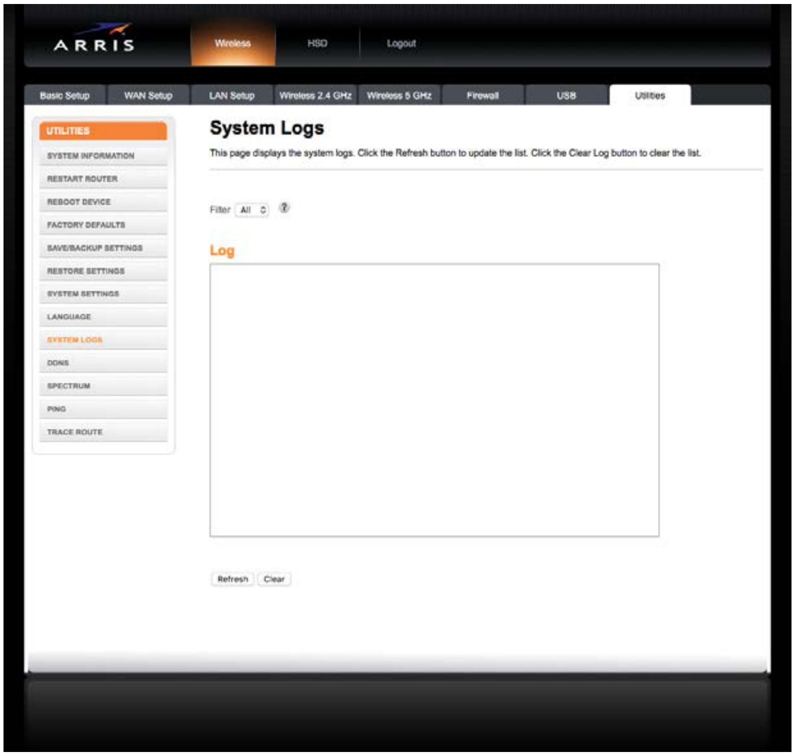
This page allows you to select a language for the screen display text. Click the arrow to display the drop-down list.



For changes to take effect, you must click the **Apply** button.

Language – Sets the language for the screen display text.

Utilities – System Logs



System Logs

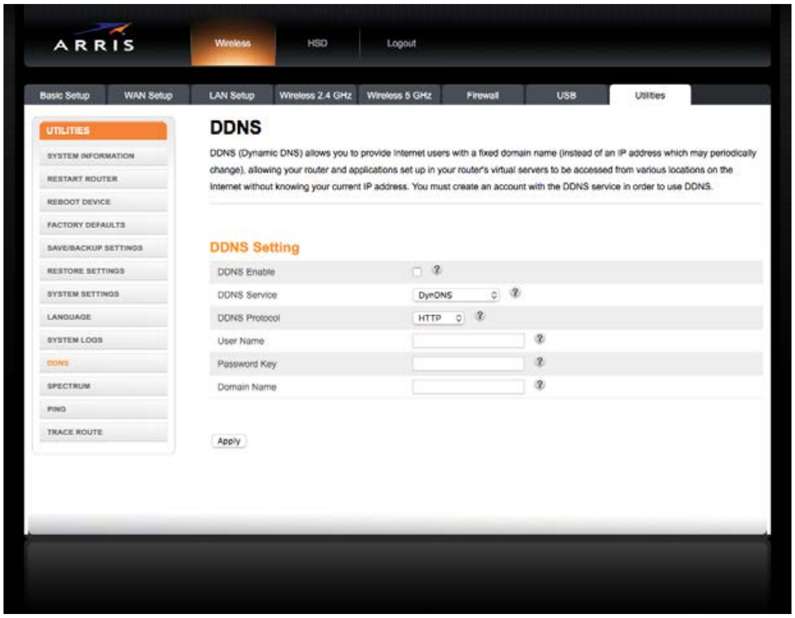
This page displays the system logs. Click the Refresh button to update the list. Click the Clear Log button to clear the list.

Filter All

Log:

This page displays the system logs. Click the **Refresh** button to update the list. Click the **Clear** Log button to clear the list.

Utilities – DDNS



DDNS

DDNS (Dynamic DNS) allows you to provide Internet users with a fixed domain name (instead of an IP address which may periodically change), allowing your router and applications set up in your router's virtual servers to be accessed from various locations on the Internet without knowing your current IP address. You must create an account with the DDNS service in order to use DDNS.

DDNS Setting

DDNS Enable	□
DDNS Service	DynDNS
DDNS Protocol	HTTP
User Name	
Password Key	
Domain Name	

DDNS (Dynamic DNS) allows you to provide Internet users with a fixed domain name (instead of an IP address which may periodically change). This allows your gateway and applications set up in your gateway's virtual servers to be accessed from various locations on the Internet without knowing your current IP address. For changes to take effect, you must click the Apply button.

Note: You must first create an account with a DDNS provider in order to use DDNS. The DDNS provider maps your chosen domain name to your IP address.

DDNS Setting:

DDNS Enable – Check this box to enable DDNS on your system.

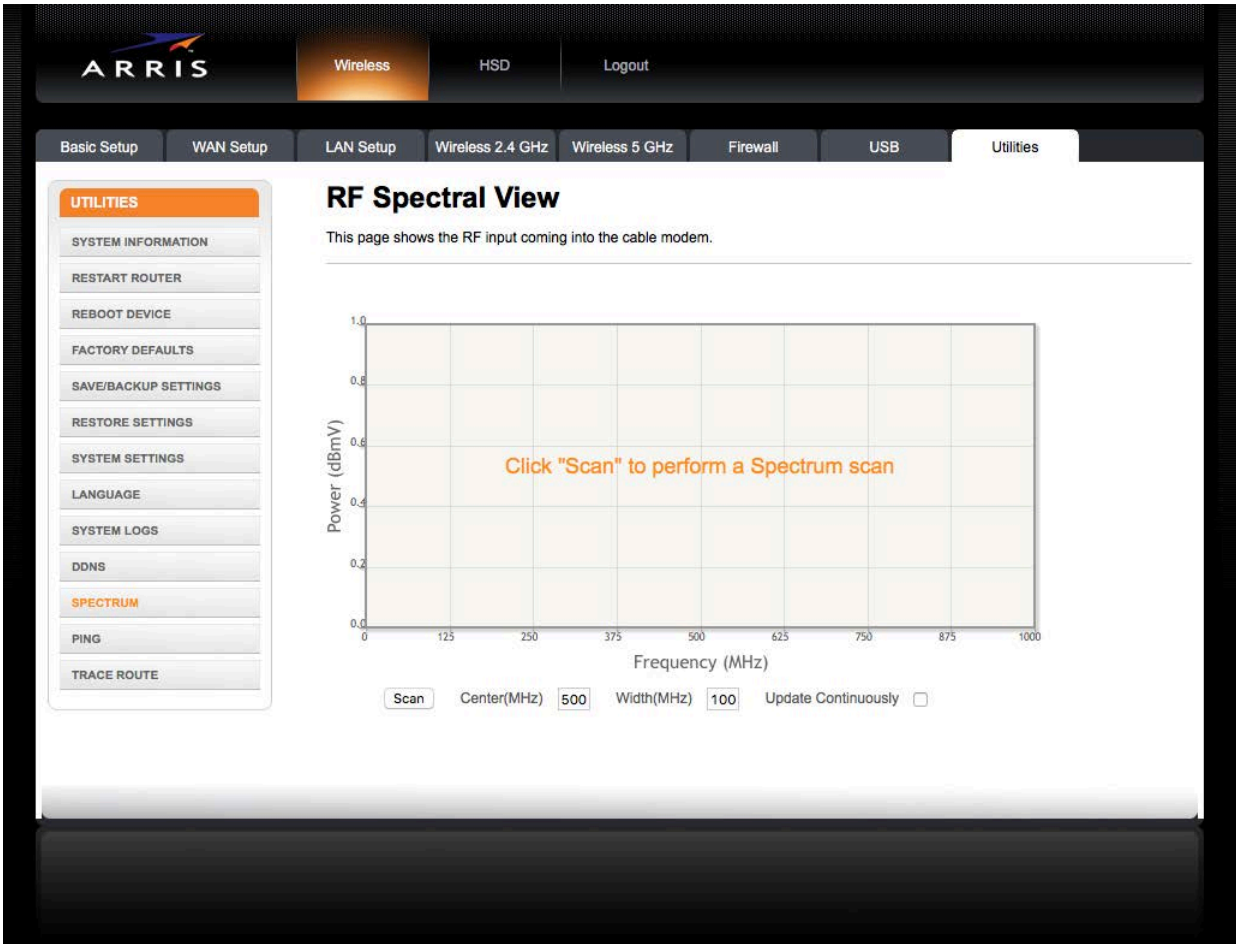
DDNS Service – Sets the DDNS provider that our account is with. The options are DynDNS, TZO, FreeDNS, ZoneEdit, NoIP, EasyDNS, or DomainsGoogle.

User Name – Enter the user name for your DDNS account.

Password Key – Enter the password for your DDNS account. (Provided by your DDNS provider.)

Domain Name – Enter the domain name you selected to use with your DDNS account.

Utilities - RF Spectral View



RF Spectral View

This page shows the RF input coming into the cable modem.

Click "Scan" to perform a Spectrum scan

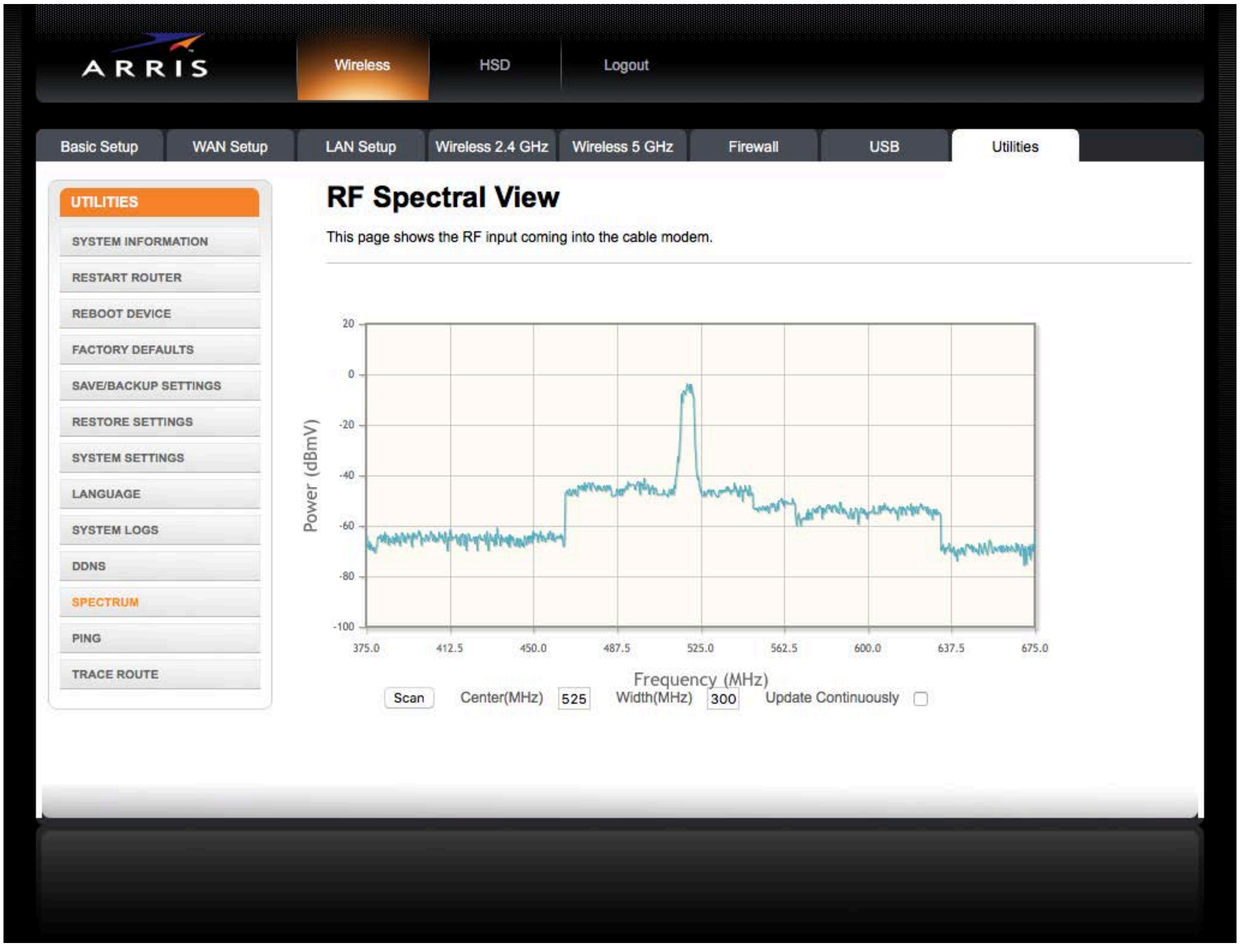
Center(MHz) 500 Width(MHz) 100 Update Continuously □

Center (MHz) – the frequency to place at the center of the graph. For best results, the selected frequency should be a multiple of 6 (for North American DOCSIS) or 8 (for Euro-DOCSIS).

Width (MHz) – the bandwidth to display. All Gateways with this screen can show downstream frequencies; Model 16 and newer Gateways can also show upstream frequencies.

Update Continuously – check this box to have the Spectrum Analyzer run until you exit the page.

When you have filled in the fields, click **Scan**. It may take several seconds for the Gateway to display the results.

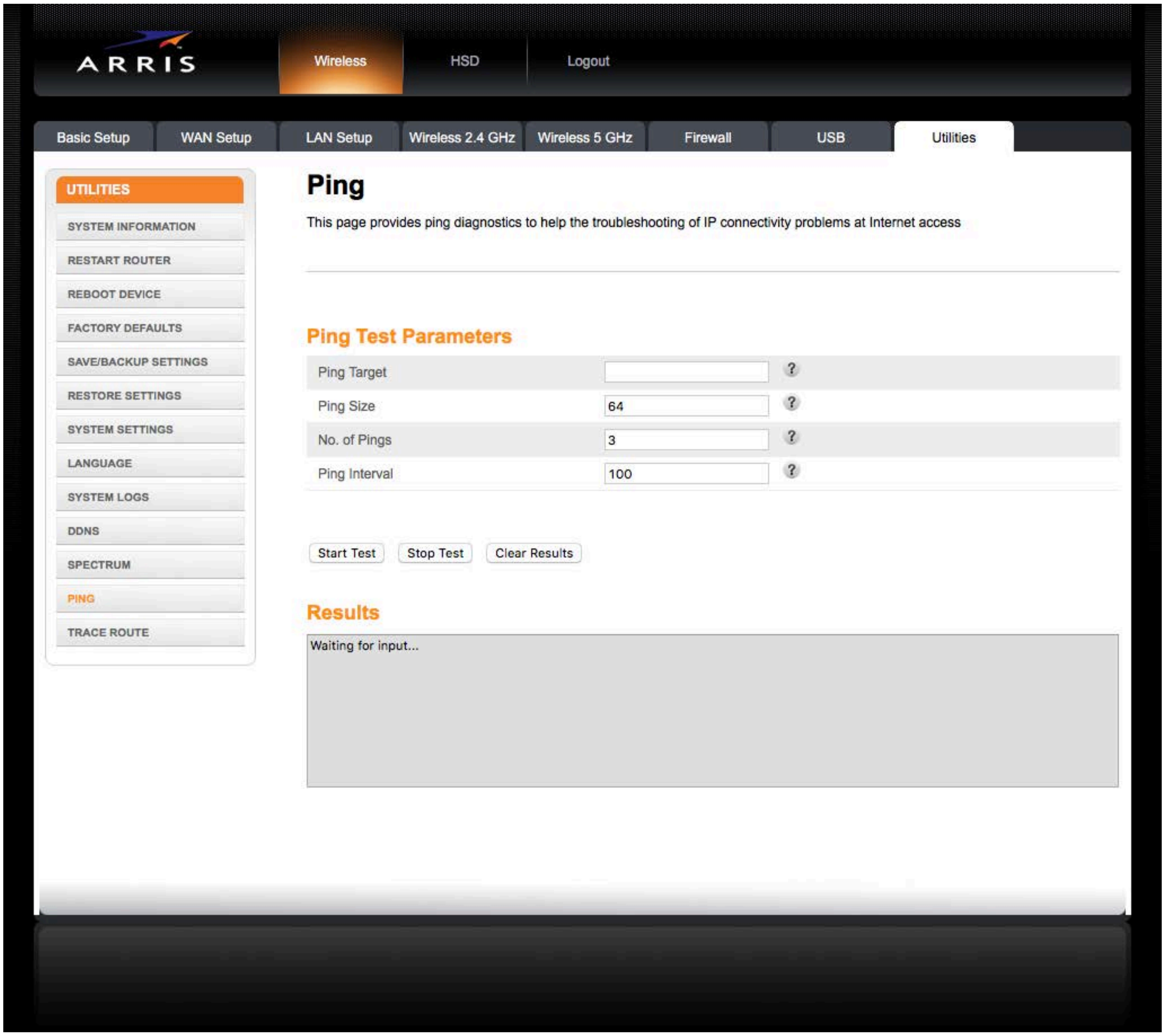


RF Spectral View

This page shows the RF input coming into the cable modem.

Center(MHz) 525 Width(MHz) 300 Update Continuously □

Utilities - Ping



Ping

This page provides ping diagnostics to help the troubleshooting of IP connectivity problems at Internet access

Ping Test Parameters

Ping Target	
Ping Size	64
No. of Pings	3
Ping Interval	100

Results

```
Waiting for input...
```

This page allows you to test connectivity using the standard Ping mechanism.

Ping Test Parameters:

Ping Target – The IP address of a remote site. The site must allow Pings.

Ping Size – The size of the UDP Echo (ping) packet, in bytes. The default is 64. Larger packet sizes can be used to test high-bandwidth connections, or to verify that the remote site is not vulnerable to certain Ping-based attacks.

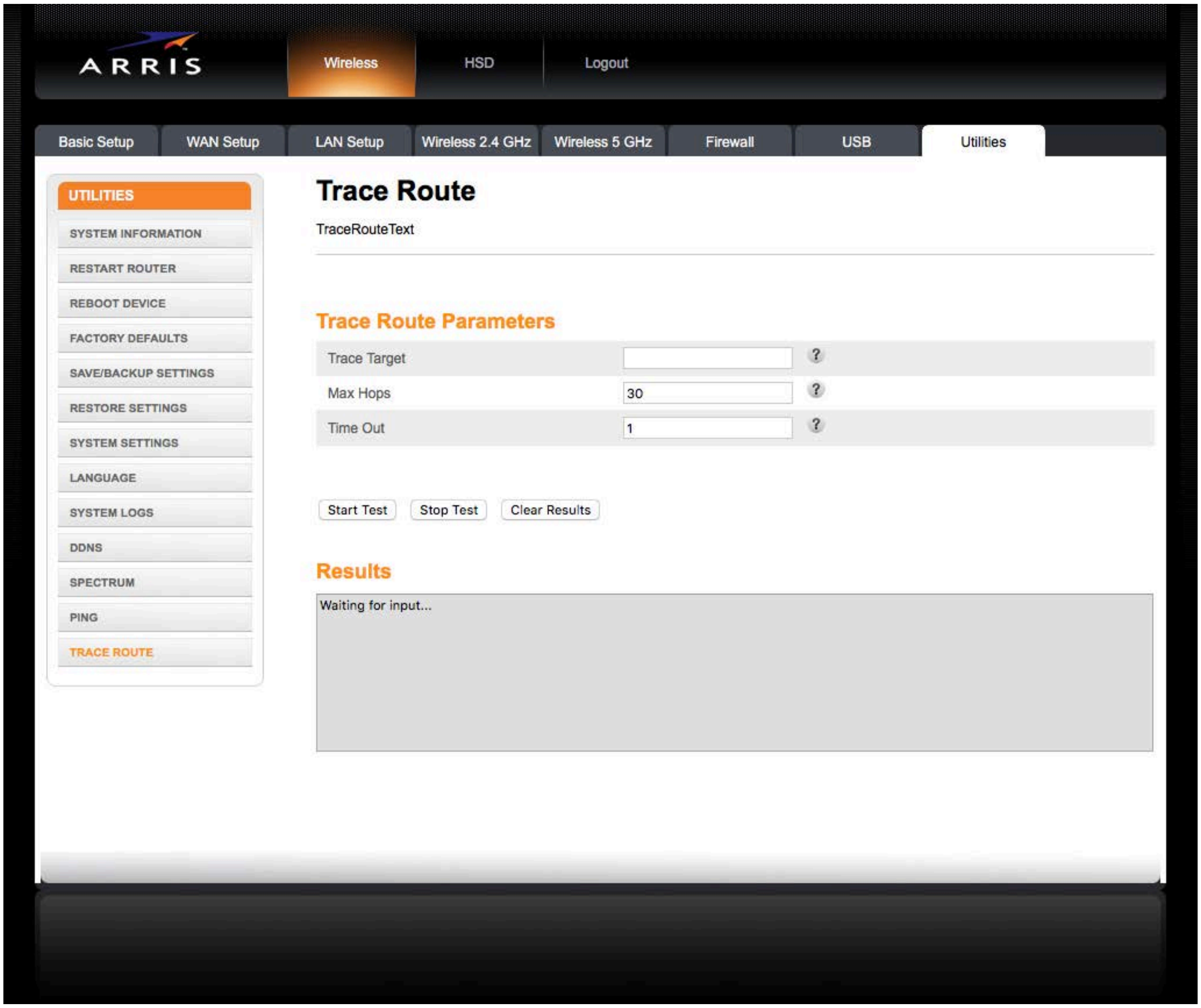
No. of Pings – The number of Ping packets to send.

Ping Interval – The time, in seconds, between pings.

Click **Start Test** to begin the test. Click **Stop Test** to end the test.

The **Clear Results** button erases the output in the Results text box.

Utilities - Trace Route



Trace Route

TraceRouteText

Trace Route Parameters

Trace Target	
Max Hops	30
Time Out	1

Results

Waiting for input...

This utility tests connectivity by recording the routers (hops) the data goes through to reach the destination.

Trace Route Parameters:

Trace Target – The IP address of the destination.

Max Hops – The maximum number of intermediate routers (hops) before the Gateway terminates the test.

Time Out – The timeout period, in seconds, to receive responses from a hop before moving to the next hop.

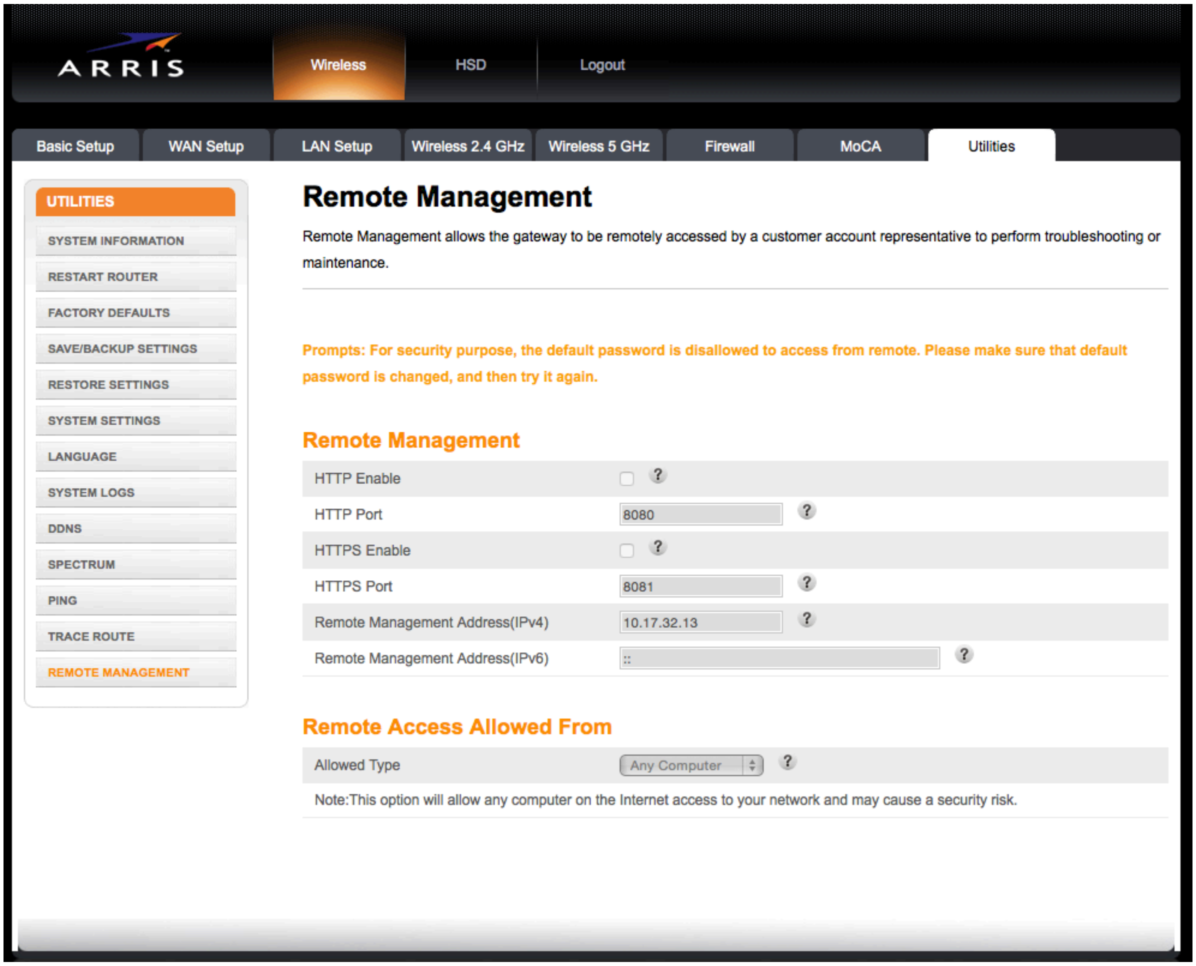
Adjust the parameters as needed, then click **Start Test** to begin the traceroute. Click **Stop Test** to quit.

To erase text in the Results text box, click **Clear Results**.

Note: some hops may display "* * *" in place of response times. This happens when the Trace Route utility does not receive a response before the timeout, or when that router has Ping disabled.

Utilities - Remote Management

Note: Remote Management is not available on all Gateway products.



Remote Management

Remote Management allows the gateway to be remotely accessed by a customer account representative to perform troubleshooting or maintenance.

Prompts: For security purpose, the default password is disallowed to access from remote. Please make sure that default password is changed, and then try it again.

Remote Management

HTTP Enable	□ ?
HTTP Port	8080 ?
HTTPS Enable	□ ?
HTTPS Port	8081 ?
Remote Management Address(IPv4)	10.17.32.13 ?
Remote Management Address(IPv6)	:: ?

Remote Access Allowed From

Allowed Type	Any Computer ?

Note:This option will allow any computer on the Internet access to your network and may cause a security risk.

Remote Management allows a technician to troubleshoot or maintain the gateway from a remote location.

Remote Management fields:

HTTP Enable – Check this box to enable non-encrypted HTTP access.

HTTP Port – Enter the port used for remote HTTP access. Default: 8080.

HTTPS Enable – Check this box to enable encrypted HTTPS access.

HTTPS Port – Enter the port used for remote HTTPS access. Default: 8081.

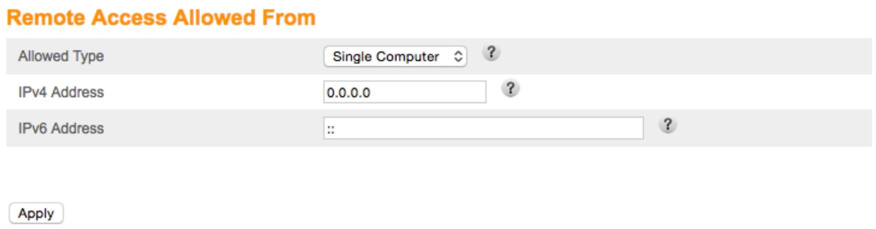
Remote Management Address (IPv4) – The IPv4 address used to access this Gateway.

Remote Management Address (IPv6) – The IPv6 address used to access this Gateway.

Remote Access Allowed From:

Allowed Type – Select one of:

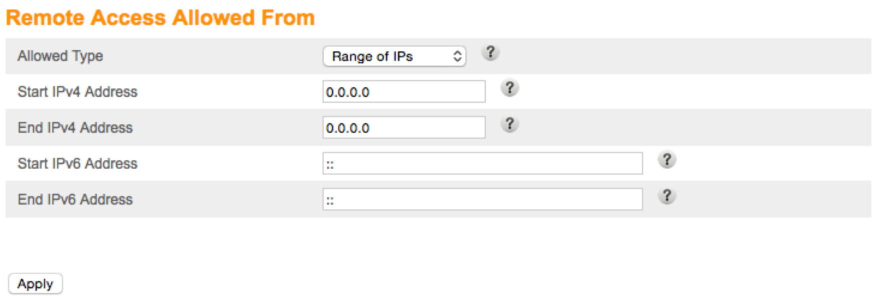
- Single Computer – Allow access only from the specified IP address. The following fields let you enter an IPv4 or IPv6 address of the remote device.



Remote Access Allowed From

Allowed Type	Single Computer
IPv4 Address	0.0.0.0
IPv6 Address	::

- Range of IPs – Allow access from any IP address in the specified range. The following fields let you enter the beginning and ending IPv4 or IPv6 addresses in the range.



Remote Access Allowed From

Allowed Type	Range of IPs
Start IPv4 Address	0.0.0.0
End IPv4 Address	0.0.0.0
Start IPv6 Address	::
End IPv6 Address	::

- Any Computer – Allow access from any computer.

When all fields are set properly, click the **Apply** button.

Note: You must change the "admin" password to something other than the default (password) to enable Remote Management or make changes to this screen.

Corporate Headquarters

ARRIS · Suwanee · Georgia · 30024 · USA

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

www.arris.com