SURFboard®

SBR-AC1750 Wireless Router

User Guide

DRAFT 1.0 March 2015

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

Chapter 1

Safety and Regulatory Information

Important Safety Instructions

- **Read This Before You Begin** — When using your equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock, and injury to persons, including the following:
- Read all of the instructions listed here and/or in the user manual before you operate this device. Give particular attention to all safety precautions. Retain the instructions for future reference.
- This device must be installed and used in strict accordance with manufacturer's instructions, as described in the user documentation that is included with the device.
- Comply with all warning and caution statements in the instructions. Observe all warning and caution symbols that are affixed to this device.
- To prevent fire or shock hazard, do not expose this device to rain or moisture. The device must not be exposed to dripping or splashing. Do not place objects filled with liquids, such as vases, on the device.
- This device was qualified under test conditions that included the use of the supplied cables between system components. To ensure regulatory and safety compliance, use only the provided power and interface cables and install them properly.
- Different types of cord sets may be used for connections to the main POWER supply circuit. Use only a main line cord that complies with all applicable device safety requirements of the country of use.
- Installation of this device must be in accordance with national wiring codes and conform to local regulations.
- Operate this device only from the type of power source indicated on the device's marking label. If you are not sure of the type of power supplied to your home, consult your dealer or local power company.
- Do not overload outlets or extension cords, as this can result in a risk of fire or electric shock. Overloaded AC outlets, extension cords, frayed power cords, damaged or cracked wire insulation, and broken plugs are dangerous. They may result in a shock or fire hazard.
- Route power supply cords so that they are not likely to be walked on or pinched by items placed upon or against them. Pay particular attention to cords where they are attached to plugs and convenience receptacles, and examine the point where they exit from the device.
- Place this device in a location that is close enough to an electrical outlet to accommodate the length of the power cord.
- Place the device to allow for easy access when disconnecting the power cord of the device from the AC wall outlet.
- Do not connect the plug into an extension cord, receptacle, or other outlet unless the plug can be fully inserted with no part of the blades exposed.
- Place this device on a stable surface.
- It is recommended that the customer install an AC surge protector in the AC outlet to which this device is connected. This is to avoid damaging the device by local lightning strikes and other electrical surges.
- Postpone installation until there is no risk of thunderstorm or lightning activity in the area.
- Do not use this product near water: for example, near a bathtub, washbowl, kitchen sink or laundry tub, in a wet basement, or near a swimming pool.
- Do not cover the device or block the airflow to the device with any other objects. Keep the device away from excessive heat and humidity and keep the device free from vibration and dust.
- Wipe the device with a clean, dry cloth. Never use cleaning fluid or similar chemicals. Do not spray cleaners directly on the device or use forced air to remove dust.
- For added protection, unplug the device from the wall outlet and disconnect the cables to avoid damage to this device due to lightning and power surges.
- Upon completion of any service or repairs to this device, ask the service technician to perform safety checks to determine that the device is in safe operating condition.
- Do not open the device. Do not perform any servicing other than that contained in the installation and troubleshooting instructions. Refer all servicing to qualified service personnel.
- This device should not be used in an environment that exceeds 104º F (40º C).

SAVE THE ABOVE INSTRUCTIONS

Note to CATV System Installer — This reminder is provided to call the CATV system installer's attention to Article 820.93 and 820.100 of the National Electric Code, which provides guidelines for proper grounding and, in particular, specifies that the Coaxial cable shield shall be connected to the grounding system of the building, as close to the point of cable entry as practical.

FCC STATEMENTS

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the device and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

FCC CAUTION: Any changes or modifications not expressly approved by ARRIS for compliance could void the user's authority to operate the equipment.

FCC Radiation Exposure Statement

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter except those already approved in this filing. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

Cet emetteur ne doit pas etre Co-place ou ne fonctionnant en meme temps qu'aucune autre antenne ou emetteur. Cet equipement devrait etre installe et actionne avec une distance minimum de 20 centimetres entre le radiateur et votre corps

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destinations. The firmware setting is not accessible by the end user.

INDUSTRY CANADA (IC) STATEMENT

This device complies with Industry Canada's license-exempt RSS's. Operation is subject to the following two conditions:

- This device may not cause interference, and
- This device must accept any interference, including interference that may cause undesired operation of the device.

CAN ICES-3 (B)/NMB-3 (B)

In Canada, RLAN devices are restricted from using the 5600-5650 MHz frequency band.

CAUTION: To reduce the potential for harmful interference to co-channel mobile satellite systems, use of the 5150-5250 MHz frequency band is restricted to indoor use only.

High power radars are allocated as primary users (meaning they have priority) of 5250-5350 MHz and 5650-5850 MHz frequency bands. These radars could cause interference and/or damage to License Exempt–Local Area Network (LE-LAN) devices.

The device meets the exemption from the routine evaluation limits in section 2.5 of RSS 102 and compliance with RSS-102 RF exposure, users can obtain Canadian information on RF exposure and compliance.

AVIS D'INDUSTRIE CANADA (IC)

Le present appareil est conforme aux CNR d’Industrie Canada applicables aux appareils radio exempts de licence. L’exploitation est autorisee aux deux conditions suivantes :

(1) l’appareil ne doit pas produire de brouillage;
(2) l’utilisateur de l’appareil doit accepter tout brouillage radioelectrique subi, meme si le brouillage est susceptible d’en compromettre le fonctionnement.

CAN ICES-3 (B)/NMB-3 (B)

Au Canada, les appareils de réseau local sans fil ne sont pas autorisés à utiliser les bandes de fréquence 5600-5650 MHz.

AVERTISSEMENT: afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux, les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur.

Les radars à haute puissance sont définis en tant qu'utilisateurs principaux (c.-à-d. prioritaires) des bandes de fréquences 5250-5350 MHz et 5650-5850 MHz. Ces radars peuvent causer de l'interférence ou des dommages susceptibles de nuire aux appareils exempts de licence–réseau local (LAN-EL).

Le dispositif rencontre l'exemption des limites courantes d'evaluation dans la section 2.5 de RSS 102 et la conformite a l'exposition de RSS-102 rf, utilisateurs peut obtenir l'information canadienne sur l'exposition et la conformite de rf.

IC RADIATION EXPOSURE STATEMENT

IMPORTANT NOTE: This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

DÉCLARATION DE IC SUR L'EXPOSITION AUX RAYONNEMENTS

NOTE IMPORTANTE: cet équipement est conforme aux limites d'exposition aux rayonnements établies par IC pour un environnement non contrôlé. Cet équipement doit être installé et utilisé de manière à maintenir une distance d'au moins 20 cm entre la source de rayonnement et votre corps.

WIRELESS LAN INFORMATION

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

- The IEEE 802.11 Standard on Wireless LANs (Revision B, Revision G, and Revision N), as defined and approved by the Institute of Electrical Electronics Engineers
- The Wireless Fidelity (Wi-Fi) certification as defined by the Wireless Ethernet Compatibility Alliance (WECA).

Restrictions on the Use of Wireless Devices

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

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

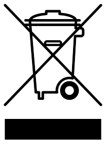
The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of the devices included with this product, or the substitution or attachment of connecting cables and equipment other than specified by the manufacturer. Correction of the interference caused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

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

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

SECURITY WARNING: This device allows you to create a wireless network. Wireless network connections may be accessible by unauthorized users. For more information on how to protect your network, visit the ARRIS Support website at www.arris.com/consumer.

CARING FOR THE ENVIRONMENT BY RECYCLING



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

Recycling your ARRIS Equipment

Please do not dispose of this product with your residential or commercial waste. Some countries or regions, such as the European Union, have set up systems to collect and recycle electrical and electronic waste items. Contact your local authorities for information about practices established for your region.

Getting Started

The ARRIS SURFboard® SBR-AC1750 Wireless Router is a 3x3 dual-band 11ac router, allowing users to connect to the Internet through a separate DOCSIS-compliant cable modem. With Qualcomm solution and StreamBoost application to provide best throughput in different applications.

The SBR-AC1750 Wireless Router has the following features:

- **Remote management capability**: allows you to make changes to your Wireless Router's configuration from anywhere on the Internet.
- **Smart stream management**: Qualcomm StreamBoost™ technology automatically gives applications and devices the bandwidth they need for the best online experience
- **Convenience**: supports Ethernet and 802.11a/b/g/n/ac wireless connections; both can be used simultaneously

This guide provides a product overview and instructions for installing and configuring the SBR-AC1750. It also includes procedures for setting up secure wireless network connections and managing your SBR-AC1750 and network configurations.

What about Security

Having a high-speed, always-on connection to the Internet requires a certain amount of responsibility to other Internet users—including the need to maintain a reasonably secure system. While no system is 100% secure, you can use the following tips to enhance your system's security:

- Keep the operating system of your computer updated with the latest security patches. Run the system update utility at least weekly.
- Keep your email program updated with the latest security patches. In addition, avoid opening email containing attachments, or opening files sent through chat rooms, whenever possible.
- Install a virus checker and keep it updated.
- Avoid providing web or file-sharing services over your Wireless Router. Besides certain vulnerability problems, most cable companies prohibit running servers on consumer-level accounts and may suspend your account for violating your terms of service.
- Use the cable company's mail servers for sending email.
- Avoid using proxy software unless you are certain that it is not open for abuse by other Internet users (some are shipped open by default). Criminals can take advantage of open proxies to hide their identity when breaking into other computers or sending spam. If you have an open proxy, your cable company may suspend your account to protect the rest of the network.
- The SBR-AC1750 ships with wireless LAN security set by default (for the same reasons that you should run only secured proxies). See the security label on your product for the factory security settings. If you need to modify the default wireless security settings, see Configuring Your Wireless Connection.

Ethernet or Wireless?

There are two ways to connect your computer (or other equipment) to the SBR-AC1750. The following will help you decide which is best for you:

Ethernet

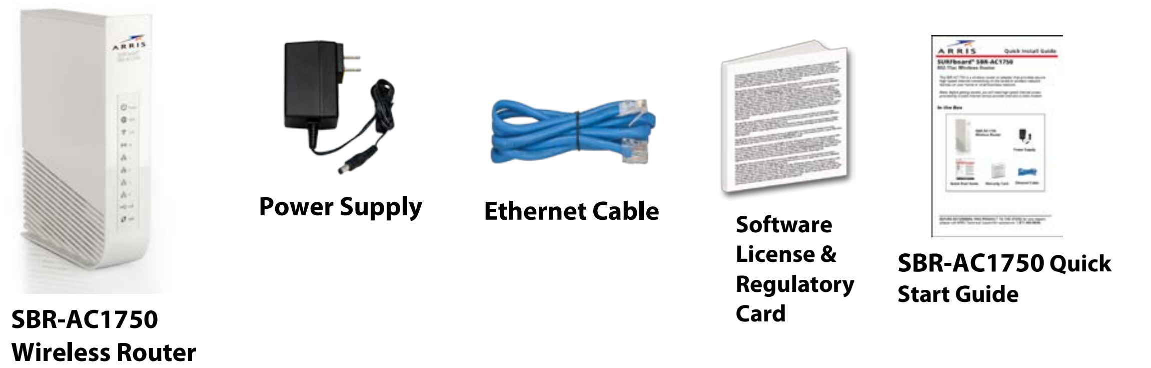
Ethernet is a standard method of connecting two or more computers into a Local Area Network (LAN). You can use the Ethernet connection if your computer has built-in Ethernet hardware.

Note: To connect more than four computers to the SBR-AC1750 through the Ethernet ports, you need an Ethernet hub (available at computer retailers).

The Wireless Router package comes with one 4-foot (1.2m) Ethernet cable (the connectors look like wide telephone connectors); you can purchase more cables if necessary at a computer retailer. If you are connecting the Wireless Router directly to a computer, or to an Ethernet hub with a cross-over switch, ask for Category 5e (CAT5e) straight-through cable. CAT5e cable is required for gigabit Ethernet (Gig-E), not regular CAT5 cable.

In the Box

Before installing the SBR-AC1750, check that the following items are included in the box. If any items are missing, please call ARRIS Technical Support at **1-877-466-8646**.



SBR-AC1750 Wireless Router

Power Supply

Ethernet Cable

Software License & Regulatory Card

SBR-AC1750 Quick Start Guide

Figure 1 – SBR-AC1750 Package Contents

Additional Items You May Need

If you are installing the SBR-AC1750 yourself, make sure you have the following items on hand before continuing:

- **Wireless Router package:** see In the Box for a list of items in the package.
- **Ethernet Cable:** In addition to the Ethernet cable provided, you will need an additional Ethernet cable. This is a standard Ethernet cable with RJ45 type connectors on both ends. Ethernet cables are available for purchase from any electronics retailer or discount store.

- **Information packet:** your cable company should furnish you with a packet containing information about your service and how to set it up. Read this information carefully and contact your cable company if you have any questions.

System Requirements

The SBR-AC1750 Wireless Router operates with most computers. The following describes requirements for each operating system; see the documentation for your system for details on enabling and configuring networking.

To use the Wireless Router, you need DOCSIS high-speed Internet service from your cable company. Telephone service requires that the cable company has PacketCable support.

Recommended Hardware

The following hardware configuration is recommended. Computers not meeting this configuration can still work with the SBR-AC1750, but may not be able to make maximum use of SBR-AC1750 throughput.

- CPU: P4, 3GHz or faster
- RAM: 1GB or greater
- Hard drive: 7200 RPM or faster
- Ethernet: Gig-E (1000BaseT)

Windows

Windows XP , Windows Vista, Windows 7, or Windows 8. A supported Ethernet or wireless LAN connection must be available.

MacOS

System 7.5 to MacOS 9.2 (Open Transport recommended) or MacOS X. A supported Ethernet or wireless LAN connection must be available.

Linux/other Unix

Hardware drivers, TCP/IP, and DHCP must be enabled in the kernel. A supported Ethernet or wireless LAN connection must be available.

Contact Information

For technical support or additional ARRIS product information:

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

Chapter 3

Product Overview

Front Panel

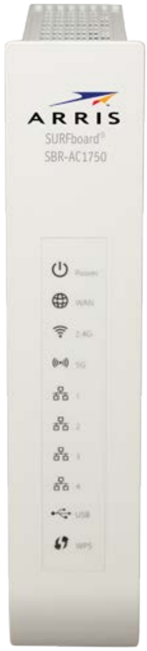


Figure 2 – SBR-AC1750 Front View

The SBR-AC1750 front panel has the following LEDs:

- **Power:** indicates whether AC power is available to the unit.
- **WAN:** indicates the status of WAN connectivity.
- **2.4G:** indicates the status of the 2.4 GHz wireless LAN.
- **5G:** indicates the status of the 5 GHz wireless LAN.
- **LAN (1 - 4):** indicates the status of LAN connectivity.
- **USB:** indicates whether a USB device is attached.
- **WPS:** indicates Wireless Protected Setup (WPS) is active.

SBR-AC1750 Indicator Lights

The Wireless Router has several LED indicator lights to assist in troubleshooting:

LED	Color/Behavior	Description
Power	Solid green	System power is on.
WAN	Solid green	An IP address has been received and is ready to transmit data, or bridge mode is active.
	Flashing green	The Ethernet cable connection has been detected.
	Off	No Ethernet cable is connected to the Wireless Router.
2.4G Wi-Fi	Solid green	The wireless port has linked with a wireless client.
		Wireless is disabled.
5G Wi-Fi	Solid green	The wireless port has linked with a wireless client.
		Wireless is disabled.
WPS	Solid green	WPS has been started.
	Flashing green (slow flash)	WPS has been started, and Wireless Router is ready to accept a client connection.
	Flashing green (quick flash)	WPS error. **NOTE TO REVIEWERS: What kind of error? What should the user do to correct it?**
LAN 1 – 4	Solid green	10/100/1000Mbps link detected.
	Flashing green	Receiving/transmitting data at 10/100/1000Mbps.
	Off	No Ethernet connection.
USB	Solid green	USB device successfully connected and active.
	Flashing green	USB device read/write activity.
	Off	No USB device connected, or the attached USB device can now be safely removed.

Using the Reset Button

Use the **Reset** button, on the back of the Wireless Router, to reset the Wireless Router and perform initialization as if you power cycled the unit. You may need to reset the Wireless Router if you are having problems connecting to the Internet. You will not use this button often.

Use a pointed **non-metallic** object to press this button. The **Reset** button is recessed to prevent accidental resets.

Resetting the Router to Factory Defaults

To reset the router to factory defaults, press and hold the **Reset** button (**1**) on the back of the Wireless Router for more than fifteen seconds. This restores the wireless setup configuration and router configuration parameters to the factory defaults. You may need to do this if a configuration error has locked out all access.

Rear Panel

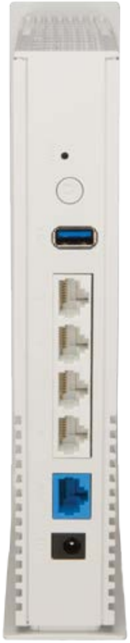
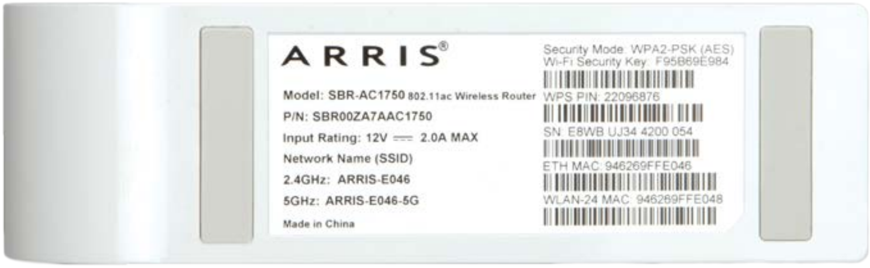


Figure 3 – SBR-AC1750 Rear View

The SBR-AC1750 rear panel has the following connectors and controls:

- **Reset button:** resets the Wireless Router as if you power cycled the unit. Use a pointed non-metallic object to press this button.
- **USB:** USB host connector - future support for external USB devices
- **Ethernet (1 - 4):** connectors for use with a computer LAN port.
- **WAN:** connector for the cable modem.
- **Power:** connector for the power cord.

Gateway Label



ARRIS®

Model: SBR-AC1750 802.11ac Wireless Router

P/N: SBR00ZA7AAC1750

Input Rating: 12V ⎓ 2.0A MAX

Network Name (SSID)

2.4GHz: ARRIS-E046

5GHz: ARRIS-E046-5G

Made in China

Security Mode: WPA2-PSK (AES)

Wi-Fi Security Key: F95B69E984

WPS PIN: 22096876

SN: E8WB UJ34 4200 054

ETH MAC: 946269FFE046

WLAN-24 MAC: 946269FFE048

Figure 4 – SBR-AC1750 Label

The gateway label is located on the bottom of the SBR-AC1750. It contains specific router ID information that you may need when contacting your service provider or ARRIS Technical Support.

When contacting your service provider for assistance, you may need to provide the following information listed on the gateway label :

- Router model name (**SBG6900-AC**)
- Router serial number (**SN**)

Chapter 4

Installing the Router

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

There are a number of factors to consider when choosing a location to install your Wireless Router:

- Is an AC outlet available nearby? For best results, the outlet should not be switched and should be close enough to the Wireless Router that extension cords are not required.
- Is the cable modem nearby? Can you easily run cables between the wireless router's location and the cable modem?
- If you are connecting devices to the Ethernet ports, can you easily run cables between the Wireless Router's location and those devices?
- If you want to mount the Wireless Router on a wall, does the location provide a solid surface for secure attachment? For best results when mounting the Wireless Router on drywall, position the Wireless Router so at least one of the screws are fastened to a stud. This may prevent the Wireless Router from pulling out of the wall in the future.
- If you want to install the Wireless Router on a desktop, is there enough space on either side to keep the vents clear? Blocking the vents may cause overheating.
- How close are your wireless devices? The Wireless Router wireless connection range is typically 100–200 feet (30m–65m). A number of factors can affect connection range, as described below.

Desktop Mounting Instructions

Position the Wireless Router so that:

- Air flows freely around it.
- The rear faces the nearest wall.
- It will not fall to the floor if bumped or moved.
- The sides of the unit are not blocked.

Cleaning Instructions

Clean the Wireless Router using only a clean, slightly moistened, cloth. Do not use aerosols in the vicinity of the Wireless Router.

Factors Affecting Wireless Range

A number of factors can affect the usable range for wireless connections.

Increases range	■ Raising the unit above the devices (for example, installing the Wireless Router in the upper floor of a multi-story dwelling)
Decreases range	■ Lowering the unit below the devices (for example, installing the Wireless Router in a basement) ■ Metal or concrete walls between the Wireless Router and other devices ■ Large metal appliances, aquariums, or metal cabinets between the Wireless Router and other devices ■ Interference and RF noise (2.4 GHz wireless phones, microwave ovens, or other wireless networks)

Note: Note that decreasing the range of your wireless network may be beneficial, as long as the decreased range is sufficient for your needs. By limiting your network's range, you reduce interference with other networks and make it harder for unwanted users to find and connect to your network.

Note: Setting the transmit power level to High increases the range. Setting it to Medium or Low decreases the range proportionately.

Connect the SBR-AC1750

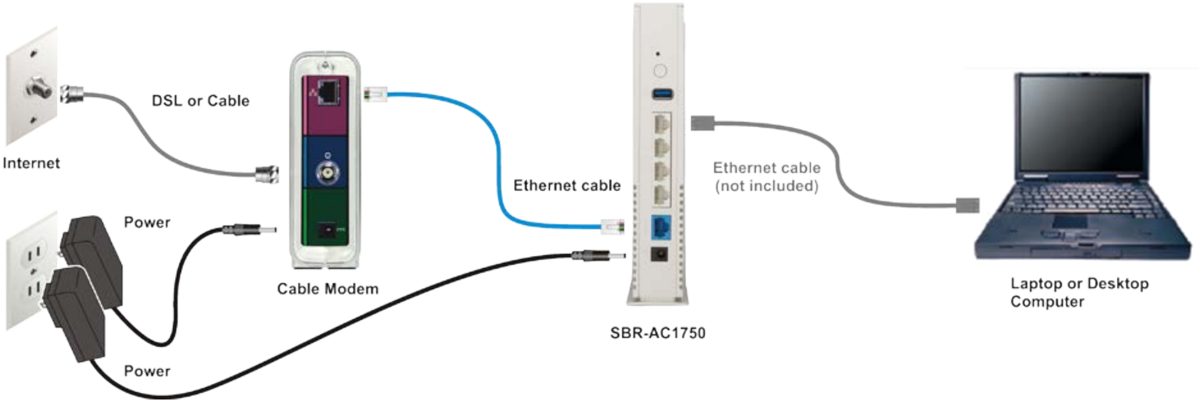


Figure 5 – SBR-AC1750 Connection Diagram

1. Unplug the power to turn off your cable modem.

   If your cable modem has a battery backup, remove the battery to be sure the cable modem is powered off.

2. Connect one end of the blue Ethernet cable (included) to your cable modem, and the other end to the WAN port on your Wireless Router.

3. Reconnect the power cable on your cable modem to turn it back on.

   Wait approximately two minutes to allow your cable modem to fully power up. Replace the battery , if applicable.

4. Connect the power adapter (included) to the power connector on the back of the Wireless Router, and then connect the power adapter to an available AC outlet. Wait until the 2.4G and 5G LEDs on the front panel of the Wireless Router turn solid green.

5. To manage the setup of your Wireless Router, you can connect a computer using a second Ethernet cable (not provided). Or, you can connect wirelessly by using the preset wireless security settings printed on the security label located on the bottom of your Wireless Router.

6. Open a browser on your computer to access the management interface of the Wireless Router. If the webpage does not display correctly, try another browser. See Accessing the Configuration Interface (page 25) for more information.

Chapter 5

Configuring Your Ethernet Connection

If your computer is equipped with a LAN card providing an Ethernet connection, you may have to configure your computer's TCP/IP settings. The steps that follow will guide you through setting your computer's TCP/IP settings to work with the Wireless Router.

Requirements

Make sure you have the following before attempting to configure your Ethernet connection:

- Computer with Ethernet interface
- Ethernet cable (supplied)
- IP address, subnet, gateway, and DNS information for installations not using DHCP

How to use this Chapter

The following list shows the procedures for modifying the TCP/IP settings on the computer. The procedure is slightly different depending on the operating system that you are using. Please ensure you are using the correct steps for the operating system on your computer. Follow the links below for instructions to configure your Ethernet connection on your operating system.

- TCP/IP Configuration for Windows XP (page 20)
- TCP/IP Configuration for Windows Vista (page 21)
- TCP/IP Configuration for Windows 7 or Windows 8 (page 21)
- TCP/IP Configuration for MacOS X (page 22)

TCP/IP Configuration for Windows XP

Follow these steps to configure the Ethernet interface on a Windows XP operating system.

TCP/IPv6 Note: This procedure shows the configuration of TCP/IPv4. TCP/IPv6 is not installed or enabled by default in Windows XP. If your cable provider requires TCP/IPv6 you must first install and enable it on your Windows XP system. Refer to Microsoft support materials on Windows XP for installation instructions. Once installed and enabled, follow this same configuration example, but select TCP/IPv6 at the appropriate step.

1. From the computer, select Start > Settings > Control Panel and double-click Network Connections in the Control Panel.

   The Network Connection window displays a list of LAN connections and associated network adapters.

2. Double-click the local area connection to be used for your device's network connection.

   The Local Area Connection Status widow displays.

3. Click Properties.
4. Select TCP/IP by clicking it one time. Then click Properties.
5. Click the General tab. Then click Obtain an IP address automatically and click OK.
6. Click OK to accept the new settings, and OK again to close the Properties window.
7. You may have to restart your computer in order for your computer to obtain a new IP address from the network.

TCP/IP Configuration for Windows Vista

Follow these steps to configure the Ethernet interface on a Windows Vista operating system.

1. Open the Vista Control Panel.
2. Double-click Network and Sharing Center to display the Network and Sharing Center Window.
3. Click Manage network connections. If prompted for a connection, choose Local Area Connection.

   The Network Connections window displays.
4. Double-click the Local Area Connection to open the Properties window:

   Note: If Windows requests permission to continue, click Continue.
5. Double-click Internet Protocol Version 4 (TCP/IPv4) to configure TCP/IPv4.

   Note: If your cable provider requires TCP/IP version 6, double-click Internet Protocol Version 6 (TCP/IPv6) to configure TCP/IPv6.

   The TCP/IP properties window for the version you selected displays.
6. For either TCP/IPv4 or TCP/IPv6, select Obtain an IP address automatically and Obtain DNS server address automatically, unless instructed otherwise by your cable provider.
7. Click OK to accept the new settings and close the Properties window.

TCP/IP Configuration for Windows 7 or Windows 8

Follow these steps to configure the Ethernet interface on a Windows 7 or Windows 8 operating system.

1. Open the Windows Control Panel.
2. Click Network and Internet.
3. Click Network and Sharing Center.
4. Click Local Area Connection to open the Status window.
5. Click Properties to open the Properties window.

6. Select Internet Protocol Version 4 (TCP/IPv4) and click Properties to configure TCP/IPv4.

   Note: If your cable provider requires TCP/IP version 6, select Internet Protocol Version 6 (TCP/IPv6) and click Properties to configure TCP/IPv6.

   The TCP/IP properties window for the version you selected displays.

7. For either TCP/IPv4 or TCP/IPv6, select Obtain an IP address automatically and Obtain DNS server address automatically, unless instructed otherwise by your cable provider.
8. Click OK to accept the new settings and close the Properties window. Then click Close to back out of the remaining setup screens.

TCP/IP Configuration for MacOS X

Follow these steps to configure the Ethernet interface on a MacOS X operating system.

1. Open System Preferences, either by choosing System Preferences from the Apple menu or by clicking the System Preferences icon in the dock.
2. Click the Network icon.
3. Choose Automatic from the Location drop-down menu, and Built-in Ethernet from the Show menu.
4. Choose the TCP/IP tab, if necessary.

   If you are using TCP/IPv4, go to **step 5**.
   If your cable provider requires TCP/IPv6, go to **step 8**.

5. Choose Using DHCP from the Configure IPv4 menu.
6. If necessary, click the Renew DHCP Lease button.
7. Close the System Properties application.

   TCP/IPv4 configuration is completed.

8. If you are using TCP/IPv6, click Configure IPv6 near the bottom of the previous window.
9. Choose Automatically from the Configure IPv6 drop-down menu and click OK.
10. Close the System Properties application.

Troubleshooting Tips

Solutions

The Wireless Router is plugged in, but the Power light is Off

Check all power connections. Is the power cord plugged in firmly at both ends?

If you plugged the power cord into a power strip, make sure the strip is switched on.

Avoid using an outlet controlled by a wall switch, if possible.

Finally, check the fuse or circuit breaker panel.

I'm not getting on the Internet (all connections)

It may take over 30 minutes to establish a connection the first time you power up your Wireless Router, especially when many people are online. Always leave your Wireless Router plugged into AC power and connected to the cable system.

Check the front panel lights:

- The **Power** and **Online** lights should be on.
- If the **Power** light blinks for more than 30 minutes, call your cable company for assistance.

Check your cable connections. Connectors should be tight. The coax cable should not be pinched, kinked, or bent sharply—any of these can cause a break or short in the cable (you may have to replace the cable). If you have one or more splitters between the Wireless Router and CATV outlet, remove the splitters and connect the Wireless Router directly to the outlet.

Proceed to the Ethernet or wireless solutions if necessary.

I'm not getting on the Internet (Ethernet)

If you are using a hub, is the hub turned on?

Are you using the right type of Ethernet cable? Use the supplied cable for direct connection to a computer; use a cross-over cable for connection to a hub.

Press the **Reset** button on the back of the Wireless Router.

A misconfiguration could lock out all access to the Wireless Router router. If you think this has happened, see Resetting the Router to Factory Defaults (page **Error! Bookmark not defined.**).

I'm not getting on the Internet (Wireless)

Check the indicator lights, see Using the Wireless Router — the Wi-Fi light should be on.

Does your connection utility discover your wireless LAN? If you turned off "Broadcast SSID" you need to manually enter the name of your wireless LAN in the connection utility.

Change your security mode to “disabled”. Enable one of the other security modes as soon as you find the problem.

A misconfiguration could lock out all access to the SBR-AC1750. If you think this has happened, see Resetting the Router to Factory Defaults (page **Error! Bookmark not defined.**).

My wireless Internet connection stops working sometimes

This is usually caused by interference. Two common sources are 2.4GHz “remote” telephones and microwave ovens. If you cannot remove the interfering product, try using a different channel or setting Protected Mode.

I can get on the Internet, but everything is slow

If the Web site you are visiting is very popular, that site may be having trouble servicing all the requests. If other sites download quickly, wait for a few minutes and try again. Usage during peak hours may also affect the connection speed.

Other communications on the LAN, or interference with wireless connections, may slow down your connection.

Chapter 7

Basic Configuration

The router ships with a basic factory default configuration that should allow you to immediately access the Internet after installing the hardware according to your User's Guide.

If you need to modify the routers default basic settings, or if you want to configure advanced settings, refer to the appropriate instructions in this document.

As a minimum, it is recommended that you:

- Change the default login password
- Change the default wireless network name, also called the Service Set Identifier (SSID)

Wireless LAN Default Security Setting: The router ships with wireless LAN security set by default. See the security label on your product for the factory security settings: network name (SSID), encryption method, network key, and WPS PIN.

If you need to modify the router's default wireless security settings, or if you want to configure any other settings, refer to the appropriate instructions in this document.

Note: You must set up your computer and other client devices to work with the security settings on the router. Refer to the documentation for your client device for instructions on setting security. If your computer or client device supports Wi-Fi Alliance WPS (Wireless Protected Setup), activate WPS on your computer or client device and the router simultaneously to easily set up your system security.

Accessing the Configuration Interface

Perform the following steps to access the configuration interface.

1. If security has been properly set up on your computer to access the wireless LAN on the router, use the connection utility for your operating system to connect to the wireless LAN using its network name (SSID), as shown on the security label.

Note: If you cannot access the wireless LAN, you must first establish a wired Ethernet connection between your computer and the router.

2. In your web browser, type **http://192.168.0.1/** to access the wireless router setup.

   The Login screen displays.

3. 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.

   The System Basic Setup screen displays.

4. Set basic setup configuration parameters as required for your system.

Note: Most configuration parameters that you may want to set can be accessed on the System Basic Setup screen or under the More LAN Settings or More Wireless Settings links.

Configuring Your Wireless Network

Perform the following procedures to make the basic configuration settings for your wireless network.

Enabling or Disabling the Wireless Network.

Perform the following steps to enable the wireless network.

1. Access and log into the configuration interface.
2. Click the **Basic Setup** tab.
3. Click the **Enable Wireless** checkbox in either the Wireless 2.4 Ghz section or the Wireless 5 GHz section to enable wireless networking for that frequency.
4. Click the **Apply** button.

Changing Your Login Password

You should change your login password to something other than the default password.

Note: The default user name is "admin," the default password is "password" (both lower case).

Perform the following steps to change your password.

1. Access and log into the configuration interface via a direct wired Ethernet or wireless connection.
2. Click the **Utilities** tab.
3. Click System Settings in the side menu.
4. Enter your old password in the **Current Password** field.
5. Enter your new password in both the **New Password** and **Confirm New Password** fields.

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.)

6. Click the **Apply** button.

Changing the Default Wireless Network Name (SSID)

While still on the Basic Setup screen, perform the following steps to change your wireless 2.4 GHz and/or wireless 5 GHz network name.

1. Enter a unique user friendly name to identify your wireless network in the Wireless Network Name (SSID) field under either Wireless 2.4 GHz or Wireless 5 GHz.

Note: This name is also referred to as the Service Set Identifier (SSID). The name can be up to 32 characters long.

2. Click the **Apply** button at the bottom of the screen.

Configuring Wi-Fi Protected Setup (WPS)

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.

Perform the following steps to enable the wireless network.

1. Access and log into the configuration interface.
2. Click the **Basic Setup** tab.
3. Click **WPS Settings** in the side menu.
4. Click the Wi-Fi Protected Setup (WPS) Enable checkbox and click the **Apply** button to enable WPS on your system.
5. Select the mode from the WPS Mode drop-down menu. It can be set to PBC (Push Button Control) or PIN Code.
    - If your client device has a WPS button, select PBC and go to step 6a.
    - If your client device has a PIN number select PIN Code and go to step 6b.
6. a) If using PBC, press the WPS buttons on the client device and on your router simultaneously to start the WPS association.

    b) If using PIN codes, enter the enrollee's PIN in the Enrollee PIN Code field, and then click the Start WPS Association icon. Enter the router's PIN code in the Device PIN Code field if requested during connection.
7. 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's ready to accept a client connection) and then turns off. If the WPS light turns off, start the association process over.

Troubleshooting Your Wireless Connection

The three main factors that affect wireless network performance are:

- Range from the client devices
- Interference from other wireless devices
- Client device hardware/software configuration

Factors Affecting Wireless Range

How close are your wireless devices to your Wireless Router? The Wireless Router's wireless connection range is typically 100 to 200 feet (30m to 65m).

Note: You should try to centralize the Wireless Router in relation to where the wireless client devices will usually be located.

A number of factors can affect the usable range for wireless connections, as described in this table.

Effect on Range	Factor
Increases range	▪ Raising the unit above the devices (for example, installing the Wireless Router in the upper floor of a multi-story dwelling) ▪ Setting the transmit power level to High
Decreases range	▪ Lowering the unit below the devices (for example, installing the Wireless Router in a basement) ▪ Metal or concrete walls between the Wireless Router and client devices ▪ Large metal appliances, aquariums, or metal cabinets between the Wireless Router and client devices ▪ Interference and RF noise (2.4 GHz wireless phones, microwave ovens, or other wireless networks) ▪ Setting the transmit power level to Medium or Low ▪ Setting the wireless mode to 5 GHz reduces interference but also decreases range.

Note: Decreasing the range of your wireless network may be beneficial, as long as the decreased range is sufficient for your needs. By limiting your network's range, you reduce interference with other networks and make it harder for unwanted users to find and connect to your network.

Interference from Other Wireless Devices

Interference from other equipment operating at 2.4 GHz or 5 GHz in the area of your wireless network can significantly affect the range and performance of your network, such as:

- Cordless phones
- Wireless speakers
- Microwave ovens
- Baby monitors
- Gaming consoles, such as Wii™, Xbox, and PlayStation®
- Any other devices operating at 2.4 GHz or 5 GHz

Note: If your cordless phones or other wireless devices are interfering with your wireless network's performance, replace them with a similar device that operates on a different frequency if possible. For example, change to 5.8 GHz cordless phones.

Client Device Hardware/Software Configuration

Client device hardware/software configuration can also affect your wireless network performance.

For example, your computer's operating system, network adapter, processor, and hard drive access speed can all affect the transfer speeds that you experience across the network.

If wireless performance is slow, check the following items.

Verify which 802.11 Standard the Wireless Clients Can Use

If your client device network adapters use the older 802.11b or 802.11g standards, you should upgrade them to the 802.11n standard. Network adapters using the older standards can reduce the performance of your entire network.

802.11b (becoming more rare but not extinct yet) is much slower than 802.11g, which is slower than 802.11n. The MAXIMUM theoretical limit for each standard is as follows.

- 802.11b: 11 Mbps
- 802.11g: 54 Mbps
- 802.11n: 130 Mbps to 450 Mbps (depending on the wireless router AND wireless client hardware)

Note: Actual maximum throughput performance typically does not exceed 50% of the above values.

Perform a Site Survey to Determine the Best Channel

Use wireless network scanning software such as MetaGeek's free inSSIDer tool to see how many other wireless routers and access points are broadcasting.

For wireless 2.4 GHz, try to find the cleanest channel among channels 1, 6, and 11. These are the only three channels that do not overlap. If there are no good options among channels 1, 6 and 11, you can try channel 4 or 8. However, selecting these channels can cause degraded throughput speeds if there is a lot of traffic on channel 1, 6, or 11. For wireless 5 GHz, choose a channel that is farthest away from the channel used by any other unit operating in the area.

It is a trial and error process to find the best channel. The best setting may change at any time depending on all of the other wireless routers in the environment.

Note: When Touchstone 16xx Gateways are set to Auto channel, they will automatically select the cleanest of the available channels upon boot up.

Adjust the Gateway's Wireless Configuration Settings

- Security Mode/Encryption Algorithm
  - The recommended security mode/encryption algorithm is WPA2-PSK (AES) for best performance. All other options will result in degraded throughput speeds. For example, using WEP and WPA reduces throughput by approximately 80% comparatively.
  - Note that Security Mode WEP and WPA are not compatible with the 802.11n standard. Performance would be limited to 802.11g speeds of 54mbps. Also, 802.11n requires WPA2 and AES.

- Wireless Mode
  - Set your wireless mode to optimize performance based on the type of network adapters being used by your network devices, e.g., 802.11b, 820.11g, and 802.11n. Select the proper mode to support all of the wireless devices that will connect to your router. It's best to have an environment with only one standard and set the Gateway to that standard. Since this is not always feasible, ONLY include the standards that are used in your environment.
  - The presence of 802.11b devices in an active network will cause the greatest performance degradation.
- BG Protection
  - This option allows you to properly operate 802.11b client devices in 802.11g networks. These older 802.11b devices required the unit to add overhead to most transmissions.
- Operation Mode
  - The options are Mixed mode or Greenfield. Select Mixed mode if you network consists of a mix of 802.11 b, g, and n clients. Select Greenfield if your network consists of ONLY 802.11n clients. The Greenfield mode improves efficiency of networks using only 802.11n devices by eliminating support for the 802.11a/b/g client devices.
- Channel Bandwidth (802.11n only)
  - Options are 20 MHz or 20/40 MHz . The default setting is 20 MHz. If your wireless network is in a very clean RF environment setting the Channel Bandwidth to 20/40 will increase your throughput by "bonding" two channels. However, if there are any other wireless routers or access points within range of the device it will stay in 20 MHz bandwidth regardless of this setting. This is a WiFi Alliance requirement. (You can verify the channel bandwidth by using the previously mentioned wireless network scanning software, MetaGeek's inSSIDer.)
- Guard Interval (802.11n only)
  - This is the time in nanoseconds between symbols for 802.11n frames. 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).

Setting Up Your WAN Connection

A Dynamic or DHCP (Dynamic Host Configuration Protocol) connection is the most commonly used WAN connection type.

Note: Do not change this setting unless your Internet Service Provider tells you to use another connection type.

Perform the following steps to change your connection type.

1. Access and log into the configuration interface.
2. Click the **WAN Setup** tab.
3. Click Dynamic, Dynamic (IPV6), Static, or Static (IPV6) in the side menu to display the appropriate screen for configuring that type of WAN connection.

4. Set the required configuration parameters for the connection type you selected as provided by your Internet Service Provider.

Note: Refer to WAN Setup in Web GUI Screens Overview (page 42) for specific instructions on setting the various connection type configuration parameters.

5. Click the **Apply** button at the bottom of the screen.

Chapter 8

Advanced Configuration

The following are the most common advanced configuration options for your router:

- WAN Setup
- LAN Setup
- Wireless Setup
- Firewall
- Utilities

Note: Refer to Web GUI Screens Overview (page 42) for additional advanced configuration options.

LAN Setup – Configuring DHCP

DHCP (Dynamic Host Protocol Configuration) is enabled by default on your router which allows your router to act as a DHCP server and automatically assign an IP address to each device 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 or device and a new IP address must be entered each time it moves to a new location on the network.

Perform the following steps to configure DHCP.

1. Access and log into the configuration interface.
2. Click the **LAN Setup** tab.
3. Click **LAN Settings** or **LAN Settings (IPV6)** in the side menu to display the LAN Settings screen.
4. Click the **Enable DHCP Server** checkbox under DHCP Server Settings.
5. Enter the Start IP Address and End IP Address for the range of IP addresses that the DHCP Server will be allowed to assign to a network device.
6. Enter the Lease Time in seconds before the assigned IP address will expire. (After the lease time is up, the user is automatically assigned a new dynamic IP address.)

Note: Refer to LAN Setup (page 48) for specific instructions on setting the various DHCP configuration parameters.

7. Click the **Apply** button at the bottom of the screen.

LAN Setup – Adding and Deleting DHCP Clients

The DHCP Client screen 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.

Perform the following steps to configure the DHCP Clients.

1. Access and log into the configuration interface.
2. Click the **LAN Setup** tab.
3. Click **Client List** in the side menu to display the Client List screen.
4. Click the **Add** button to add a reserved IP client. Select an existing DHCP client and then click the **Delete** button to delete the client. Click the **Refresh** button to update the Clients List.

LAN Setup – Selecting the NAT Mode

NAT (Network Address Translation) allows your router to manipulate IP addresses so that just one single IP address can represent an entire group of computers on your network and let them all communicate with the Internet. This conserves IP addresses and is necessary since there are a finite number of available IP addresses for use.

Perform the following steps to select the NAT Mode.

1. Access and log into the configuration interface.
2. Click the **LAN Setup** tab.
3. Click **LAN Settings** in the side menu to display the LAN Settings screen.
4. Select the **NAT Mode** from the NAT Mode field drop-down list. The optional modes are:

   Bridged - Data will pass through the device directly without any routing.

   Routed with NAT - Data will be routed by the device and all the outgoing packets will be NATed.

   Routed without NAT - Data will be routed by the device but all the outgoing packets will not be NATed.
5. Click the **Apply** button at the bottom of the screen.

Note: A dialog box displays “Restarting your router is recommended when NAT settings change.” Click **OK** to restart.

Wireless Setup – Setting the Wireless Mode

You can set your wireless mode to optimize performance based on the type of network adapters being used by your network devices, e.g., 802.11b, 820.11g, and 802.11n. Select the proper mode to support all of the wireless devices that will connect to your router.

Perform the following steps to set your wireless mode.

1. Access and log into the configuration interface.
2. Click the Wireless 2.4 GHz and/or Wireless 5 GHz tab.
3. Click Advanced in the side menu to display the Advanced Settings screen.
4. Under Wireless Network Settings select the proper mode from the Wireless Mode drop-down list.

   2.4 GHz Options: B/G mixed, B only, G only, N only, G/N mixed, and B/G/N mixed.

   5 GHz Options: A/N mixed, A only, and N only.
5. Click the Apply button at the bottom of the screen.

Note: Refer to Advanced (page 56) for instructions on setting additional advanced wireless configuration parameters.

Wireless Setup – Setting the 802.11n Operation Mode

The 802.11 operation mode must be set to work properly with the selected wireless mode setting. The default setting, **Mixed Mode**, is for networks with a mix of 802.11b/g/n client devices. Mixed Mode can be used with any Wireless Mode setting. If all of your network devices are 802.11n devices, you can improve the efficiency of your network by setting the Wireless Mode to “N only” and setting the 802.11n operation mode to Greenfield.

Perform the following steps to set your 802.11n operation mode.

1. Access and log into the configuration interface.
2. Click the **Wireless 2.4 GHz** tab.
3. Click **Advanced** in the side menu to display the Advanced Settings screen.
4. Under 802.11n Specific Settings select the proper mode from the Operation Mode drop-down list.

   Options are: Greenfield and Mixed Mode.
5. Click the **Apply** button at the bottom of the screen.

Note: Refer to Advanced (page 56) for instructions on setting additional advanced wireless configuration parameters.

Wireless Setup – Using MAC Address Filtering

MAC address filtering allows you to restrict access to your wireless network to those computers you specifically authorize to connect. This filter type is called an Allowed List. Optionally, you can block specific computers from accessing your network. This filter type is called a Blocked List. You have to choose one type or the other.

Perform the following steps to set up MAC address filtering.

1. Access and log into the configuration interface.
2. Click the **Wireless 2.4 GHz** and/or **Wireless 5 GHz** tab.
3. Click **MAC Address Control** in the side menu to display the MAC Address Control screen.
4. Under **MAC Address Filtering** select the proper filter type from the **MAC Address Filter Type** drop-down list.

   Options are: None, Allowed List, and Blocked List.
5. Under **MAC Address Filter List** click the **Add** button to display the Add MAC Address dialog box.
6. Enter the MAC address of a computer that you want to add to the filter list, and then click the **Add MAC Address** button.

Note: If you don't know how to find your computer's MAC address, see Finding the MAC Address of a Computer (page 35).

7. Repeat Step 6 for each MAC address you want to add.

Note: To delete a MAC address, first select a MAC address in the list and then click the **Delete** button.

8. Click the **Apply** button.

Finding the MAC Address of a Computer

Use the specific operating system of your computer to find its MAC address, as follows.

Windows:

From the Start menu, find and select the **Control Panel**. Double-click **Network Connections** (Windows XP), or **Network & Sharing Center** (Windows Vista or Windows 7). Then double-click either "Wireless Network Connection" for a wireless connection, or "Local Area Connection" for an Ethernet connection. Next click the **Details** button (Windows Vista or Windows 7), or click the Support tab and then the **Details** button (Windows XP). The "Physical Address" line shows the MAC address.

MacOS X:

Open System Preferences and click the Network icon. To find the Ethernet MAC address, select **Built-in Ethernet** from the Show drop-down, then click the Ethernet tab. The "Ethernet ID" field shows the MAC address. To find the wireless MAC address, select **Airport** from the Show drop-down, then click the Airport tab. The "Airport ID" field shows the MAC address.

Linux:

Open a shell window and type **/sbin/ifconfig** (and press Enter). The wireless interface is eth1 (unless there is no Ethernet adapter, in which case the interface is eth0).

Firewall – General Firewall Configuration 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 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 will not leave your network completely vulnerable to hacker attacks, but it is recommended that you enable the firewall whenever possible.

Perform the following steps to enable the firewall and make general firewall settings.

1. Access and log into the configuration interface.
2. Click the **Firewall** tab.
3. Click **Firewall Settings** in the side menu to display the Firewall Settings screen.
4. Check the **Enable Firewall** checkbox to enable the firewall on your network.
5. Check the **Enable DoS Attack Protection Firewall** checkbox to protect against DoS attacks.
6. Check the **Enable Ping Blocking** checkbox to protect against PoD attacks.
7. Check the **Enable IPSec Pass Through** checkbox to allow IPSec tunnels to pass through the router.
8. Check the **Enable PPTP Pass Through** checkbox to allow PPTP tunnels to pass through the router.
9. Check the **Enable L2TP Pass Through** checkbox to allow L2TP tunnels to pass through the router.
10. Check the **Enable Block Fragmented IP Packets** checkbox to block fragmented IP packets.
11. Click the **Apply** button at the bottom of the screen.

Firewall – Configuring a Virtual Server (Port Forwarding)

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, applications that allow remote access to your computer, some gaming and videoconferencing applications, and others.

If you have a server in your network that you want to make available to the general Internet, you can configure a virtual server. The firewall passes requests from the Internet to the designated computer on your network. This function works by allowing 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.

Perform the following steps to configure a virtual server.

1. Access and log into the configuration interface.
2. Click the **Firewall** tab.
3. Click **Virtual Servers** in the side menu to display the Virtual Server Configuration screen.
4. Check the **Add** button to display the **Add Virtual Server** dialog box.
5. Enter the following parameters in the dialog box.

   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.

6. Click the **Add Virtual Server** button to add the virtual server.

Note: To delete a virtual server, first select a virtual server in the list and then click the **Delete** button.

Firewall – Configuring Port Triggers

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.

Perform the following steps to add a port trigger.

1. Access and log into the configuration interface.
2. Click the **Firewall** tab.
3. Click **Port Triggers** in the side menu to display the Port Triggers screen.
4. Check the **Add** button to display the Add Port Trigger dialog box.
5. Enter the following parameters in the dialog box.

   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.

6. Click the **Add Port Trigger** button to add the port trigger.

Note: To delete a port trigger, first select a port trigger in the list and then click the **Delete** button.

Firewall – Configuring Client IP Filters

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

Perform the following steps to add a client IP filter.

1. Access and log into the configuration interface.
2. Click the **Firewall** tab.
3. Click **Client IP Filters** in the side menu to display the Client IP Filter Configuration screen.
4. Check the **Add** button to display the Add Client IP Filter dialog box.
5. Enter the following parameters in the dialog box.

   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.

6. Click the **Add Client IP Filter** button to add the filter.

Note: To delete a client IP filter, first select a client IP filter in the list and then click the **Delete** button.

Firewall – Configuring Client IPV6 Filters

The router can be configured to restrict access to the Internet, email, or other network services.

Perform the following steps to add a client IPV6 filter.

1. Access and log into the configuration interface.
2. Click the **Firewall** tab.

3. Click **Client IPV6 Filters** in the side menu to display the Client IPV6 Filter Configuration screen.

4. Check the **Add** button to display the Add Client IP Filter dialog box.

5. Enter the following parameters in the dialog box.

   Action/Direction - Select either Allow+Incoming or Deny+Outgoing to allow data watching this filter and watch incoming data or deny data watching and watch outgoing data.

   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.

6. Click the **Add Client IP** Filter button to add the filter.

Note: To delete a client IP filter, first select a client IP filter in the list and then click the **Delete** button.

Firewall – Configuring DMZ for Gaming or Conferencing Applications

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.

Perform the following steps to put a computer in the DMZ.

1. Access and log into the configuration interface.

2. Click the **Firewall** tab.

3. Click **DMZ** in the side menu to display the DMZ Settings screen.

4. Enter the following parameters.

   Enable DMZ – Click this checkbox 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.

5. Click the **Apply** button at the bottom of the screen.

Note: To remove the computer from the DMZ, delete the entries and uncheck the Enable DMZ checkbox.

Utilities – Viewing Network System Information

You can view status and system information for your network on the Utilities – System Information screen.

Perform the following steps to view system status information.

1. Access and log into the configuration interface.
2. Click the **Utilities** tab.
3. Click **System Information** in the side menu to display the System Information screen.

Note: Refer to System Information (page 64) for an explanation of the various status information parameters.

Utilities – Restarting the Router

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

Perform the following steps to restart the router.

1. Access and log into the configuration interface.
2. Click the **Utilities** tab.
3. Click **Restart Router** in the side menu to display the Restart Router screen.
4. Click the **Restart** button to restart the router.

Utilities – Reverting to Factory Default Settings

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 function.

Perform the following steps to revert to factory default settings.

1. Access and log into the configuration interface.
2. Click the **Utilities** tab.
3. Click **Factory Defaults** in the side menu to display the Factory Defaults screen.
4. Click the **Factory Defaults** button to reset the router to factory default settings.

Utilities – Viewing the System Logs

The Utilities - System Logs screen displays the system logs.

Perform the following steps to configure the system logs.

1. Access and log into the configuration interface.
2. Click the **Utilities** tab.
3. Click **System Logs** in the side menu to display the System Logs.

When viewing the logs, click the **Refresh** button to update the list. Click the **Clear Log** button to clear the list.

Utilities – DDNS

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.

Requirements

In order to use DDNS you must first create an account with a DDNS provider. The DDNS provider maps your chosen domain name to your IP address.

Once your account is established, perform the following steps to enable DDNS.

1. Access and log into the configuration interface.
2. Click the **Utilities** tab.
3. Click **DDNS** in the side menu to display the DDNS configuration screen.
4. Click the **DDNS Enable** checkbox.

Note: Refer to DDNS (page 68) for specific instructions on setting the various DDNS configuration parameters.

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

Chapter 9

Web GUI Screens Overview

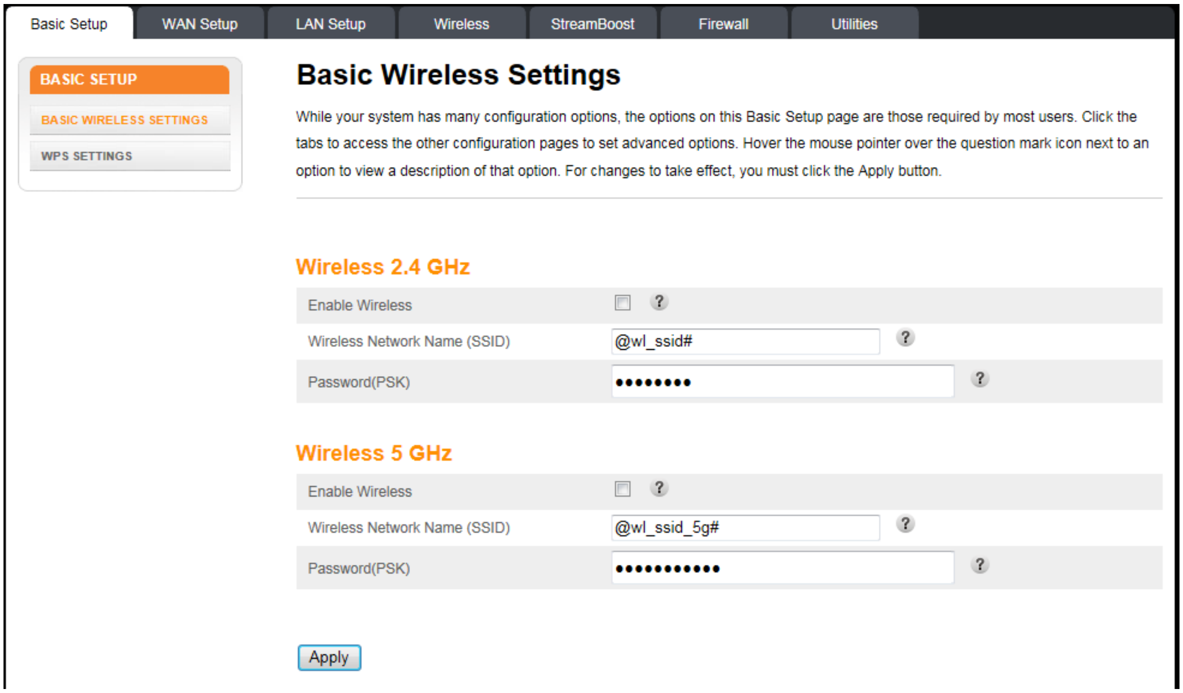
This section provides an overview of the ARRIS graphical user interface (GUI) router setup screens.

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

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

Basic Setup

Basic Wireless Settings



Basic Wireless Settings

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 2.4 GHz

Enable Wireless	□ ?
Wireless Network Name (SSID)	@wl_ssid# ?
Password(PSK)	•••••••• ?

Wireless 5 GHz

Enable Wireless	□ ?
Wireless Network Name (SSID)	@wl_ssid_5g# ?
Password(PSK)	••••••••••• ?

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 2.4 GHz/Wireless 5 GHz:

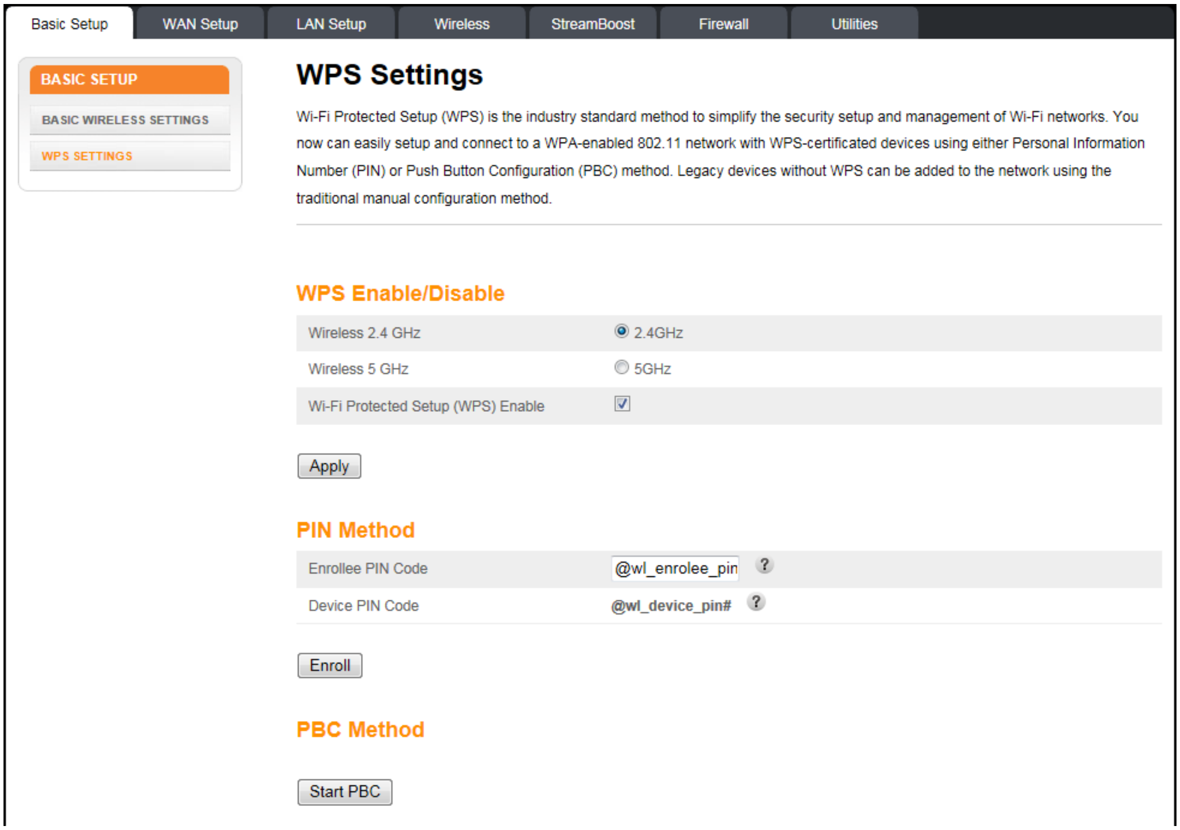
Enable Wireless – Click this checkbox to enable the wireless network on your system.

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.

Password – Sets your password. 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). 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.

WPS Settings



WPS Settings

Wi-Fi Protected Setup (WPS) is the industry standard method to simplify the security setup and management of Wi-Fi networks. You now can easily setup and connect to a WPA-enabled 802.11 network with WPS-certificated devices using either Personal Information Number (PIN) or Push Button Configuration (PBC) method. Legacy devices without WPS can be added to the network using the traditional manual configuration method.

WPS Enable/Disable

Wireless 2.4 GHz	● 2.4GHz
Wireless 5 GHz	○ 5GHz
Wi-Fi Protected Setup (WPS) Enable	☑

Apply

PIN Method

Enrollee PIN Code	@wl_enrolee_pin ?
Device PIN Code	@wl_device_pin# ?

Enroll

PBC Method

Start PBC

Wi-Fi Protected Setup (WPS) is the industry standard method to simplify the security setup and management of Wi-Fi networks. You can now easily set up and connect to a WPA-enabled 802.11 network with WPS-certified devices using either a Personal Information Number (PIN) or the Push Button Configuration (PBC) method. Legacy devices without WPS can be added to the network using the traditional manual configuration method.

WPS Enable/Disable

Wireless 2.4 GHz/Wireless 5 Ghz – Click the frequency for which you want to enable WPS.

WPS Enable – Click this checkbox to enable WPS 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.

PIN Method:

Enrollee PIN Code – If your client device has a WPS PIN number, enter it here, then click Enrolle.

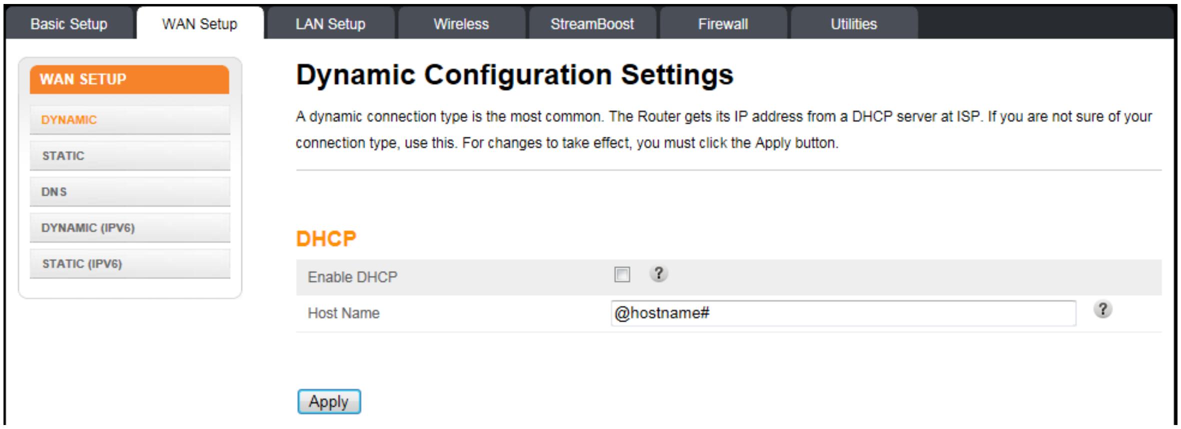
Device PIN Code – Enter this code on your computer if requested during connection.

PBC Method:

Start PBC – Click to start the PBC connection process.

WAN Setup

Dynamic



Dynamic Configuration Settings

A dynamic connection type is the most common. The Router gets its IP address from a DHCP server at ISP. 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 □

Host Name @hostname#

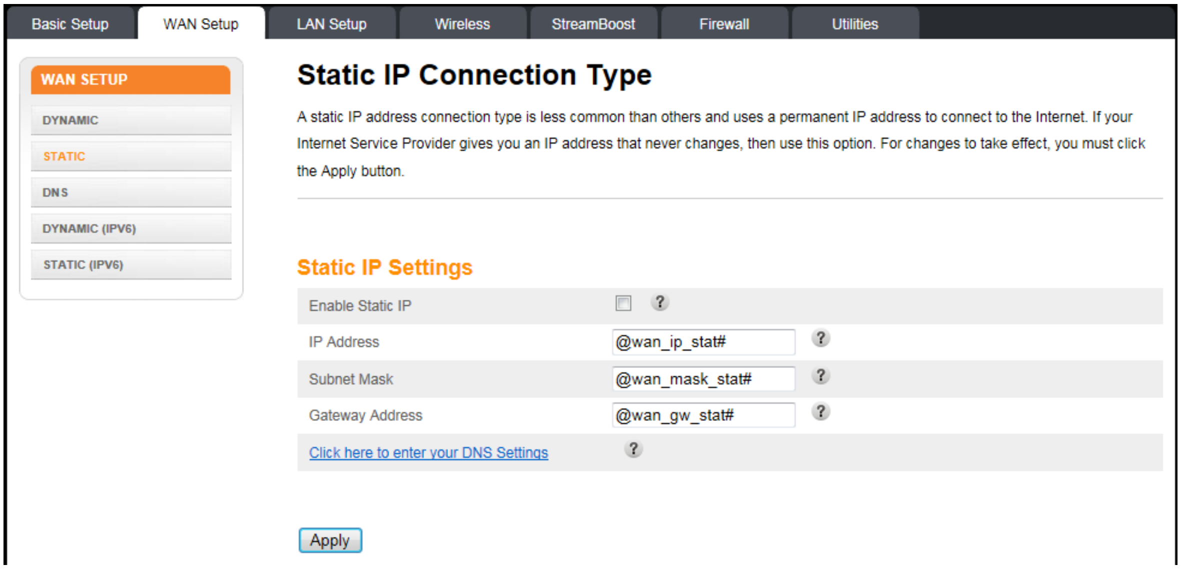
A dynamic connection type is the most common. The Wireless Router gets its IP address from a DHCP server at the cable company. If you are not sure of your connection type, use this type. For changes to take effect, you must click the **Apply** button.

DHCP

Enable DHCP – Click this checkbox to enable a DHCP connection for your system.

Host name – This field displays the host name of the Wireless Router.

Static



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	@wan_ip_stat# ?
Subnet Mask	@wan_mask_stat# ?
Gateway Address	@wan_gw_stat# ?
Click here to enter your DNS Settings	?

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 – Click this checkbox to enable a static IP address connection for your system.

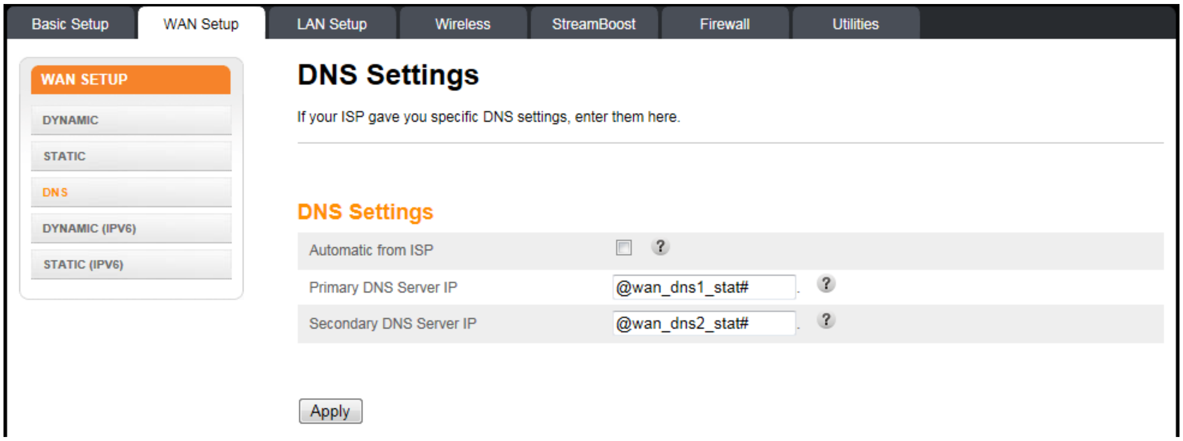
IP Address – Enter the IP address assigned by your ISP or static IP operation.

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 ISP or static IP operation.

Click here to enter your DNS Settings – If your ISP gave you specific DNS settings, click here to go to the DNS Settings screen to enter those settings.

DNS



DNS Settings

If your ISP gave you specific DNS settings, enter them here.

DNS Settings

Automatic from ISP	□ ?
Primary DNS Server IP	@wan_dns1_stat# . ?
Secondary DNS Server IP	@wan_dns2_stat# . ?

If your ISP gave you specific DNS settings, use this screen to enter them.

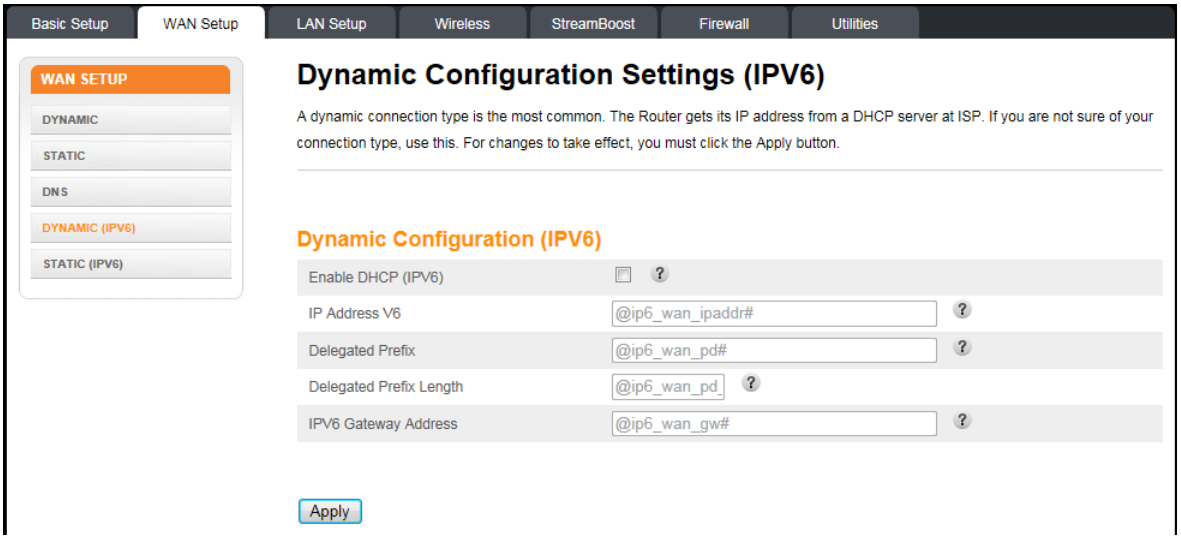
DNS Settings

Automatic from ISP – Click this checkbox if your Wireless Router should automatically get its DNS settings from your ISP.

Primary DNS Server IP – Enter the IP address of the primary DNS server.

Secondary DNS Server IP – Enter the IP address of the secondary DNS server.

Dynamic (IPV6)



Dynamic Configuration Settings (IPV6)

A dynamic connection type is the most common. The Router gets its IP address from a DHCP server at ISP. 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)	□ ?
IP Address V6	@ip6_wan_ipaddr# ?
Delegated Prefix	@ip6_wan_pd# ?
Delegated Prefix Length	@ip6_wan_pd ?
IPV6 Gateway Address	@ip6_wan_gw# ?

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) – Click this checkbox to enable a DHCP (IPV6) connection for your system.

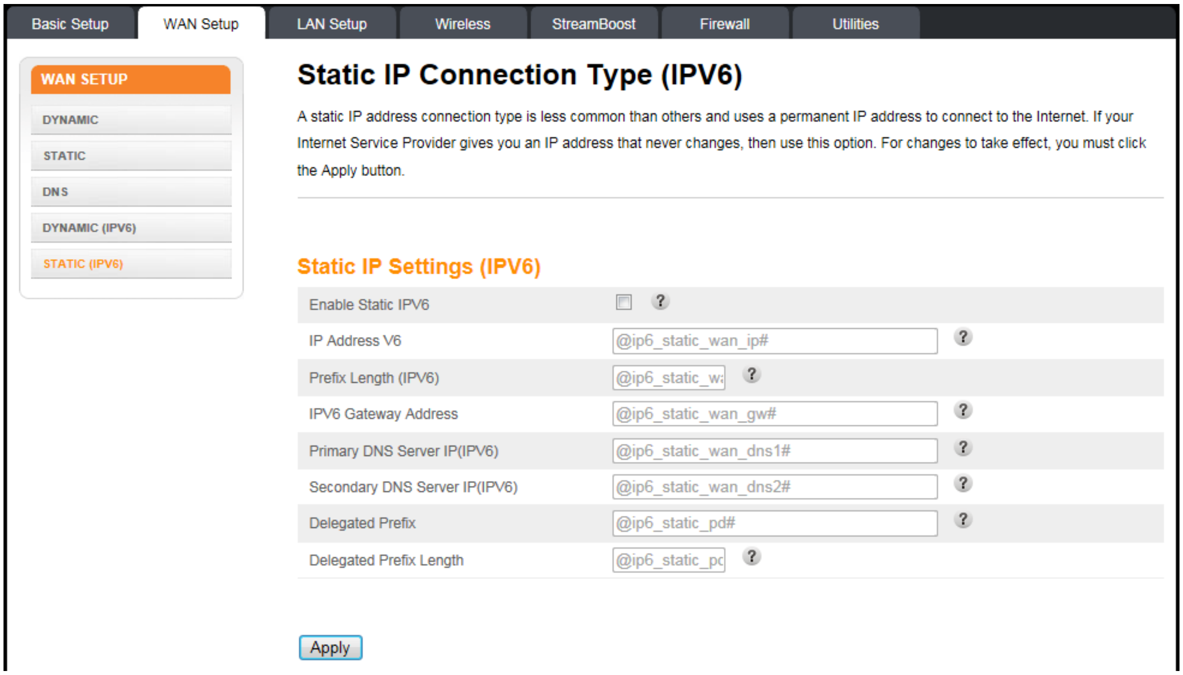
IP Address V6 – This field displays the IPV6 address automatically assigned by the MSO. An IPV6 address has eight groups of four hexadecimal digits (0-9, a-f). The groups are separated by colons (:) e.g. 2001:0db8:85a3:0000:0000:8a2e:0370:7334. A double colon (::) is shorthand for an address of all zeros.

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

Delegated Prefix Length – This field displays the assigned IPV6 prefix length.

IPV6 Gateway Address – This field displays the gateway address.

Static (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	□ ?
IP Address V6	@ip6_static_wan_ip# ?
Prefix Length (IPV6)	@ip6_static_w ?
IPV6 Gateway Address	@ip6_static_wan_gw# ?
Primary DNS Server IP(IPV6)	@ip6_static_wan_dns1# ?
Secondary DNS Server IP(IPV6)	@ip6_static_wan_dns2# ?
Delegated Prefix	@ip6_static_pd# ?
Delegated Prefix Length	@ip6_static_pc ?

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 - Click this checkbox 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. Your ISP will provide this information.

Secondary DNS Server (IPV6) – Enter the IPV6 address of the secondary DNS server. Your ISP will provide this information.

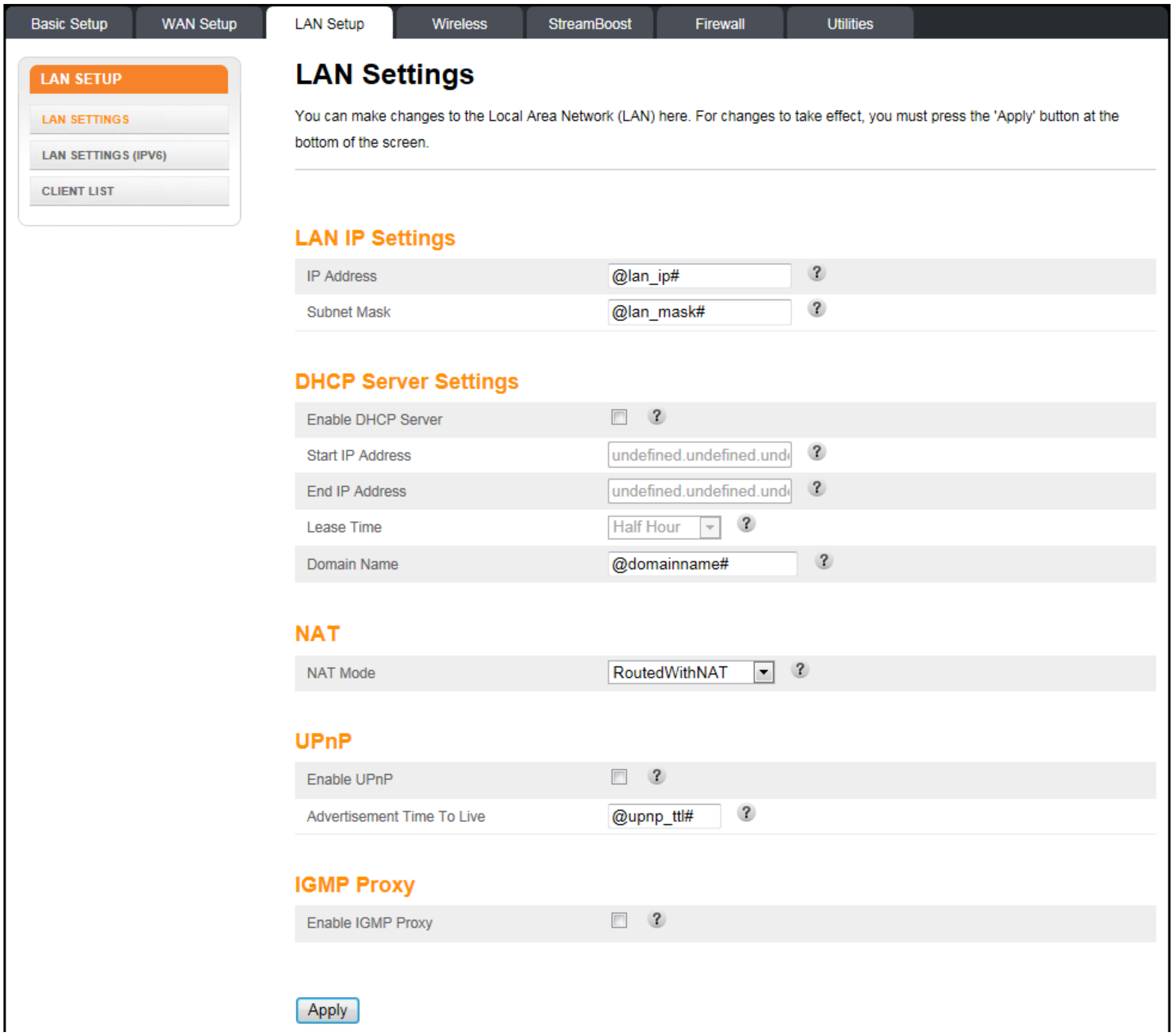
Domain Name – The entry here will be displayed as the domain name on your client devices. It can be specified by your ISP or by you.

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

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

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 IP Settings

IP Address	@lan_ip#
Subnet Mask	@lan_mask#

DHCP Server Settings

Enable DHCP Server	□
Start IP Address	undefined.undefined.und
End IP Address	undefined.undefined.und
Lease Time	Half Hour
Domain Name	@domainname#

NAT

NAT Mode	RoutedWithNAT

UPnP

Enable UPnP	□
Advertisement Time To Live	@upnp_ttl#

IGMP Proxy

Enable IGMP Proxy	□

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

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 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 – Click this checkbox 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 will be allowed to assign to a network device.

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

Lease Time – Enter the lease time in seconds before the assigned IP address will expire. (After the lease time is up, the user is automatically assigned a new dynamic IP address.)

DHCP uses the concept of a "lease" or amount of time that a given IP address will be 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.

NAT:

NAT Mode – Select the NAT Mode. Routed with NAT - Data will be routed by the device and all the outgoing packets will be NATed. Routed without NAT - Data will be routed by the device but all the outgoing packets will not be NATed. Bridged - Data will pass through the device directly without any routing.

UPnP:

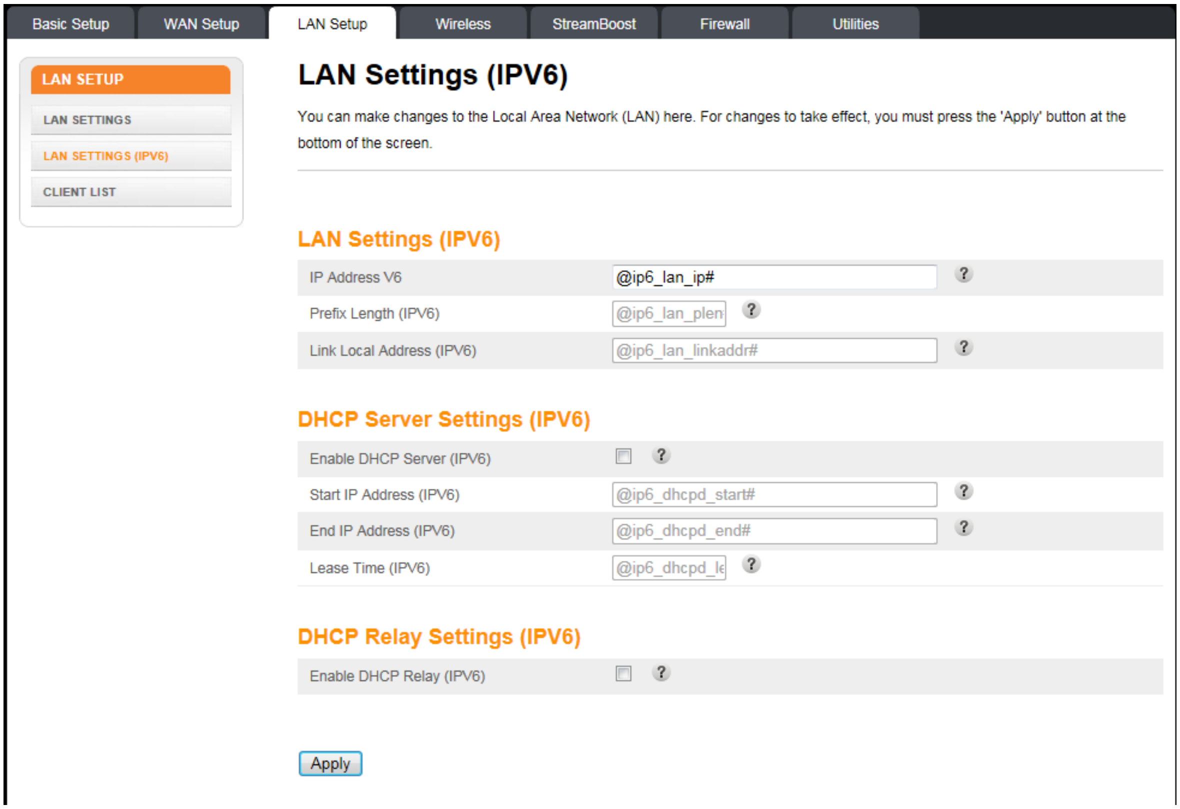
Enable UPnP – Click this checkbox to enable UPnP (Universal Plug and Play) on the system.

Advertisement Time To Live –

IGMP Proxy:

Enable IGMP Proxy – Click this checkbox to enable the IGMP (Internet Group Management Protocol) proxy on the system.

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 Settings (IPV6)

IP Address V6	@ip6_lan_ip#
Prefix Length (IPV6)	@ip6_lan_plen
Link Local Address (IPV6)	@ip6_lan_linkaddr#

DHCP Server Settings (IPV6)

Enable DHCP Server (IPV6)	□
Start IP Address (IPV6)	@ip6_dhcpd_start#
End IP Address (IPV6)	@ip6_dhcpd_end#
Lease Time (IPV6)	@ip6_dhcpd_le

DHCP Relay Settings (IPV6)

Enable DHCP Relay (IPV6)	□

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.

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) – This field displays 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 of all zeros.

Prefix Length V6 – Length of the network portion of the IPV6 address.

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

DHCP Server Settings (IPV6):

Enable DHCP Server (IPV6) – Click this checkbox 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 will be allowed to assign to a network device.

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

Lease Time V6 – Enter the lease time in seconds before the assigned IPV6 address will expire. (After the lease time is up, the user is automatically assigned a new dynamic IP address.)

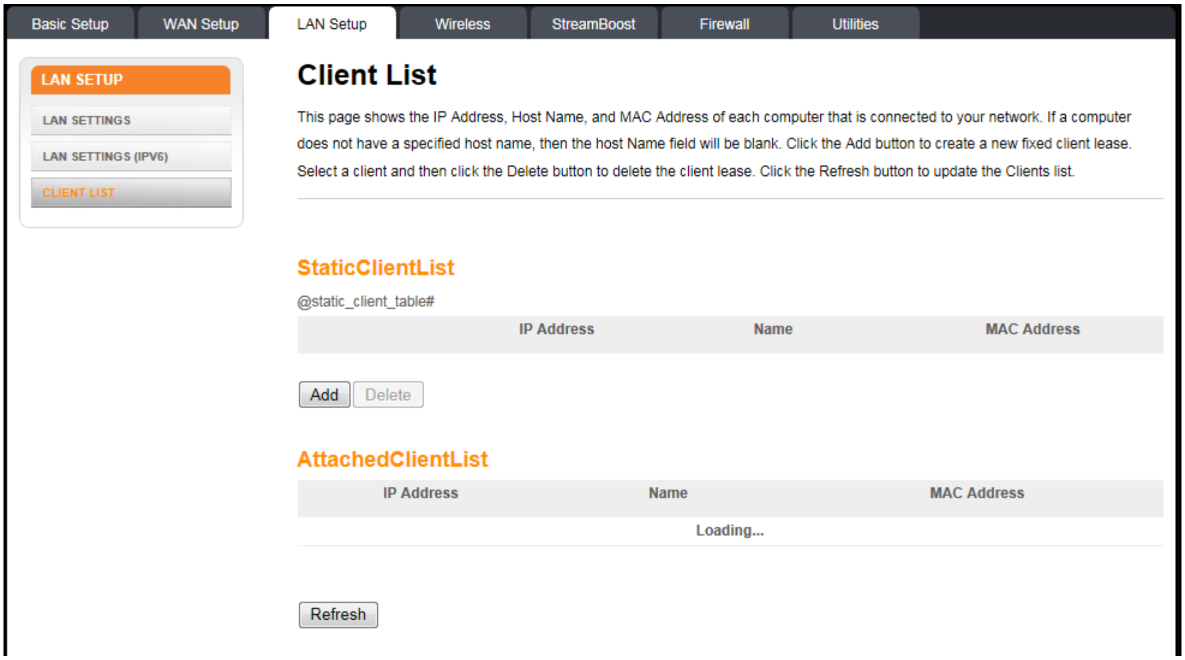
DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer or other network device. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. Using very short leases, DHCP can dynamically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

DNS Relay Settings (IPV6):

Enable DNS Relay (IPV6) – Click this checkbox to enable DNS Relay and mask the DNS address.

Click this checkbox to enable Domain Name System (DNS) relay functionality on your system. The DNS Relay feature allows the system to act as a DNS server to other IP stations, while it simply forwards the requests to real DNS servers and then sends their responses back to the original requesters. Your gateway basically acts as an intermediate between the requester and the real DNS servers. When DNS Relay is enabled, the gateway will act as a DNS server, send requests to the Internet Service Provider's DNS server, and cache the information for later access. When DNS relay is disabled, the computer will pull domain name/IP address information directly from the ISP's DNS server.

Client List



Client List

This page shows the IP Address, Host Name, 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.

StaticClientList

@static_client_table#

IP Address	Name	MAC Address

AttachedClientList

IP Address	Name	MAC Address
	Loading...	

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.

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.

Static Client List:

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

IP Address – Enter the client's IP address.

Name – Enter a name for the client.

MAC Address – Enter the client's MAC address.

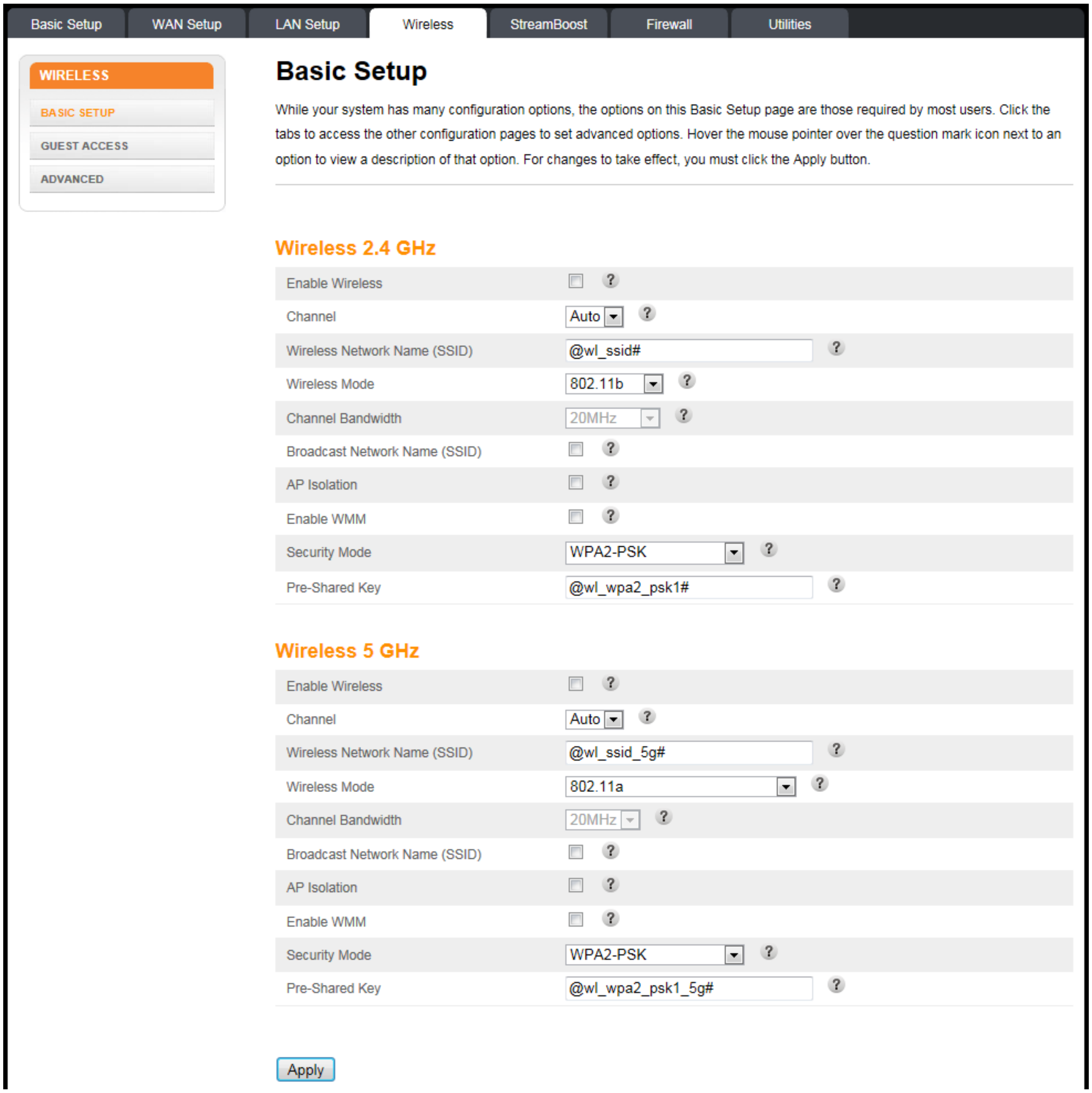
Select a client and then click the **Delete** button to delete the client lease.

Attached Client List:

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

Wireless

Basic Setup



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 2.4 GHz

Enable Wireless	☐ ?
Channel	Auto ?
Wireless Network Name (SSID)	@wl_ssid# ?
Wireless Mode	802.11b ?
Channel Bandwidth	20MHz ?
Broadcast Network Name (SSID)	☐ ?
AP Isolation	☐ ?
Enable WMM	☐ ?
Security Mode	WPA2-PSK ?
Pre-Shared Key	@wl_wpa2_psk1# ?

Wireless 5 GHz

Enable Wireless	☐ ?
Channel	Auto ?
Wireless Network Name (SSID)	@wl_ssid_5g# ?
Wireless Mode	802.11a ?
Channel Bandwidth	20MHz ?
Broadcast Network Name (SSID)	☐ ?
AP Isolation	☐ ?
Enable WMM	☐ ?
Security Mode	WPA2-PSK ?
Pre-Shared Key	@wl_wpa2_psk1_5g# ?

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.

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.

Wireless 2.4 GHz/Wireless 5 GHz

Enable Wireless – Click this checkbox to enable the wireless network on your system.

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, it's best to choose channel 1, 6, or 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.

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.

Wireless Mode – Sets the wireless mode. 2.4 GHz Options are: B/G mixed, B only, G only, and G/N mixed. 5 GHz Options are: A only, A/N mixed, and A/N/AC mixed. Select the proper mode to support all of the wireless devices that will 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. 802.11ac support bandwidth up to 1.3Gb/s.)

Channel Bandwidth – Sets the 802.11n Channel Bandwidth. Options are 20 MHz, 40MHz,20/40 MHz, or 80 MHz (5 GHz only). The default setting is 20/40 MHz.

Broadcast Network Name (SSID) – Click this checkbox 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.

AP Isolation – Click this checkbox to enable AP isolation. When enabled each of your wireless clients will be in its own virtual network and will not be able to communicate with one another. This may be useful if you have many quests using your network.

Enable WMM – Click this checkbox to enable Wi-Fi Multimedia (WMM) functionality. Enabling WMM can help control latency and jitter when transmitting multimedia content over a wireless connection. Disabling WMM will reduce wireless performance in 802.11n mode.

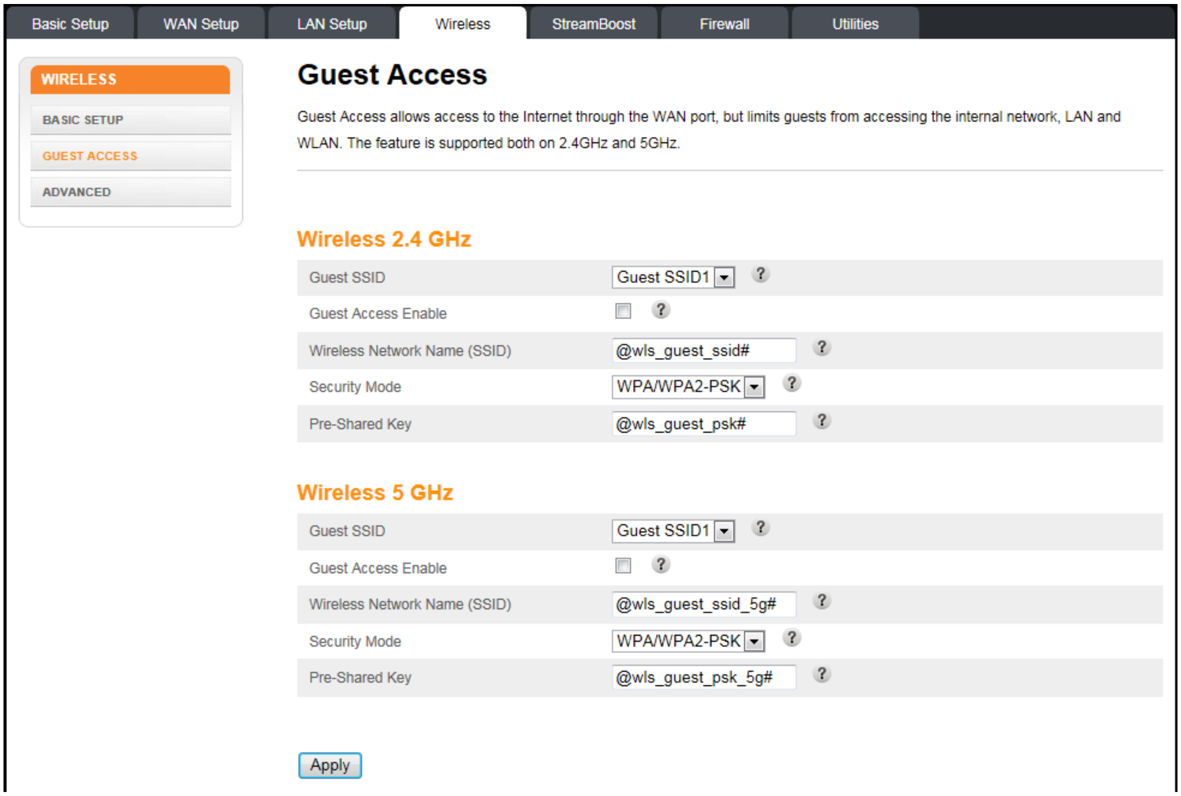
This quality of service mechanism uses four access categories, which in order of priority are: voice, video, best effort, and background. This ensures that applications with low tolerance for latency and jitter are treated with higher priority than less-sensitive data applications. WMM sets different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

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

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 printable special characters (such as $, !, ?, &,

#, @, and others). A hexadecimal key must be 64 characters long. Valid characters are numbers "0" through "9" and letters "a" through "f".

Guest Access



Guest Access

Guest Access allows access to the Internet through the WAN port, but limits guests from accessing the internal network, LAN and WLAN. The feature is supported both on 2.4GHz and 5GHz.

Wireless 2.4 GHz

Guest SSID	Guest SSID1
Guest Access Enable	☐
Wireless Network Name (SSID)	@wls_guest_ssid#
Security Mode	WPA/WPA2-PSK
Pre-Shared Key	@wls_guest_psk#

Wireless 5 GHz

Guest SSID	Guest SSID1
Guest Access Enable	☐
Wireless Network Name (SSID)	@wls_guest_ssid_5g#
Security Mode	WPA/WPA2-PSK
Pre-Shared Key	@wls_guest_psk_5g#

Guest access allows access to the Internet through the WAN port, but it limits guests from accessing the internal network, LAN, and WLAN. The feature is supported both on 2.4 GHz and 5 GHz.

Wireless 2.4 GHz/Wireless 5 GHz:

Guest SSID –

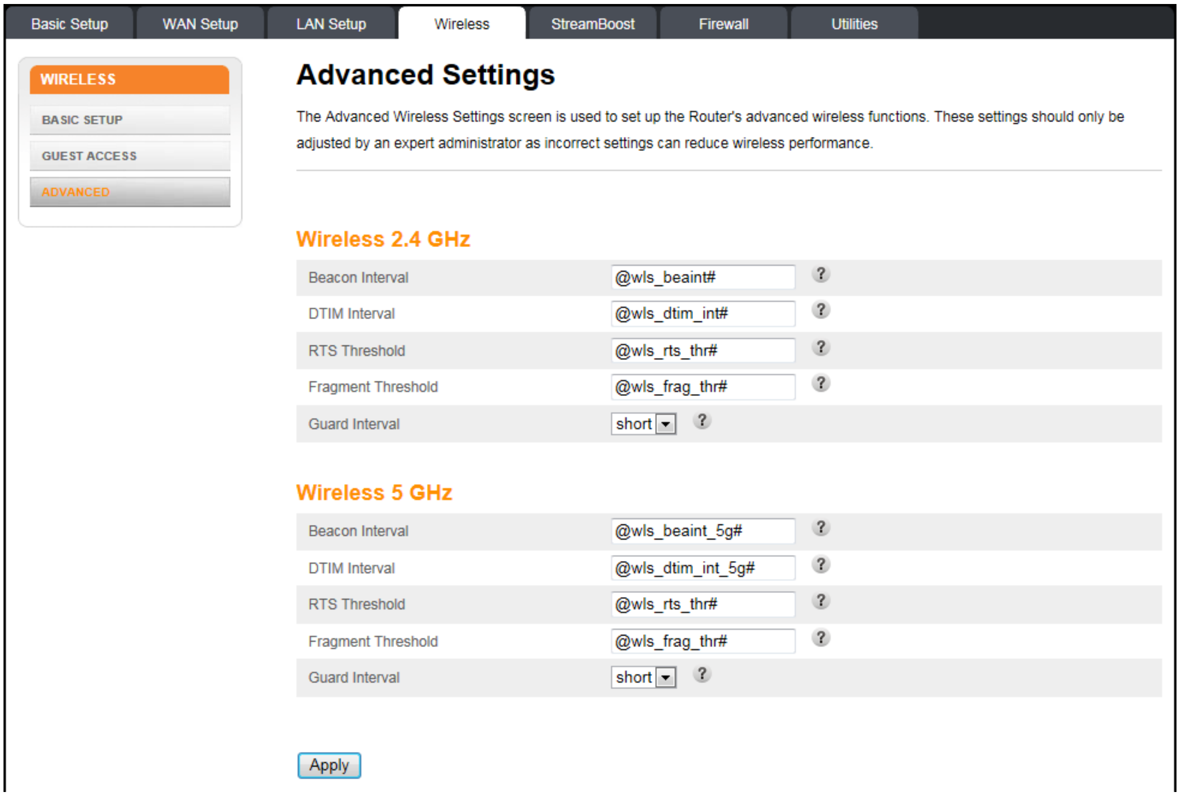
Guest Access Enable – Click this checkbox to enable guest access for your system.

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

Security mode – Sets the security mode for your router. Available options are WPA/WPA2-PSK or Open.

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’ as well as most other characters. A hexadecimal key must be 64 characters long. Valid characters are numbers ‘0’ through ‘9’ and letters ‘a’ through ‘f’.

Advanced



Advanced Settings

The 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 2.4 GHz

Beacon Interval	@wls_beaint#
DTIM Interval	@wls_dtim_int#
RTS Threshold	@wls_rts_thr#
Fragment Threshold	@wls_frag_thr#
Guard Interval	short

Wireless 5 GHz

Beacon Interval	@wls_beaint_5g#
DTIM Interval	@wls_dtim_int_5g#
RTS Threshold	@wls_rts_thr#
Fragment Threshold	@wls_frag_thr#
Guard Interval	short

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 2.4 GHz/Wireless 5 GHz:

Note: These older 802.11b devices required the unit to add overhead to most transmissions. Performance will increase if no 802.11b devices are present and this feature is disabled (OFF). The unit will auto detect 802.11b devices and set 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 compliance with most client devices, the Beacon Interval should remain set at the default of 100ms. The allowable setting range is from 20 to 1024ms.

DTM 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 compliance with most client devices, the DTIM Interval should be left at 1 ms. The allowable setting range is from 1 to 255 ms.

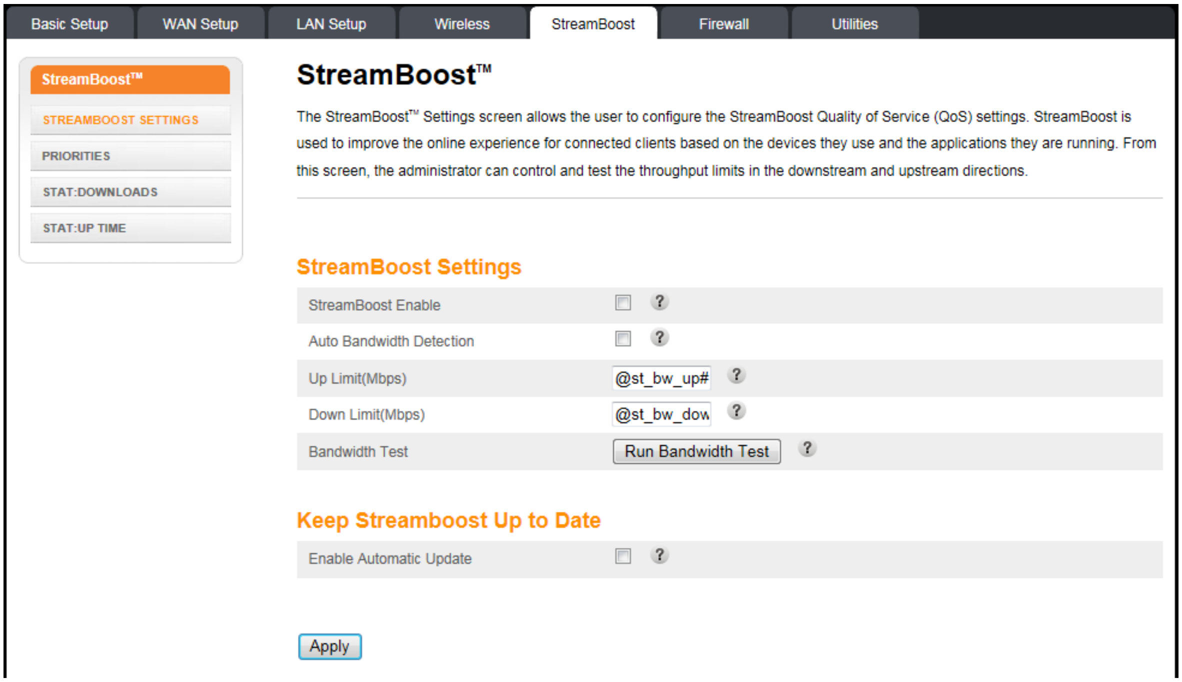
RTS Threshold – Sets the packet size limit. When the threshold is passed, the ready to send/clear to send (RTS/CTS) function is invoked. The default setting is 2347 bytes. The allowable setting range is from 1 to 2347 bytes.

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.

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).

StreamBoost

StreamBoost Settings



StreamBoost™

The StreamBoost™ Settings screen allows the user to configure the StreamBoost Quality of Service (QoS) settings. StreamBoost is used to improve the online experience for connected clients based on the devices they use and the applications they are running. From this screen, the administrator can control and test the throughput limits in the downstream and upstream directions.

StreamBoost Settings

StreamBoost Enable	□	?
Auto Bandwidth Detection	□	?
Up Limit(Mbps)	@st_bw_up#	?
Down Limit(Mbps)	@st_bw_dow	?
Bandwidth Test	Run Bandwidth Test	?

Keep Streamboost Up to Date

Enable Automatic Update	□	?

Apply

The StreamBoost Settings screen lets users configure the StreamBoost Quality of Service (QoS) settings. StreamBoost is used to improve the online experience for connected clients based on the devices they use and the applications they are running. From this screen, the administrator can control and test the throughput limits in the downstream and upstream directions.

StreamBoost Settings:

StreamBoost Enable – Click this checkbox to enable StreamBoost technology.

Auto Bandwidth Detection – Click this checkbox to enable Auto Bandwidth Detection.

Up Limit (Mbps) –

Down limit (Mbps) –

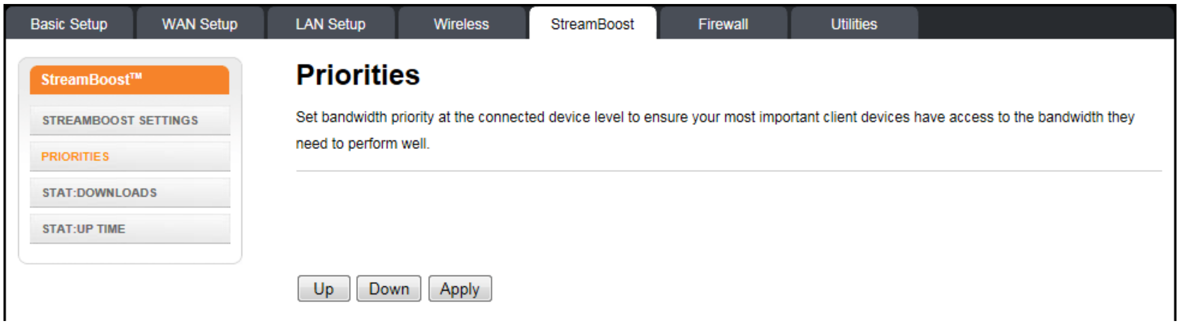
NOTE TO REVIEWERS: What do I need to say about Up Limit and Down Limit? What do these fields do?

Bandwidth Test – Click this button to run the bandwidth test.

Keep StreamBoost Up to Date:

Enable Automatic Update – Click this checkbox to enable automatic StreamBoost updates during your initial 3-year manufacturer service term. The service term will begin on the date of manufacture and run for three years or until April 1st, 2017, whichever comes first. (After the 3-year period, the manufacturer may make further updates available via firmware updates.) StreamBoost updates may improve your router's Internet traffic management capabilities through better traffic identification and bandwidth management techniques. In exchange, your Wireless Router will provide anonymous, performance-related information to the StreamBoost server for improved future StreamBoost service.

Priorities

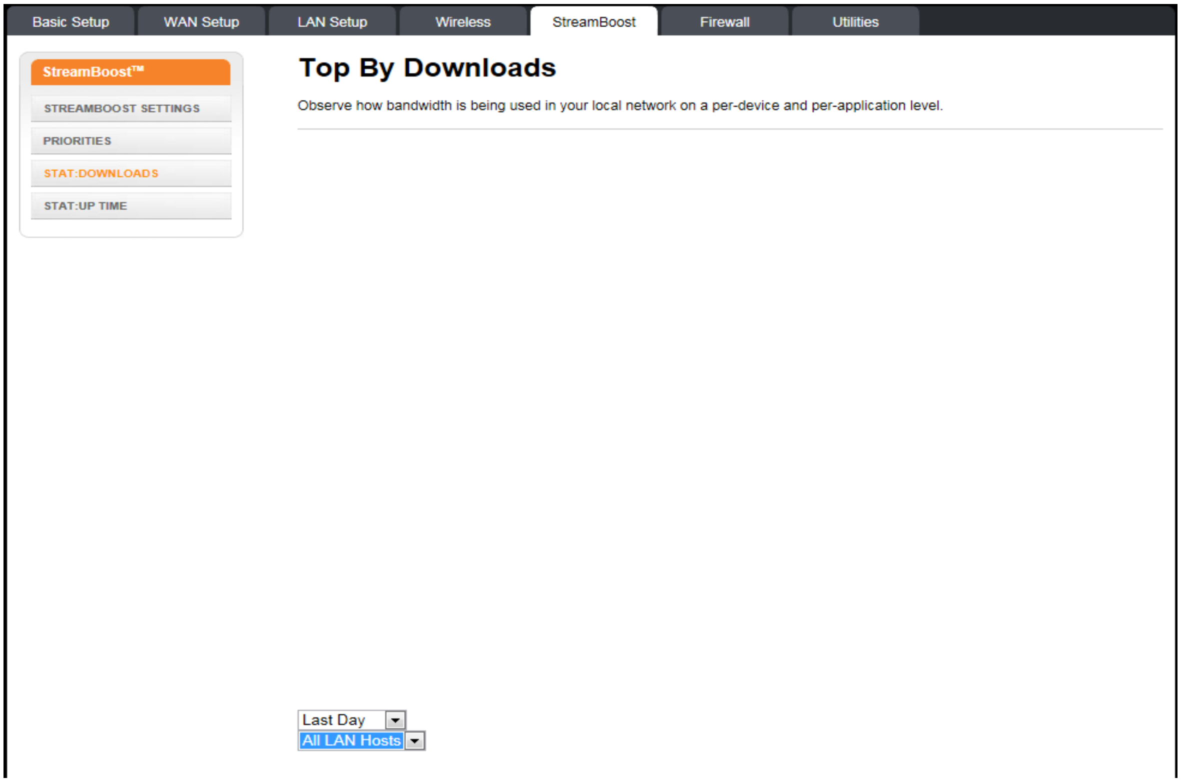


Priorities

Set bandwidth priority at the connected device level to ensure your most important client devices have access to the bandwidth they need to perform well.

Set bandwidth priority at the connected device level to ensure that your most important client devices have access to the bandwidth they need to perform well.

STAT: Downloads



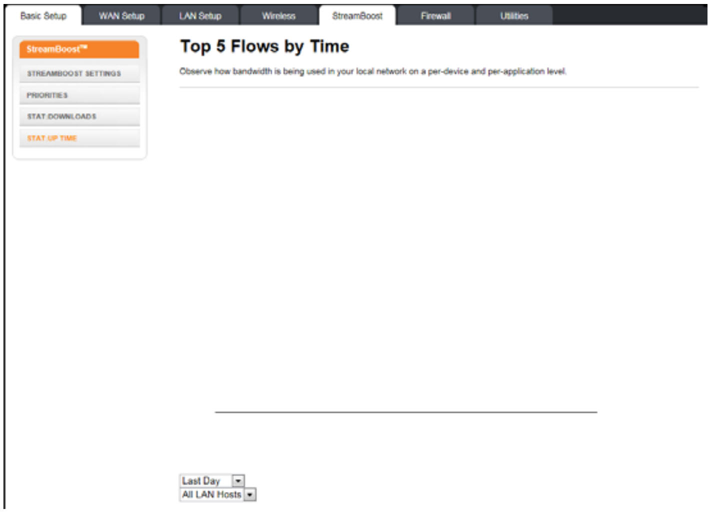
Top By Downloads

Observe how bandwidth is being used in your local network on a per-device and per-application level.

Observe how bandwidth is being used in your local network on a per-device and per-application level.

NOTE TO REVIEWERS: What should users do with this screen? Will the dropdown boxes at the bottom be labeled in any way?

STAT: Up Time



Top 5 Flows by Time

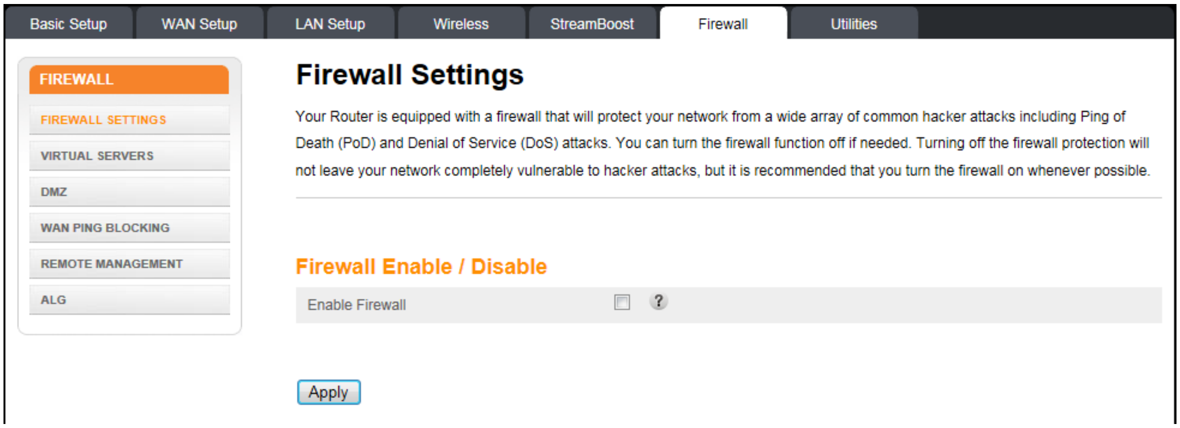
Observe how bandwidth is being used in your local network on a per-device and per-application level.

Last Day ▾
All LAN Hosts ▾

Observe how bandwidth is being used in your local network on a per-device and per-application level.

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

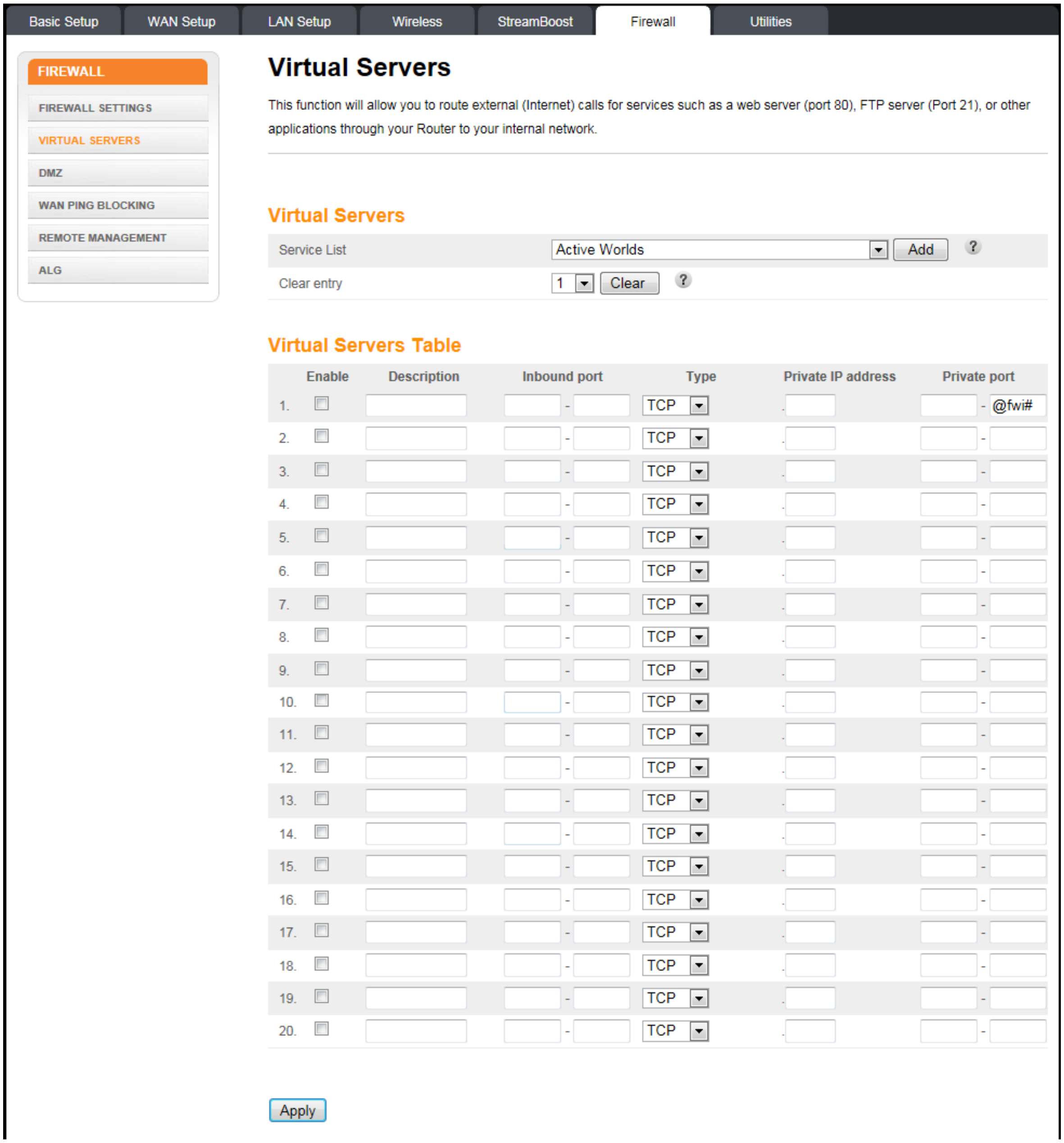
Enable Firewall □ ?

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 disable the firewall function if needed. Turning off the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you enable the firewall whenever possible. For changes to take effect, you must click the **Apply** button.

Firewall Enable/Disable:

Enable Firewall – Click this checkbox to enable the firewall on your system.

Virtual Servers



Virtual Servers

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

Service List	Active Worlds ▾ Add ?
Clear entry	1 ▾ Clear ?

Virtual Servers Table

	Enable	Description	Inbound port	Type	Private IP address	Private port
1.	☐		-	TCP ▾		- @fwi#
2.	☐		-	TCP ▾		-
3.	☐		-	TCP ▾		-
4.	☐		-	TCP ▾		-
5.	☐		-	TCP ▾		-
6.	☐		-	TCP ▾		-
7.	☐		-	TCP ▾		-
8.	☐		-	TCP ▾		-
9.	☐		-	TCP ▾		-
10.	☐		-	TCP ▾		-
11.	☐		-	TCP ▾		-
12.	☐		-	TCP ▾		-
13.	☐		-	TCP ▾		-
14.	☐		-	TCP ▾		-
15.	☐		-	TCP ▾		-
16.	☐		-	TCP ▾		-
17.	☐		-	TCP ▾		-
18.	☐		-	TCP ▾		-
19.	☐		-	TCP ▾		-
20.	☐		-	TCP ▾		-

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:

Service List – Select the kind of service you would like to set up, and click **Add**.

Clear Entry – To clear an entry from the Virtual Servers Table, select the entry that you want to clear and click **Clear**.

Virtual Servers Table:

Description – Enter a name for the virtual server.

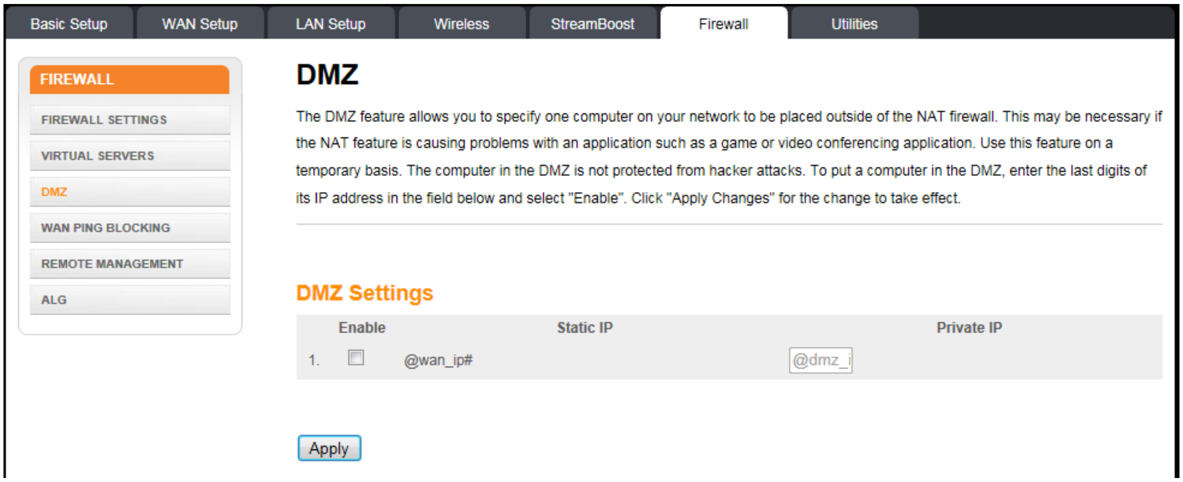
Inbound Port – Enter the inbound port range for the virtual server. It should be the same range as the local port.

Type – 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.

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

DMZ



DMZ

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 last digits of its IP address in the field below and select "Enable". Click "Apply Changes" for the change to take effect.

DMZ Settings

	Enable	Static IP	Private IP
1.	□	@wan_ip#	@dmz_i

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.

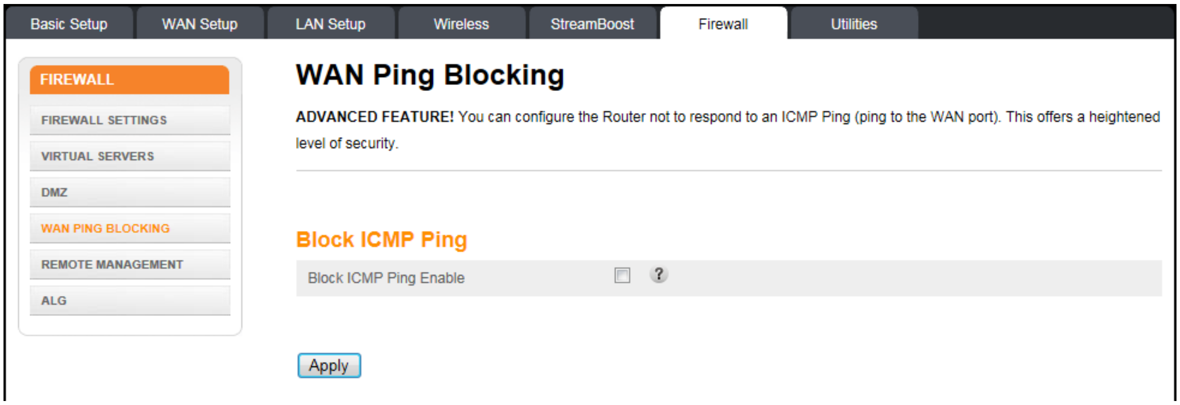
IP Address Of Virtual DMZ Host:

Enable DMZ – Click this checkbox to enable DMZ on your network.

Static IP – Displays the Static 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.

WAN Ping Blocking



WAN Ping Blocking

ADVANCED FEATURE! You can configure the Router not to respond to an ICMP Ping (ping to the WAN port). This offers a heightened level of security.

Block ICMP Ping

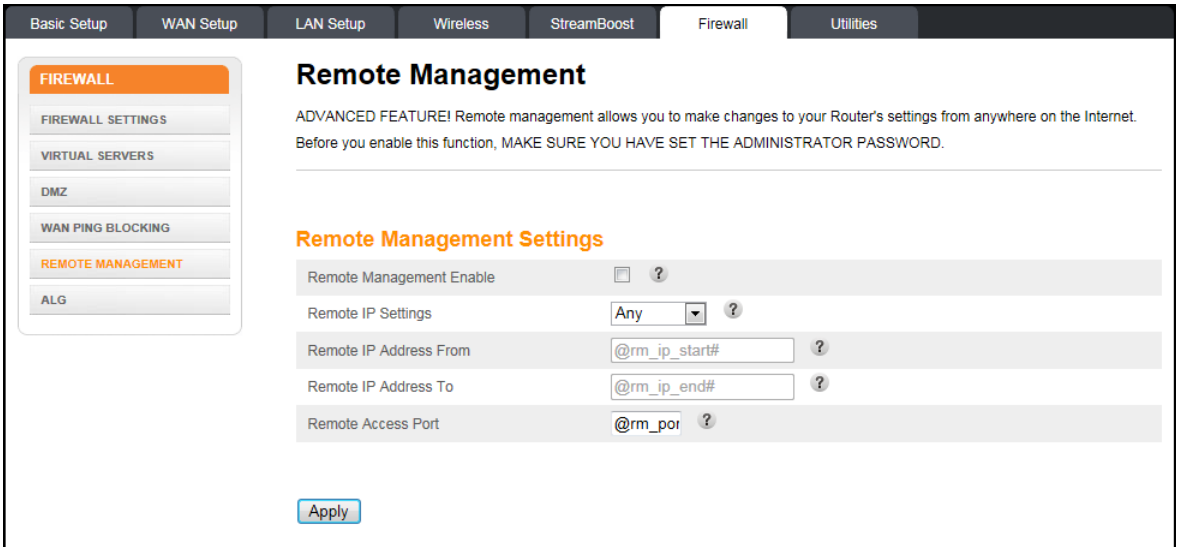
Block ICMP Ping Enable ☐ ?

You can configure the Wireless Router not to respond to an ICMP Ping (ping to the WAN port). This offers a heightened level of security.

Block ICMP Ping:

Block ICMP Ping Enable – Click this checkbox to enable WAN Ping Blocking.

Remote Management



Remote Management

ADVANCED FEATURE! Remote management allows you to make changes to your Router's settings from anywhere on the Internet. Before you enable this function, MAKE SURE YOU HAVE SET THE ADMINISTRATOR PASSWORD.

Remote Management Settings

Remote Management Enable	☐ ?
Remote IP Settings	Any ?
Remote IP Address From	@rm_ip_start# ?
Remote IP Address To	@rm_ip_end# ?
Remote Access Port	@rm_por ?

Remove management lets you make changes to your Wireless Router's settings from anywhere on the Internet. Before you enable this function, make sure you have set the administrator password.

Remote Management Settings:

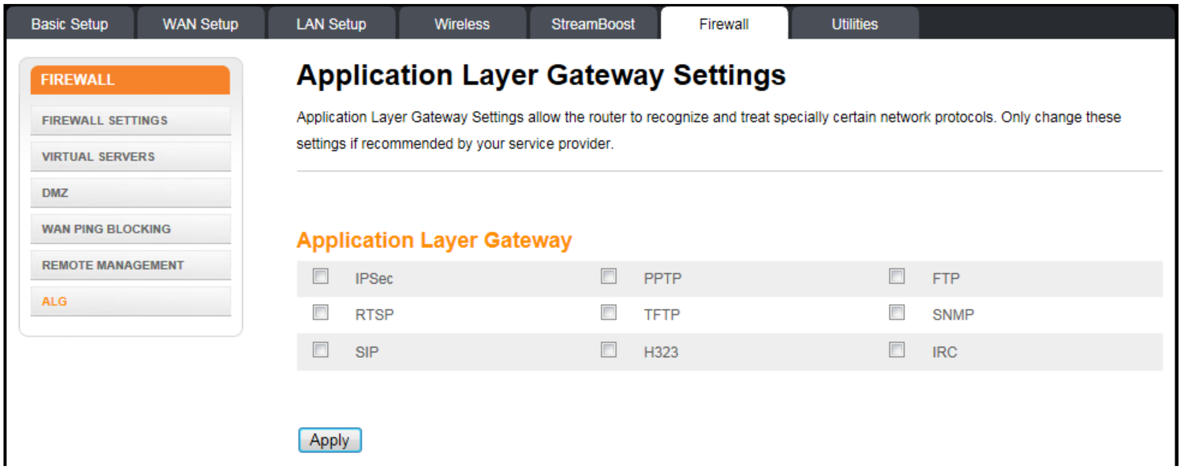
Remote Management Enable – Click this checkbox to enable the Remote Management feature.

Remote IP Settings – Select Any to allow management connections from any IP address, or select IP Range to specify a range of IP addresses that can connect.

Remote IP Address From/To – Use these fields to enter the IP addresses that can connect to make changes to your settings. You must set **Remote IP Settings** to IP Range to activate these fields.

Remote Access Port – Enter the port that you would like to use for remote access.

ALG



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

□ IPSec	□ PPTP	□ FTP
□ RTSP	□ TFTP	□ SNMP
□ SIP	□ H323	□ IRC

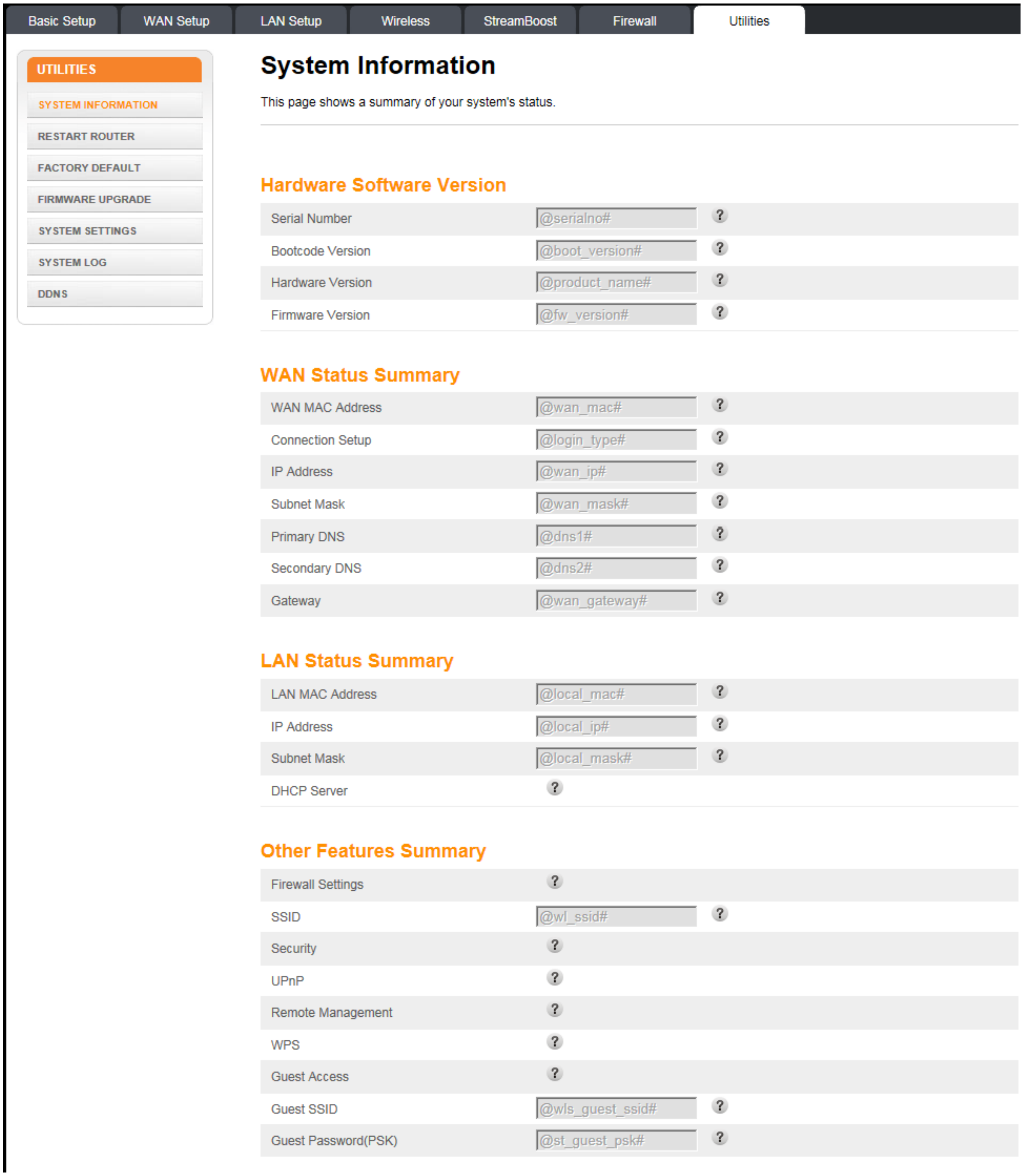
Application layer gateway settings allow the router to recognize and treat certain network protocols specially.

Application Layer Gateway:

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

Utilities

System Information



System Information

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

Hardware Software Version

Serial Number	@serialno#
Bootcode Version	@boot_version#
Hardware Version	@product_name#
Firmware Version	@fw_version#

WAN Status Summary

WAN MAC Address	@wan_mac#
Connection Setup	@login_type#
IP Address	@wan_ip#
Subnet Mask	@wan_mask#
Primary DNS	@dns1#
Secondary DNS	@dns2#
Gateway	@wan_gateway#

LAN Status Summary

LAN MAC Address	@local_mac#
IP Address	@local_ip#
Subnet Mask	@local_mask#
DHCP Server	

Other Features Summary

Firewall Settings	
SSID	@wl_ssid#
Security	
UPnP	
Remote Management	
WPS	
Guest Access	
Guest SSID	@wls_guest_ssid#
Guest Password(PSK)	@st_guest_psk#

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

Hardware Software Version:

Serial Number – This field displays the product serial number.

Bootcode Version – This field displays the bootcode version.

Hardware Version – This field displays the hardware version.

Firmware Version – This field displays the firmware version.

WAN Status Summary:

WAN MAC Address – This field displays the WAN MAC address.

Connection Setup – This field displays the connection type: Dynamic or Static

IP Address – This field displays the WAN IP address.

Subnet Mask – This field displays the WAN subnet mask.

Primary DNS – This field displays the Primary DNS IP address.

Secondary DNS – This field displays the Secondary DNS IP address.

Gateway – This field displays the gateway IP address.

LAN Status Summary:

MAC Address – This field displays the LAN MAC Address.

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

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

DHCP Server – This field displays the status of the DHCP Server: Enabled or Disabled.

Other Features Summary:

Firewall Settings - This field displays the status of the firewall settings: Enabled or Disabled.

SSID – This field displays the status of the SSID Broadcast function: Enabled or Disabled.

Security – This field displays the status of the Security feature: Enabled or Disabled.

UPNP – This field displays the status of the UPnP feature: Enabled or Disabled.

Remote Management – This field displays the status of the Remote Management feature: Enabled or Disabled.

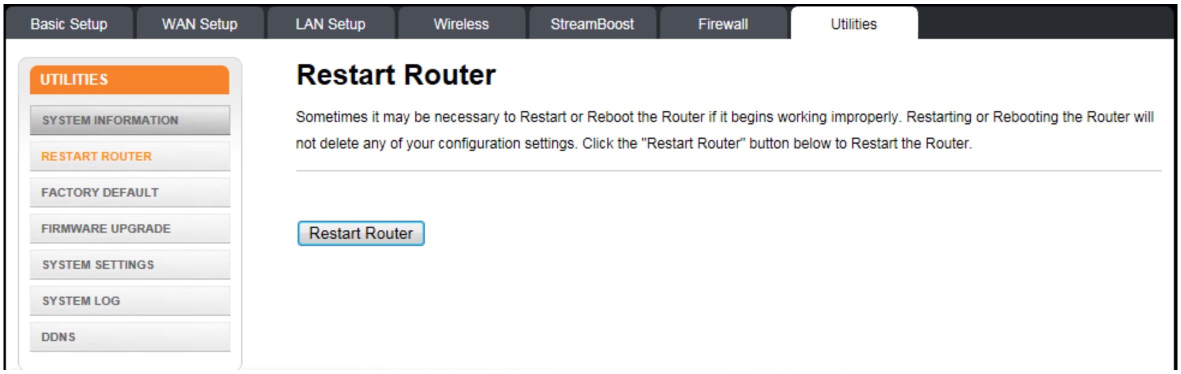
WPS – This field displays the status of the WPS function: Enabled or Disabled.

Guest Access – This field displays the status of the Guest Access function: Enabled or Disabled.

Guest SSID –

Guest Password (PSK) –

Restart Router



Restart Router

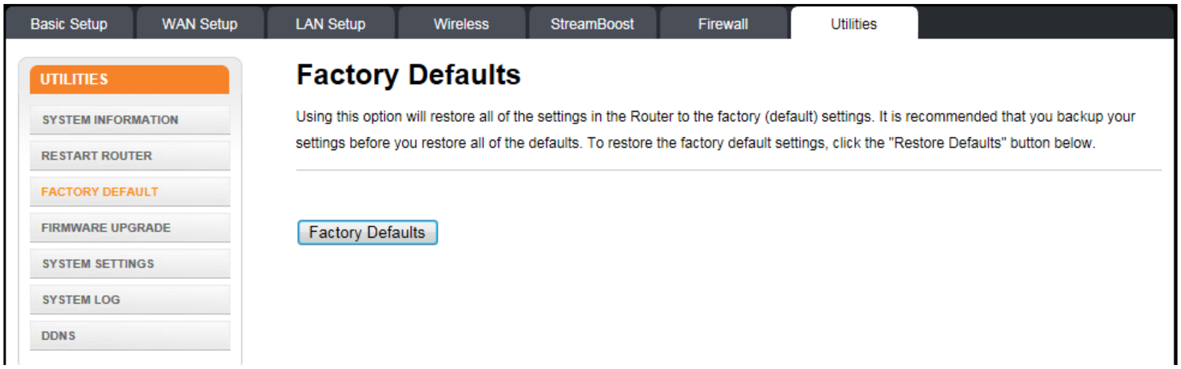
Sometimes it may be necessary to Restart or Reboot the Router if it begins working improperly. Restarting or Rebooting the Router will not delete any of your configuration settings. Click the "Restart Router" button below to Restart the Router.

It may be necessary to restart (reboot) the router if it begins working improperly. Restarting the router will 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.

Factory Default



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 "Restore Defaults" button below.

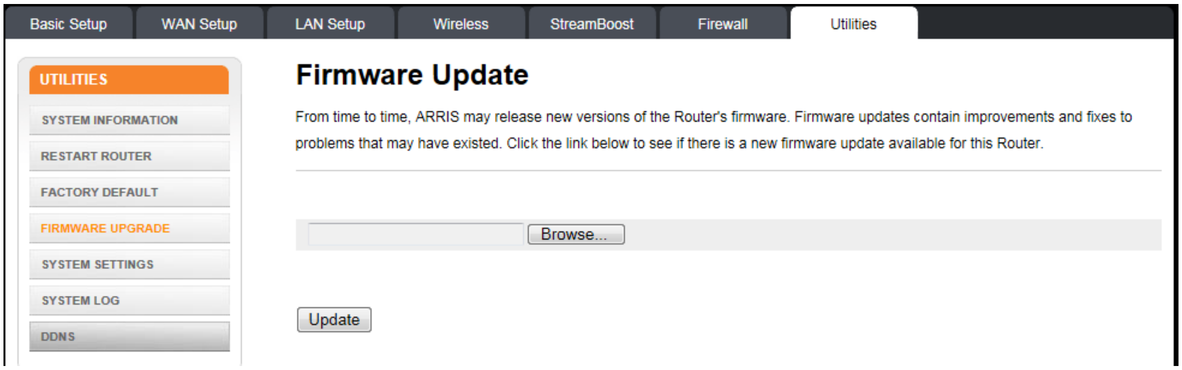
This function restores all of the router’s configuration settings to the factory default setting. Before restoring the factory defaults, you should back up your current configuration settings using the Save/Backup Settings page.

NOTE TO REVIEWERS: The text on this screen says that users can backup their settings. How do they do that?

Click the **Factory Default**s 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.

Firmware Upgrade

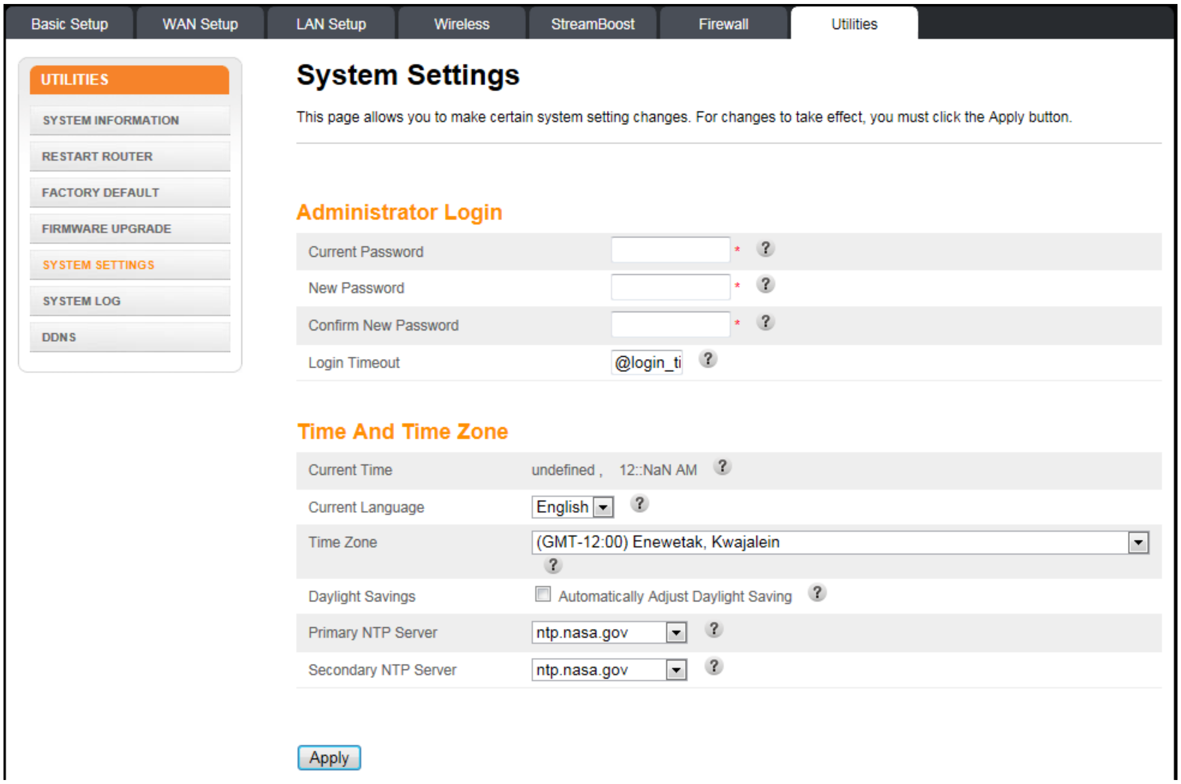


Firmware Update

From time to time, ARRIS may release new versions of the Router's firmware. Firmware updates contain improvements and fixes to problems that may have existed. Click the link below to see if there is a new firmware update available for this Router.

From time to time, ARRIS may release new versions of firmware for the Wireless Router. Firmware updates contain improvements and fixes to problems that may have existed. Click the link below to see if there is a new firmware update available for this <TSProductType).

System Settings



System Settings

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

Administrator Login

Current Password	* ?
New Password	* ?
Confirm New Password	* ?
Login Timeout	@login_ti ?

Time And Time Zone

Current Time	undefined , 12::NaN AM ?
Current Language	English ?
Time Zone	(GMT-12:00) Enewetak, Kwajalein ?
Daylight Savings	□ Automatically Adjust Daylight Saving ?
Primary NTP Server	ntp.nasa.gov ?
Secondary NTP Server	ntp.nasa.gov ?

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

Administrator Login:

Current Password – Enter your old password to change your password.

New Password/Confirm New Password – Enter your new password in both fields to change your password.

Login Timeout – Enter the number of seconds that these web pages can remain idle before the user is logged out.

Time And Time Zone:

Current Time – Displays the current time.

Current Language – Select the language you want to use.

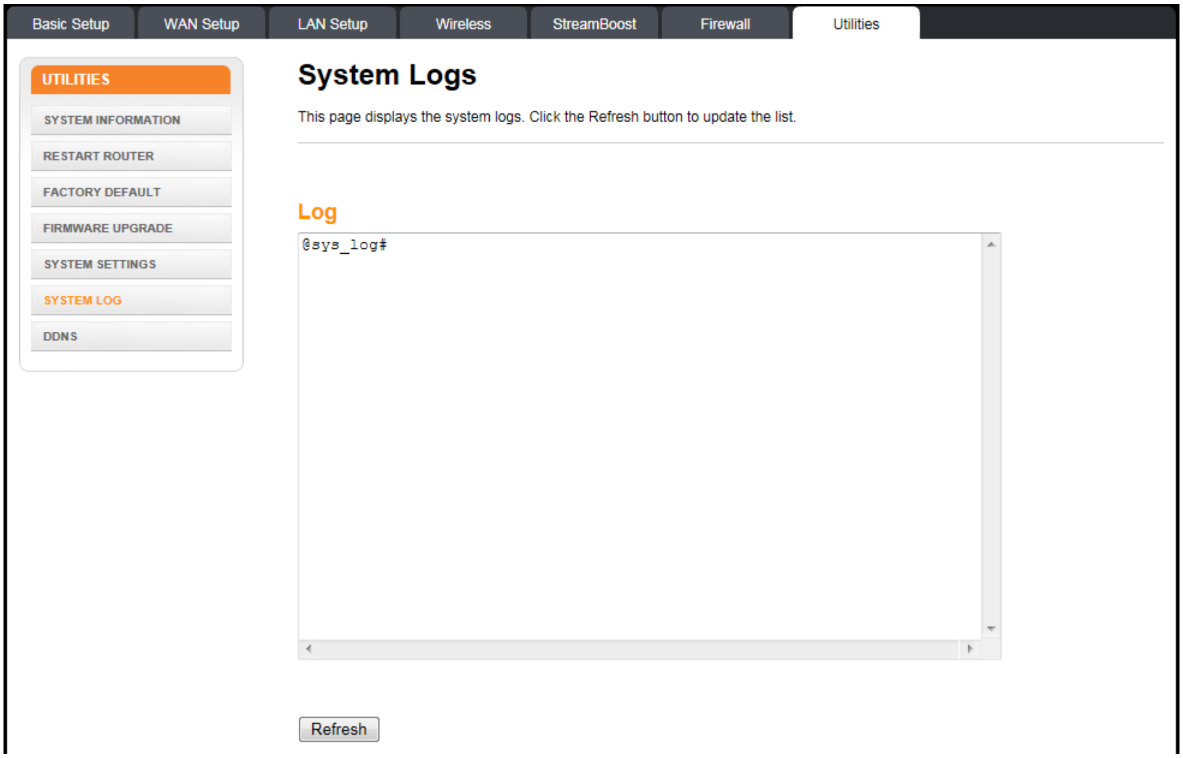
Time Zone – Select your time zone.

Daylight Savings – Click this checkbox to automatically update the system clock for Daylight Saving Time.

Primary NTP Server – The host name or IP address of the primary NTP server.

Secondary NTP Server – The host name or IP address of the secondary NTP server.

System Log



System Logs

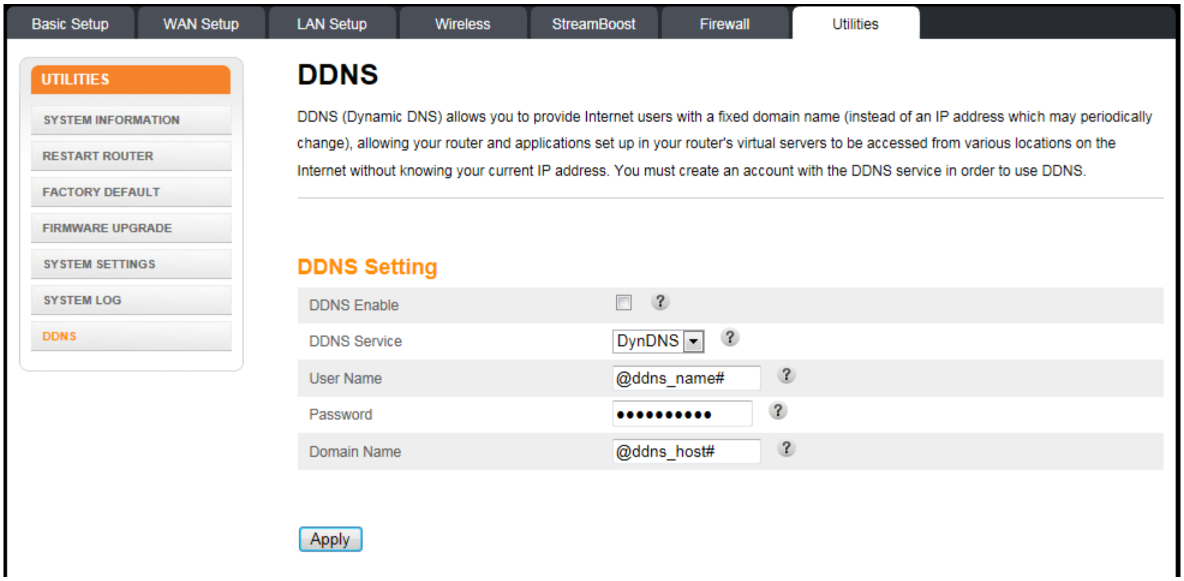
This page displays the system logs. Click the Refresh button to update the list.

Log

```
@sys_log#
```

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

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 ▾ ?
User Name	@ddns_name# ?
Password	•••••••••• ?
Domain Name	@ddns_host# ?

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 <TSProductNameLowerCase> and applications set up in your 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 – Click this checkbox to enable DDNS on your system.

DDNS Service – Sets the DDNS provider that our account is with. The options are DynDNS and TZO.

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

Password – 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.

ARRIS Contact Information

ARRIS offers broadband service providers a complete, integrated, application-oriented IP suite of back-office automation tools for network content, subscriber, and workforce management as well as advanced advertising and on demand services.

Before You Call ARRIS Support

When working with Technical Support, you can help us to expedite your call by following these guidelines:

- Please be prepared to give your Technical Support Contract ID number whenever you contact ARRIS Technical Support. If you do not know your Technical Support Contract ID number or have questions about a support contract, please contact ARRIS Technical Services at: services.orders@arris.com or **678 473-8302**.
- Be prepared to provide your name, company name, site location, serial number of the system you are calling about (if applicable), system and software version numbers, and as much detail about the problem as possible.
- Review available documentation, including release notes, product and installation manuals, and online help for information about your problem.
- Do not reboot or restart equipment or software processes prior to consulting with ARRIS Technical Support—vital data that could assist in resolving the problem can be lost when these actions are performed.
- All personnel who call Technical Support should have a high level of familiarity with the ARRIS system, including knowing the system passwords. We strongly recommend that you have personnel trained through ARRIS Educational Services programs.

ARRIS Technical Support supports ARRIS-supplied products only. Issues related to other hardware, software, or non-ARRIS networks must be addressed by your organization or the appropriate third-party vendor.

By Telephone

North America Region	
Legacy ARRIS	+1 888 221 9797 (North America)
	+1 678 473 5656 (Worldwide)
Legacy Motorola Home	+ 1 888 944 4357 (North America)
	+1 215 323 2345 (Worldwide)

Latin America Region:		
Argentina:	Legacy Motorola Home	0 800 666 3601
Aruba:	Legacy Motorola Home	215 323 2346
Bolivia:	Legacy Motorola Home	800 100 694
Brazil:	Legacy Motorola Home	0 800 891 5314
	Legacy ARRIS	+55 11 2737 7629
Chile:	Legacy Motorola Home	1230 020 5564
	Legacy ARRIS	+56 2 678 4500
Colombia:	Legacy Motorola Home	1 8005 1 80947
	Legacy ARRIS	+57 1 381 9103
Costa Rica:	Legacy Motorola Home	215 323 2346
Ecuador:	Legacy Motorola Home	215 323 2346
El Salvador:	Legacy Motorola Home	800 6625
Honduras:	Legacy Motorola Home	800 0123, then 866 842 0264
Mexico:	Legacy Motorola Home	001 866 391 2349
	Legacy ARRIS	01 800 522 7747 or +52 55 22828531
Panama:	Legacy Motorola Home	001 800 203 4345
Peru:	Legacy Motorola Home	0 800 5 3651
Puerto Rico:	Legacy Motorola Home	866 862 2627
Rep. Dominicana:	Legacy Motorola Home	1 888 751 8898
Venezuela:	Legacy Motorola Home	0 800 100 9161

Europe Region:		
Europe:	Legacy ARRIS	+31 20 311 2525
Belgium:	Legacy Motorola Home	0 800 72 163
Denmark:	Legacy Motorola Home	80 88 6748
Finland:	Legacy Motorola Home	0 800 114 263
France:	Legacy Motorola Home	0 800 90 7038
Germany:	Legacy Motorola Home	0 800 18 73019
Hungary:	Legacy Motorola Home	06 800 18164
Ireland:	Legacy Motorola Home	1 800 55 9871
Israel Golden Lines:	Legacy Motorola Home	1 809 25 2071
Israel Bezeq:	Legacy Motorola Home	1 809 42 9181
Israel Barak:	Legacy Motorola Home	1 809 31 5435
Italy:	Legacy Motorola Home	800 788 304
Luxembourg:	Legacy Motorola Home	0 800 2 5310
Netherlands - Holland:	Legacy Motorola Home	0 800 022 0176
Norway:	Legacy Motorola Home	800 15 670
Poland:	Legacy Motorola Home	00 800 111 3671
Portugal:	Legacy Motorola Home	800 81 3461
Spain:	Legacy Motorola Home	900 99 1771
Sweden:	Legacy Motorola Home	020 79 0241
Switzerland:	Legacy Motorola Home	0 800 561 872
United Kingdom:	Legacy Motorola Home	0 800 404 8439

Asia Region:		
Asia	Legacy ARRIS	+86 755 8634 9110
	Legacy Motorola Home	+1 847 725 4011 (Worldwide)

Japan Region:		
Japan:	Legacy ARRIS	+81 3 5461 7320
	Legacy Motorola Home	+1 847 725 4011 (Worldwide)

Korea Region:		
Korea:	Legacy ARRIS	+82 31 740 4203
	Legacy Motorola Home	+1 847 725 4011 (Worldwide)

China Region:		
China:	Legacy ARRIS	+86 755 8634 9110 or 4008810685 (in China only)
	Legacy Motorola Home	+1 847 725 4011 (Worldwide)

Australia / New Zealand Region:		
Australia / New Zealand	Legacy ARRIS	+86 755 8634 9110
	Legacy Motorola Home	61 3 81997220 or 1800 242664 (Australia only)

By Email

North America - Headend and Network Equipment:		
RF Optics:	Ruckus, Optics, Amps, Nodes, Transmitters, CHP, Passives, OptiMax, CoreWave, CoreView	RFOptics-support@arris.com
CMTS Products:	C3, C4, ICO, ASA, CxM, CMTS1000, CMTS1500, E6000	techsupport.na@arris.com
CMTS Product:	BSR, SRM4, HSIM4, TX32, RX48, SRM10G	tac.helpdesk@arris.com
Moxi and WHS Products:	Moxi, MCR, Portal, WHS, WHS5225, MediaPlayer, Whole Home Solution, Gateway	techsupport.na@arris.com
D5 and DVS Products:	D5, Application Manager, VIPr, Hemi, Encore, Quartet, Prelude, EGT or DVS	techsupport.na@arris.com
DVS Products:	CAS, DACs, CASMR, APEX3000, NC2000, DreamGallery, Secure Media, VideoFlow, AVP100, STBs, AS-RAC, QT Plus, CherryPicker, Encoder, Astria	tac.helpdesk@arris.com
EMP Products:	AdEdge, APS, BEQ6XXX, BME50, BMR1200, CVEx, MSP2XXX, RMS, SBSS, SVA, VMS	emp-support@arris.com
Digital Ad Insertion:	Ad Insertion, Skyvision, Spots, ACM, n5, XMS	ai-support@arris.com
Video on Demand:	Video OnDemand, VOD, nABLE, CMM, n5, XMS, Transit	vod-support@arris.com
VOD Products:	B1 Video Server, M3 Video Server, cDVR Video Solution	tac.helpdesk@arris.com
WorkAssure:	WorkAssure, I&R, SageQuest, Wireless Matrix, Tech Director, Tech Calendar, SSM Alarms	workassure-support@arris.com
Assurance Products:	ServAssure, OpsLogic, Powersense, SALIVE, EventAssure, HouseCheck, Data Warehouse, Starnodes	assurance-support@arris.com
GPON Product:	GPON, POL, Carrier Ethernet	tac.helpdesk@arris.com
Satellite and Modular Systems:	DSR, Uplink, IPTV, Encoder	tac.helpdesk@arris.com
Korea:	Legacy ARRIS Products	techsupport.korea@arris.com
Korea:	Legacy Motorola Home	tac.helpdesk@arris.com
Australia / New Zealand:	Legacy ARRIS Products	techsupport.asia@arris.com
Australia / New Zealand:	Legacy Motorola Home	support.anz@arris.com

Customer Premise Equipment:		
Touchstone Products:	TGxxx, TMxxx, Touchstone, TTM, Packet Ace, Cornerstone, HDT, Incognito, CableModem, eMTA, Telephone Gateway	techsupport.na@arris.com
CableModem:	Cable Modem, MTA	tac.helpdesk@arris.com

International (All Products):		
Latin America:	Legacy ARRIS Products	techsupport.cala@arris.com
Latin America:	Legacy Motorola Home	tac.helpdesk@arris.com
Europe:	Legacy ARRIS Products	techsupport.europe@arris.com
Europe:	Legacy Motorola Home	tac.helpdesk@arris.com
Asia:	Legacy ARRIS Products	techsupport.asia@arris.com
Asia:	Legacy Motorola Home	tac.helpdesk@arris.com
Japan:	Legacy ARRIS Products	techsupport.japan@arris.com
Japan:	Legacy Motorola Home	tac.helpdesk@arris.com

Ask ARRIS Customer Portal

The Ask ARRIS Customer Portal enables you to:

- Use innovative search technology to deliver fast, relevant, reliable information exactly when you need it, 24x7
- Manage technical support cases for your products, support level, and site location
- Access technical documentation and webcasts

To use the portal, you will need to register for the site using your support contract ID and email address. To access the customer portal:

http://www.arris.com/support

Global Knowledge Services and Training

For more information about Global Knowledge Services and the programs we offer, e-mail us at:

training@arris.com

ARRIS Enterprises, Inc.
3871 Lakefield Drive
Suwanee, GA 30024 USA

www.arris.com

365-095-27433 x.1 3/15