



**MOTOROLA**



---

## ***User Guide***

---

**SURFboard® SBG6400**

**Wireless Cable Modem Gateway**

**Firmware: D30GW-HARRIER-1.3.0.0-GA-01-NOSH**

© 2014 ARRIS Enterprises, Inc. All rights reserved.

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

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

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

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

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



# Safety and Regulatory Information

## IMPORTANT SAFETY INSTRUCTIONS

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

- Read all of the instructions listed here and/or in the user manual before you operate this device. Give particular attention to all safety precautions. Retain the instructions for future reference.
- This device must be installed and used in strict accordance with manufacturer's instructions, as described in the user documentation that is included with the device.
- Comply with all warning and caution statements in the instructions. Observe all warning and caution symbols that are affixed to this device.
- To prevent fire or shock hazard, do not expose this device to rain or moisture. The device must not be exposed to dripping or splashing. Do not place objects filled with liquids, such as vases, on the device.
- This device was qualified under test conditions that included the use of the supplied cables between system components. To ensure regulatory and safety compliance, use only the provided power and interface cables and install them properly.
- Different types of cord sets may be used for connections to the main POWER supply circuit. Use only a main line cord that complies with all applicable device safety requirements of the country of use.
- Installation of this device must be in accordance with national wiring codes and conform to local regulations.
- Operate this device only from the type of power source indicated on the device's marking label. If you are not sure of the type of power supplied to your home, consult your dealer or local power company.
- Do not overload outlets or extension cords, as this can result in a risk of fire or electric shock. Overloaded AC outlets, extension cords, frayed power cords, damaged or cracked wire insulation, and broken plugs are dangerous. They may result in a shock or fire hazard.
- Route power supply cords so that they are not likely to be walked on or pinched by items placed upon or against them. Pay particular attention to cords where they are attached to plugs and convenience receptacles, and examine the point where they exit from the device.
- Place this device in a location that is close enough to an electrical outlet to accommodate the length of the power cord.
- Place the device to allow for easy access when disconnecting the power cord of the device from the AC wall outlet.
- Do not connect the plug into an extension cord, receptacle, or other outlet unless the plug can be fully inserted with no part of the blades exposed.
- Place this device on a stable surface.
- Avoid damaging the device with static by touching the coaxial cable when it is attached to the earth-grounded coaxial cable-TV wall outlet.
- Always first touch the coaxial cable connector on the device when disconnecting or reconnecting the Ethernet cable from the device or user's PC.
- 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 104° F (40° C).

### SAVE THE ABOVE INSTRUCTIONS

**Note to CATV System Installer** — This reminder is provided to call the CATV system installer's attention to Articles 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.

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 RSS-210 of the Industry Canada Rules. 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)

## 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.

## AVIS D'INDUSTRIE CANADA (IC)

Cet appareil est conforme à la réglementation RSS-210 d'Industrie Canada. Son utilisation est assujettie aux deux conditions suivantes :

- Cet appareil ne doit pas causer d'interférences et
- Cet appareil doit accepter toute interférence reçue, y compris les interférences causant un fonctionnement non désiré.

## 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.

**SECURITY WARNING:** This device allows you to create a wireless network. Wireless network connections may be accessible by unauthorized users. For more information on how to protect your network, see the [Change the Default User Name and Password](#) for instructions or visit the ARRIS Support website: [www.arrisi.com/consumer](http://www.arrisi.com/consumer).

## CARING FOR THE ENVIRONMENT BY RECYCLING



When you see this symbol on a 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.

# Contents

<b>Safety and Regulatory Information</b> .....	<b>i</b>
<b>Getting Started</b> .....	<b>1</b>
In The Box .....	1
Additional Items You May Need (Not Included).....	2
System Requirements.....	2
Contact Information .....	2
<b>Product Overview</b> .....	<b>3</b>
Front Panel.....	3
Wi-Fi Protected Setup™ (WPS).....	4
Rear Panel.....	5
Gateway Label .....	6
<b>Installing the Gateway</b> .....	<b>7</b>
Connect the SBG6400 to Your Computer .....	7
Establish an Internet Connection.....	8
<b>Setting Up a Wireless Network Connection</b> .....	<b>9</b>
Launch the SBG6400 Quick Start Wizard .....	9
Set Up a Wireless Network Using Your Computer.....	14
Quick Connect Using the Windows Taskbar .....	14
Connect Using the Windows Control Panel.....	16
Use the SBG6400 WPS Pairing Button.....	18
Test Your Wireless Network Connection.....	18
<b>Managing Your Gateway and Connected Networks</b> .....	<b>19</b>
Start the Gateway Web Manager .....	19
Gateway Web Manager Menu Options.....	20
Get Help .....	22
Overview Help .....	22
Help Links .....	23
Field Level Help.....	23
View the Gateway Product Information .....	24
View the Gateway Status.....	24
Back Up Your Gateway Configuration.....	25
Restore Your Gateway Settings .....	26
Reset Your Gateway Settings.....	27
Exit the SBG6400 Web Manager.....	28
<b>Protecting &amp; Monitoring Your Wireless Network</b> .....	<b>29</b>
Prevent Unauthorized Access.....	29
Change the Default User Name and Password.....	29

Set Up Firewall Protection .....	31
Set Up Parental Controls .....	32
Set Up Port Triggers .....	34
Set Up Port Forwarding.....	35
Set Up the DMZ Host .....	37
Store Remote Firewall Logs.....	37
<b>Creating Wi-Fi Networks .....</b>	<b>39</b>
Set Up Your Wireless Primary Network.....	39
Enable or Disable WPS on Your Wireless Network .....	40
Set Up a Wireless Guest Network.....	41
Change Your Wireless Network Name (SSID) .....	43
Change the Wireless Channel.....	44
<b>Troubleshooting Tips .....</b>	<b>45</b>
Solutions .....	45
Front Panel LED Icons and Error Conditions.....	46
<b>Gateway Configuration Screen Definitions .....</b>	<b>47</b>
Basic Screens .....	47
Setup .....	47
DHCP .....	48
DDNS .....	50
Backup and Restore .....	51
Advanced Screens.....	52
Options .....	52
IP Filtering.....	54
MAC Filtering.....	55
Port Filtering.....	55
Port Triggers .....	56
Port Forwarding .....	57
DMZ Host.....	59
Firewall Screens.....	60
Protection Level .....	60
Parental Control .....	62
Local Log.....	64
Remote Log.....	65
<b>Warranty Information .....</b>	<b>67</b>



## Tables

Table 1: SBG6400 Package Contents .....	1
Table 2: SBG6400 Front Panel LED Icons .....	3
Table 3: SBG6400 Rear Panel Ports & Connectors.....	5
Table 4: SBG6400 Web Manager Main Menu Options .....	21
Table 5: Troubleshooting Solutions .....	45
Table 6: Front Panel LED Icons and Error Conditions .....	46
Table 7: Basic Setup Screen-Field Descriptions .....	48
Table 8: Basic DHCP Screen-Field Descriptions .....	49
Table 9: Basic DDNS Screen-Field Descriptions .....	50
Table 10: Basic Backup & Restore -Field Descriptions .....	51
Table 11: Advanced Options-Field Descriptions .....	53
Table 12: Advanced IP Filtering -Field Descriptions .....	54
Table 13: Advanced MAC Filtering -Field Descriptions .....	55
Table 14: Advanced Port Filtering -Field Descriptions.....	56
Table 15: Advanced Port Triggers -Field Descriptions .....	57
Table 16: Advanced Port Forwarding-Field Descriptions .....	59
Table 17: Advanced DMZ Host-Field Descriptions .....	59
Table 18: Firewall Protection Level -Field Descriptions.....	61
Table 19: Firewall Parental Control-Set Time Zone-Field Descriptions .....	62
Table 20: Firewall Parental Control -Field Descriptions.....	63
Table 21: Firewall Local Log -Field Descriptions .....	64
Table 22: Firewall Remote Log -Field Descriptions .....	66

## Figures

Figure 1 – SBG6400 Front View .....	3
Figure 2 – SBG6400 Rear View.....	5
Figure 3 – SBG6400 Connection Diagram .....	7
Figure 4 – SBG6400 Quick Start Wizard Opening Screen .....	10
Figure 5 – SBG6400 Quick Start Wizard Welcome Screen .....	10
Figure 6 – SBG6400 Quick Start Wizard-Step 2 of 6 Screen .....	11
Figure 7 – SBG6400 Quick Start Wizard-Step 3 of 6 Screen .....	12
Figure 8 – SBG6400 Quick Start Wizard-Step 4 of 6 Screen .....	12
Figure 9 – SBG6400 Quick Start Wizard-Step 5 of 6 Screen .....	13
Figure 10 – SBG6400 Quick Start Wizard-Step 6 of 6 Screen.....	13
Figure 11 – Sample Available Wireless Networks Window .....	14
Figure 12 – Windows Taskbar Icons .....	14

Figure 13 – Sample Available Wireless Networks Window .....	15
Figure 14 –Network Connection Window .....	15
Figure 15 –Network Connection-Create Network Password Window .....	16
Figure 16 – Control Panel-Network and Sharing Center Window .....	16
Figure 17 – Manually Connect to a Wireless Network Window .....	17
Figure 18 – Manually Connect to a Wireless Network Window .....	17
Figure 19 – SBG6400 Main Screen .....	20
Figure 20 – SBG6400 Web Manager Main Menu Buttons.....	20
Figure 21 – SBG6400 Web Manager Main Menu Links .....	21
Figure 22 – Help Overview Screen.....	22
Figure 23 – Help Links Screen.....	23
Figure 24 – SBG6400 Status – Product Information Screen.....	24
Figure 25 – SBG6400 Status Connection Screen .....	25
Figure 26 – SBG6400 Backup and Restore Screen .....	26
Figure 27 – Restore Factory Defaults Screen .....	27
Figure 28 – Change User Name Screen.....	30
Figure 29 – Change User Password Screen .....	30
Figure 30 – Firewall Protection Level Screen.....	31
Figure 31 – Parental Control-Change Time Zone Screen .....	32
Figure 32 – Firewall Parental Control Screen.....	33
Figure 33 – Advanced Port Triggers Screen.....	34
Figure 34 – Create Port Triggers Screen .....	34
Figure 35 – Advanced Port Forwarding Screen.....	35
Figure 36 – Commonly Used Forwarded Ports List.....	36
Figure 37 – Advanced DMZ Host Screen.....	37
Figure 38 – Firewall Remote Log Screen .....	38
Figure 39 – Wireless Primary Network Settings Screen.....	39
Figure 40 – WPS Setup Screen.....	40
Figure 41 – Wireless Guest Network Screens .....	41
Figure 42 – Change Your Network Name (SSID) and Password Screens .....	43
Figure 43 – Wireless 802.11 Radio Screens.....	44
Figure 44 – Basic Setup Screen .....	47
Figure 45 – Basic DHCP Screen .....	49
Figure 46 – Basic DDNS Screen .....	50
Figure 47 – Basic Backup & Restore Screen.....	51
Figure 48 – Advanced Options Screen.....	52
Figure 49 – Advanced IP Filtering Screen .....	54
Figure 50 – Advanced MAC Filtering Screen .....	55
Figure 51 – Advanced Port Filtering Screen.....	56
Figure 52 – Advanced Create Port Triggers Screen .....	56

Figure 53 – Advanced Port Triggers Screen .....57

Figure 54 – Commonly Used Port Forwarding Port Numbers List .....58

Figure 55 – Advanced Port Forwarding Screen .....58

Figure 56 – Advanced DMZ Host Screen .....59

Figure 57 – Firewall Protection Level Screen .....61

Figure 58 – Firewall Parental Control-Set Time Zone Screen .....62

Figure 59 – Firewall Parental Control Screen .....63

Figure 60 – Firewall Local Log Screen .....64

Figure 61 – Firewall Remote Log Screen .....65

# 1

## Getting Started





The ARRIS SURFboard® SBG6400 Wireless Cable Modem Gateway is an all in one wireless DOCSIS 3.0® cable modem and two-port Ethernet router device. It provides secure ultra high-speed wired and wireless broadband connections for your computer and other wireless network devices on your home or small business network. The SBG6400 also includes a Wi-Fi® Pairing button option for quick and easy connections for your wireless devices.


This guide provides instructions for installing and configuring the SBG6400, setting up secure wireless network connections, and managing your gateway and network configurations.

### In The Box

Before installing the SBG6400, check that the following items are also included in the box. If any items are missing, please contact your service provider for assistance or call ARRIS Technical Support at **1-877-466-8646**.

**Table 1: SBG6400 Package Contents**

Item	Description
<b>SBG6400 Wireless Cable Modem Gateway</b> 	High-speed DOCSIS 3.0 cable modem, wireless access point, and 2-port Ethernet router
<b>Power Supply</b> 	Power adapter and cord for an electrical wall outlet connection
<b>Ethernet Cable</b> 	Standard Category 5 (CAT5) or higher network cable
<b>Software License &amp; Regulatory Card</b> 	Safety and regulatory information, software license, and warranty for the gateway

Item	Description
<b>SBG6400 Quick Start Guide</b>	 Provides basic information for installing the gateway and setting up a secure wireless connection on your home network.

## Additional Items You May Need (Not Included)

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

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

## System Requirements

- High-speed Internet access account
- Web browser access – Internet Explorer, Google Chrome, Firefox, or Safari
- Compatible operating systems:
  - o Windows® 8
  - o Windows 7 Service Pack 1 (SP1)
  - o Windows Vista™ SP2 or later
  - o Windows XP SP3

**Note:** Microsoft no longer supports Windows XP. The SBG6400 should still function without any problems.

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

## Contact Information

For technical support and additional ARRIS product information:

- Visit the ARRIS Support website: [www.arrisi.com/consumer](http://www.arrisi.com/consumer)
- Call ARRIS Technical Support: **1-877-466-8646**

# 2




## Product Overview




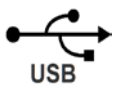
### Front Panel



Figure 1 – SBG6400 Front View

Table 2: SBG6400 Front Panel LED Icons

LED Icon	Blinking	On (Solid)
 <b>WPS Button</b>	Not applicable – no LED on button  <i><b>Note:</b> The <b>Wireless</b> LED will blink <b>Amber</b> to indicate the WPS pairing process is in progress.</i>	Not applicable – no LED on button
 <b>POWER</b>	Not applicable – icon does not blink	<b>Green:</b> Power is properly connected
 <b>RECEIVE</b>	Scanning for a downstream (receive) channel connection	<b>Green:</b> Non-bonded downstream channel is connected  <b>Blue*:</b> High-speed Internet connection with bonded downstream channels

LED Icon	Blinking	On (Solid)
 SEND	Scanning for an upstream (send) channel connection	<b>Green:</b> Non-bonded upstream channel is connected <b>Blue*:</b> High-speed Internet connection with bonded upstream channels
 ONLINE	Scanning for an Internet connection	<b>Green:</b> Startup process completed
 WIRELESS	<b>Green:</b> Wi-Fi enabled with encrypted wireless data activity. <b>Amber:</b> WPS Pairing process is underway between the SBG6400 and a WPS-enabled wireless device.	<b>Green:</b> Any of the following applies: <ul style="list-style-type: none"> <li>• <b>2.4 GHz</b> wireless connection is made between the SBG6400 and another Wi-Fi enabled device on your home network; for example, Wi-Fi telephone, tablet, or laptop.</li> <li>• The WPS Pairing process between the SBG6400 and WPS-enabled wireless device was successful.</li> <li>• The WPS Pairing process either failed or did not complete after two minutes.</li> </ul>
 USB	<b>Green:</b> Data activity in progress.	<b>Green:</b> USB connection is made between the SBG6400 and a computer.

\*Indicates DOCSIS 3.0 operation (high-speed Internet access) which may not be available in all locations. Check with your service provider for availability in your area.

## Wi-Fi Protected Setup™ (WPS)

Wi-Fi Protected Setup (WPS) is a wireless network setup option that provides a quick and easy solution for setting up a secure wireless network connection for any WPS-enabled device; such as a computer, tablet, gaming device, or printer. WPS automatically configures your wireless network connections and sets up wireless security. See [Use the SBG6400 WPS Pairing Button](#) for more information.

## Rear Panel

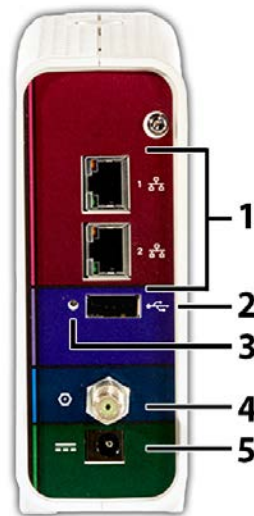






Figure 2 – SBG6400 Rear View

Table 3: SBG6400 Rear Panel Ports & Connectors

Port Name	Description
1  ETHERNET	Two one-gigabit Ethernet ports for RJ-45 cable connections: <ul style="list-style-type: none"> <li>• <b>Green</b> - LED is ON - Indicates a device connection is detected</li> <li>• <b>Green</b> - LED is Blinking - Indicates data traffic is in progress</li> <li>• <b>Amber</b> - LED is ON – Indicates 10/100 Base-T connection(s)</li> <li>• <b>Amber</b> - LED is OFF – Indicates GigE connection(s)</li> </ul>
2  USB	USB 2.0 port connection to your computer
3 <b>Reset button</b>	Can be used to reboot the gateway or reset the gateway settings. <ul style="list-style-type: none"> <li>• To reboot (or restart) the gateway, press the indented Reset button once using the end of a paper clip or other small object with a narrow tip, and then release.</li> <li>• To reset the gateway configuration back to the factory default settings, press and hold the indented Reset button for 15 seconds using the end of a paper clip or other small object with a narrow tip, and then release. See <a href="#">Reset Your Gateway Settings</a> for more information on an alternative method to reset the gateway settings using the SBG6400 Web Manager.</li> </ul> <p><b>WARNING!</b> Resetting to factory defaults also deletes any custom gateway configurations, including your user passwords and other security settings. You should back up the gateway configuration files before resetting the gateway. See <a href="#">Back Up Your Gateway Configuration</a> for more information.</p>



Port Name	Description
3  CABLE	Coaxial cable connector
4  POWER	100 - 240VAC Power connector  <b>WARNING!</b> To avoid any damage to your SBG6400 Gateway, only use the power adapter and cord provided in the box.

## Gateway Label

The gateway label is located on the bottom of the SBG6400. It contains specific gateway ID information that you may need when contacting your service provider or ARRIS Technical Support.

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

- o Gateway model name (**SBG6400**)
- o Gateway MAC address (**HFC MAC ID**)
- o Gateway serial number (**S/N**)

# 3

## Installing the Gateway



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

### Connect the SBG6400 to Your Computer

Before installing the SBG6400:

- Check with your service provider to ensure broadband cable service is available in your area. To set up a wireless network, you will need a high-speed Internet connection provided by an Internet service provider.

**Note:** When contacting your service provider, you may need your gateway information listed on the gateway label located on the bottom of your SBG6400 (see [Gateway Label](#)).

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

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

**Note:** The following installation procedure covers the wired Ethernet connection process so that you can confirm that the SBG6400 was properly installed and can connect to the Internet.

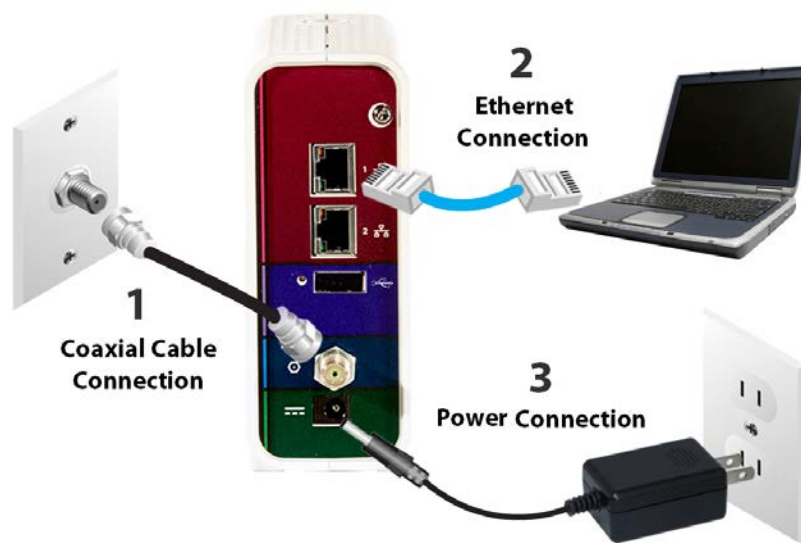


Figure 3 – SBG6400 Connection Diagram

1. Check that a coaxial cable is already connected to a cable wall outlet or RF splitter (optional).
2. Connect the other end of the coaxial cable to the Cable connector on the SBG6400.  
Use your hand to tighten the connectors to avoid damaging them.
3. Connect the Ethernet cable to an available Ethernet port on the SBG6400.
4. Connect the other end of the Ethernet cable to the Ethernet port on your computer.  
**Optional:** Repeat steps 3 and 4 for an additional computer or other network device that you want to install as a wired connection on your home network.
5. Connect the power cord to the Power port on the SBG6400.
6. Plug the other end of the power cord into an electrical wall outlet.  
**Note:** This automatically powers ON the SBG6400.

## Establish an Internet Connection

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

1. Power ON the computer connected to the SBG6400 if it is turned off, and then log in.
2. Contact your service provider to activate (provision) the SBG6400. You may have to provide the **HFC MAC ID** listed on the [gateway label](#).  
**Note:** Your service provider may allow for automatic activation which will automatically launch its own special website when you open a web browser.
3. After the SBG6400 is activated, open a web browser (Internet Explorer, Google Chrome, Firefox, or Safari) on your computer.  
If the special website did not open, continue with step 4. If it did open, proceed to step 5.
4. Type a valid URL ([www.arrisi.com](http://www.arrisi.com)) in the address bar and then click or press **Enter**.  
The ARRIS website should open. If it did not open, please contact your service provider for assistance.
5. Check that the **Power**, **Receive**, **Send**, and **Online** front panel LEDs on the SBG6400 light up in sequential order. See [Front Panel](#) for additional LED status information.
  - o If all four LEDs did not light up solid and you also do not have an Internet connection, you may have to contact your service provider to reactivate the SBG6400 or check for signal issues.
  - o If you still cannot connect to the Internet, your SBG6400 may be defective. Please contact ARRIS Technical Support at **1-877-466-8646** for assistance.

## 4

## Setting Up a Wireless Network Connection

It is highly recommended that you first verify that your computer can connect to the Internet using an Ethernet connection before configuring your wireless network.

You must already have access to an Internet service in your home before setting up a wireless network connection. Also, make sure your computer and the SBG6400 are connected through an Ethernet connection.

Choose **one** of the following options to set up your wireless network connection:

- [Launch the SBG6400 Quick Start Wizard](#)
- [Set Up a Wireless Network Using Your Computer](#)
- [Use the SBG6400 WPS Pairing Button](#)

After setting up your wireless network connection, check that your wireless network connection was set up properly. See [Test Your Wireless Network Connection](#) for more information.

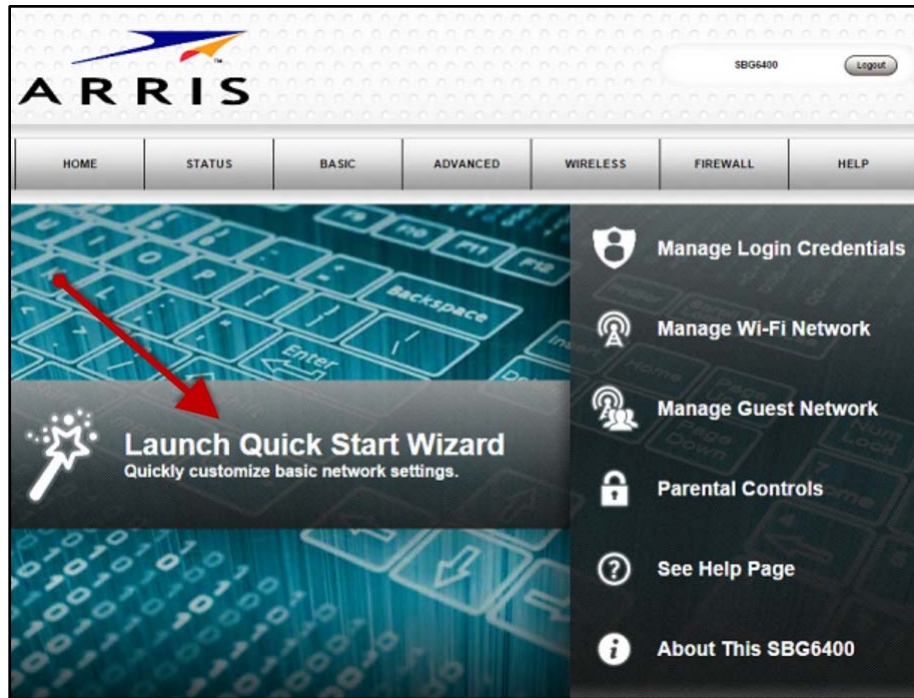
### Launch the SBG6400 Quick Start Wizard

The SBG6400 Quick Start Wizard is a six-step application to help you quickly configure the default wireless network settings on your SBG6400. It configures your wireless network name (SSID), Wi-Fi Security key (network password), and Wi-Fi Security code.

**IMPORTANT NOTE:** The quick start wizard uses the default settings already configured for your SBG6400 to help you quickly set up your wireless home network. However, the wizard will only let you change the wireless network name (SSID) and Wi-Fi Security key (network password). After completing the wizard and getting your SBG6400 connected to the Internet, you will be able to make additional network configuration changes to further customize your wireless home network and connect your wireless devices. See [Creating Wi-Fi Networks](#) for more information.

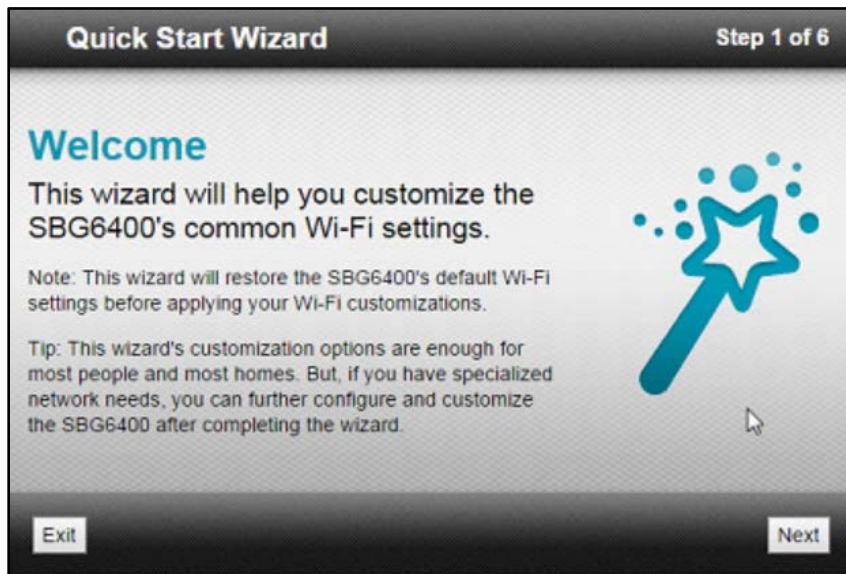
1. Open a web browser (Internet Explorer, Google Chrome, Firefox, or Safari) on the computer connected to the SBG6400.
2. Type the default LAN IP address, **http://192.168.0.1**, in the Address bar and then press **Enter**. The gateway Login screen displays.
3. Type the default username and password. Both entries are case-sensitive.  
Username: **admin**  
Password: **password**
4. Click **Login** to open the SBG6400 Web Manager. The Launch Quick Start Wizard screen displays (see Figure 4).  
**Note:** If the default user name and password are not working, your service provider may have to set up alternate login credentials. Please contact your service provider or ARRIS Technical Support for assistance.

5. Click **Launch Quick Start Wizard** to start the wizard. The Welcome screen displays (see Figure 5).



**Figure 4 – SBG6400 Quick Start Wizard Opening Screen**

**Note:** The ARRIS logo shown here and on other screenshots throughout this user guide represents the company logo for the manufacturer of the SURFboard SBG6400 Wireless Cable Modem Gateway.



**Figure 5 – SBG6400 Quick Start Wizard Welcome Screen**

- Click **Next** to open the Wi-Fi Network Name & Passphrase screen.



**Figure 6 – SBG6400 Quick Start Wizard-Step 2 of 6 Screen**

- Do one of the following to set up your wireless network name in the **Network Name (SSID)** field:
  - Keep the default network name or SSID (listed on the SBG6400 Gateway label).
  - Enter a name of your choice for your wireless network. Your new network name must contain from one to 32 alphanumeric characters.

**Note:** You have the option to customize your wireless network name (SSID) after completing the initial wireless network connection. However, you must use the default SSID listed on the gateway label for the initial gateway installation. See [Change Your Wireless Network Name \(SSID\)](#) for more information.

- Do one of the following to set up your wireless network password in the **Passphrase / Wi-Fi Security Key** field:

- Keep the default passphrase or Wi-Fi Security key (listed on the SBG6400 Gateway label).
- Enter a password of your choice for your wireless network password.

The passphrase or Wi-Fi Security key is the sign-on access code for your wireless network. The access code must contain from eight to 64 characters consisting of any combination of letters, numbers, and symbols. It should be as unique as possible to protect your wireless network and deter hackers or unauthorized access to your wireless network.

**Note:** We highly recommend that you change the default Wi-Fi Security Key to a more secure wireless password to protect your wireless network from unauthorized access. See [Prevent Unauthorized Access](#) for more information.

- Click **Next** to open the Wi-Fi Security Configuration screen (see Figure 7).

The wizard configures **WPA2-PSK** as the default wireless security code. It is the highest wireless network security level. See [Set Up Your Wireless Primary Network](#) to change the wireless security code for your wireless home network.





**Figure 7 – SBG6400 Quick Start Wizard-Step 3 of 6 Screen**

10. Click **Next** to open the User Security Configuration screen.



**Figure 8 – SBG6400 Quick Start Wizard-Step 4 of 6 Screen**

- o This screen allows you to change the current (or default) login user name and password for accessing the SBG6400 Web Manager.

**Note:** You must select each checkbox to activate the field to enter your new username and password. Otherwise, the fields are disabled. The **Next** button is disabled, if the username or password was not entered correctly. Make sure to repeat the same username and password in their respective fields.

- o Select the Change Username checkbox and then enter your new user name in both fields.
- o Select the Change Password checkbox and then enter your new password in both fields.

11. Click **Next** to open the Review Settings screen and confirm your wireless network settings.



Figure 9 – SBG6400 Quick Start Wizard-Step 5 of 6 Screen

12. Click **Apply** to accept the wireless network settings and open the Settings Applied screen or click **Previous** to go back and change your wireless network name and/or password.

Wait for your wireless network settings to be saved. When it is complete, the Settings Applied screen will open.

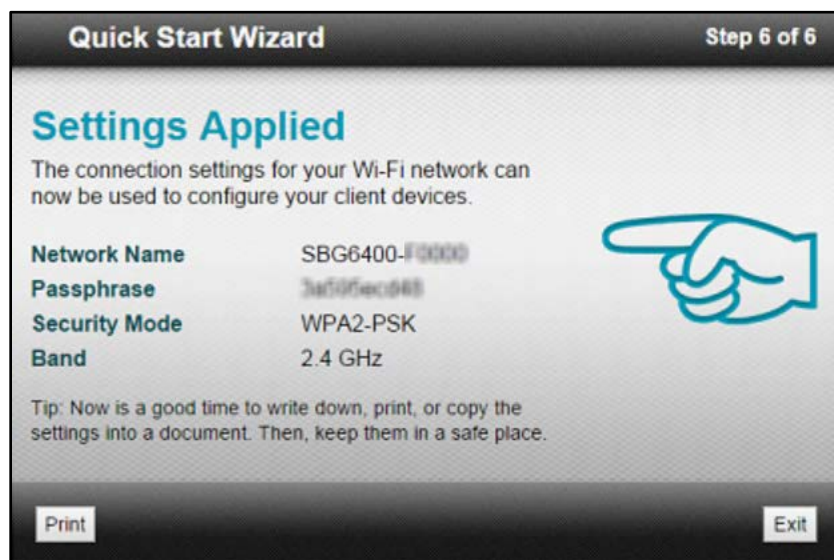


Figure 10 – SBG6400 Quick Start Wizard-Step 6 of 6 Screen

13. Click **Exit** on the Settings Applied screen.

**Note:** You can click **Print** for a printout of your wireless network settings for later use for logging onto your wireless network or changing your wireless network settings.



## Set Up a Wireless Network Using Your Computer

Use one of the following options to create your wireless network:

- [Quick Connect Using the Windows Taskbar](#)
- [Connect Using the Windows Control Panel](#)

**Note:** The steps for setting up a wireless network may differ slightly depending on the Windows operating system running on your computer. The steps used here apply to Windows 7.

### Quick Connect Using the Windows Taskbar

1. From the Windows taskbar, click the **Wireless Link** icon to open the list of available wireless networks.

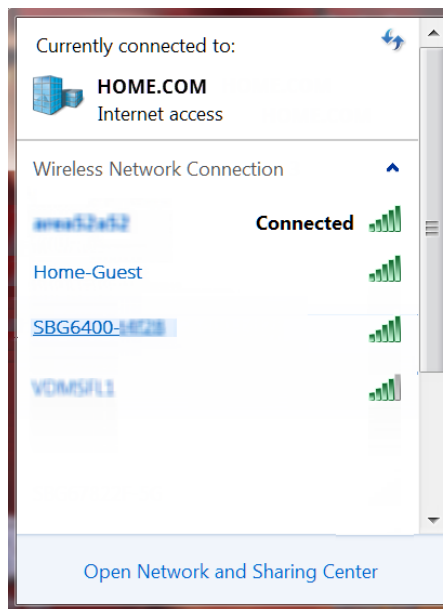


Figure 11 – Sample Available Wireless Networks Window

**Note:** If the icon is not visible, click the **Show hidden icons** button shown below.



Figure 12 – Windows Taskbar Icons

2. Locate and then left-click on the SBG6400 wireless network name or SSID (for example, **SBG6400-#####**) for your SBG6400 from the wireless networks list (see Figure 12).

The default SSID is located on the gateway label on the bottom of your SBG6400.

**Note:** You have the option to customize your wireless network name or SSID after completing your initial wireless network connection. However, you must use the default SSID listed on the gateway label for the initial gateway installation. See [Change Your Wireless Network Name \(SSID\)](#) for more information.



**Figure 13 – Sample Available Wireless Networks Window**

3. Select **Connect automatically** to set up your wireless devices for automatic connections to your home network upon log on.
4. Click **Connect** to open the Connect to a Network window.



**Figure 14 –Network Connection Window**

5. Enter a wireless network security code or passphrase for your wireless network password in the **Security key** field.  
You can use the **Wi-Fi Security Key** code listed on the SBG6400 gateway label or create your own personal password.  
**Note:** Remember to use a unique combination of letters, numbers, and characters to create a more secure password. See [Prevent Unauthorized Access](#) for more information.

6. Select **Hide characters** and then click **OK** to encrypt (or hide) your network Security key (or network password).

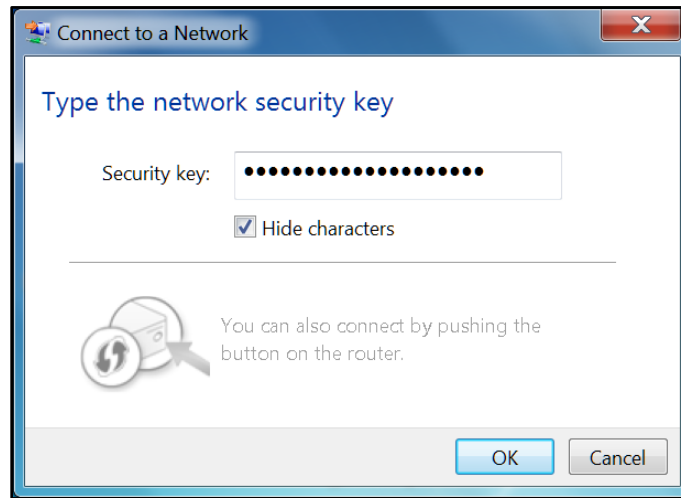


Figure 15 –Network Connection-Create Network Password Window

## Connect Using the Windows Control Panel

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

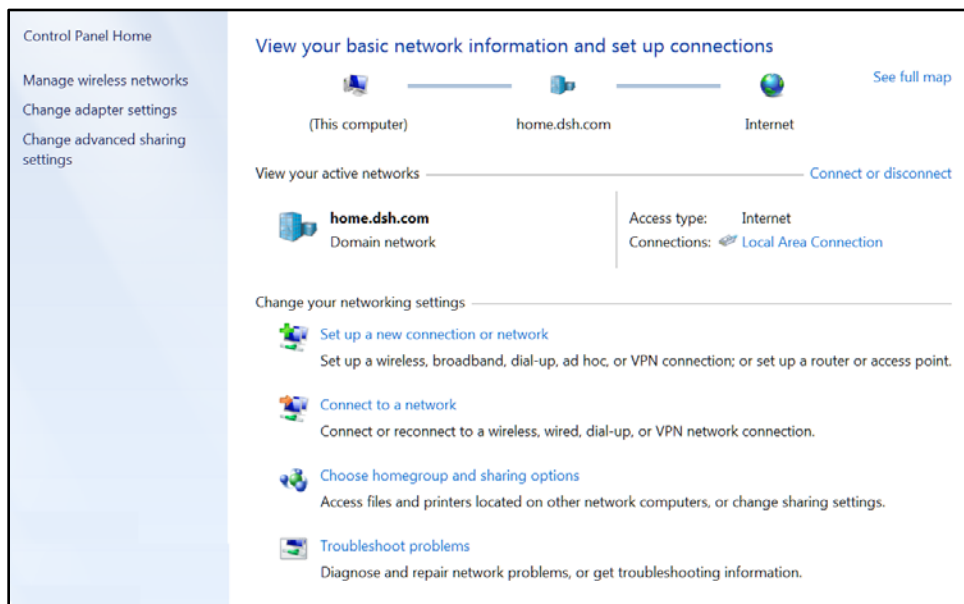
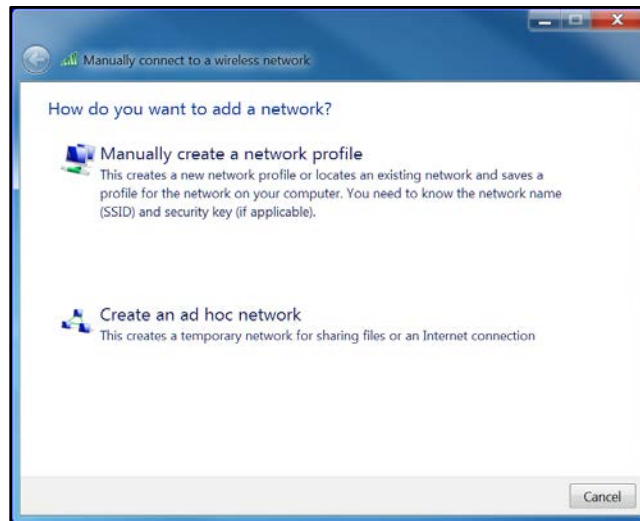


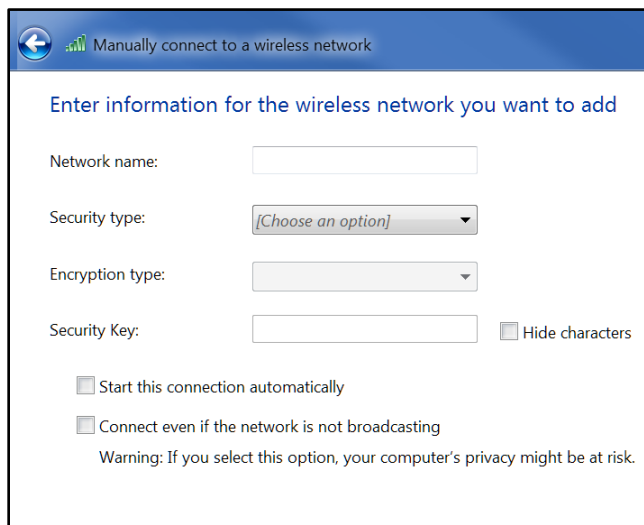
Figure 16 – Control Panel-Network and Sharing Center Window

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



**Figure 17 – Manually Connect to a Wireless Network Window**

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



**Figure 18 – Manually Connect to a Wireless Network Window**

6. Enter the ARRIS wireless network name or SSID (**SBG6400-#####**) for your SBG6400 in the **Network name** field.

The SSID name is located on the gateway label on the bottom of your SBG6400.

**Note:** You have the option to customize your wireless network name or SSID after completing your initial wireless network connection. However, you must use the default SSID listed on the gateway label for the initial gateway installation. See [Change Your Wireless Network Name \(SSID\)](#) for more information.

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

**Note:** Select **WPA2-Personal** which is the highest security level. This is also the default security level for the SBG6400.

8. Select the password encryption type from the **Encryption type** drop-down list. This is used for securing your wireless network.
  - o **TKIP** – Temporal Key Integrity Protocol
  - o **AES** – Advanced Encryption Standard (recommended). AES is the default encryption type for the SBG6400.
9. Enter a Security code or passphrase for your wireless network password in the **Security Key** field. You can use the **WI-FI SECURITY KEY** listed on the SBG6400 gateway label or create your own personal password.

**Note:** Remember to use a unique combination of letters, numbers, and characters to create a more secure password. See [Prevent Unauthorized Access](#) for more information.
10. Select **Hide characters** to prevent your Security Key or password from displaying in the field.
11. Select **Start this connection automatically** so that your wireless devices will automatically connect to your wireless network upon login.
12. Click **Next** to complete the wireless network setup.

The **Successfully added <Network name>** message for your new wireless network should appear.
13. Click **Close** to exit.

## Use the SBG6400 WPS Pairing Button

Use the WPS Pairing Button option to connect your WPS-enabled devices. The WPS Pairing button automatically assigns a random wireless network name (**SSID**) and Wi-Fi Security Key to the SBG6400 and other WPS-enabled devices to connect to your wireless home network.

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

1. Power ON your gateway and other WPS-enabled devices that you want to connect to your wireless network.
2. Press and hold the **WPS** button located on the top of the SBG6400 for five to 10 seconds and then release (see [Front Panel](#) for the SBG6400 front view).
3. If applicable, press the **WPS** button on your WPS-enabled computer or other WPS device.
4. Repeat step 3 for each additional WPS-enabled device that you want to connect to your wireless network.

## Test Your Wireless Network Connection

Perform the following connectivity test to check that the SBG6400 and other wireless devices are connected to your wireless home network:

1. If the wireless devices connected to the wireless network, disconnect the Ethernet cable from your computer and the SBG6400.
2. Open a web browser on your computer.
3. Type a valid URL ([www.arrisi.com](http://www.arrisi.com)) in the address bar, and then click or press **Enter**.

If the website did not open, please contact your service provider or call ARRIS Technical Support at **1-877-466-8646** for assistance.

## 5

## Managing Your Gateway and Connected Networks

Use the SBG6400 Web Manager to view and monitor the configuration settings and operational status of your gateway. You can also configure your network connections and wireless security settings. See [Protecting & Monitoring Your Wireless Network](#) for more information.

**Note:** If you did not purchase your gateway from a retail store, you may notice a few blocked configuration settings in the SBG6400 Web Manager that cannot be modified. This may be due to some restrictions set up by your service provider to prevent unauthorized changes to certain configuration parameters.

### Start the Gateway Web Manager

**Note:** You must use the default user name and password (listed below) to log in to the SBG6400 Web Manager for the first time. For network security purposes, we highly recommend that you should change the gateway default user name and password after logging onto the SBG6400 for the first time. See [Change the Default User Name and Password](#) for more information.

1. Open any web browser on the computer connected to the SBG6400.
2. In the Address bar, type **192.168.0.1** for the Gateway Web Manager IP address, and then press **Enter**. The gateway Login screen displays.
3. Type the default user name and password. Both entries are case-sensitive.
  - o Username: **admin**
  - o Password: **password**
4. Click **Login** to open the SBG6400 Web Manager. The SBG6400 Main Screen displays (see Figure 19).

**Note:** If the default user name and password are not working, your service provider may have to set up alternate login credentials. Please contact your service provider or ARRIS Technical Support for assistance.

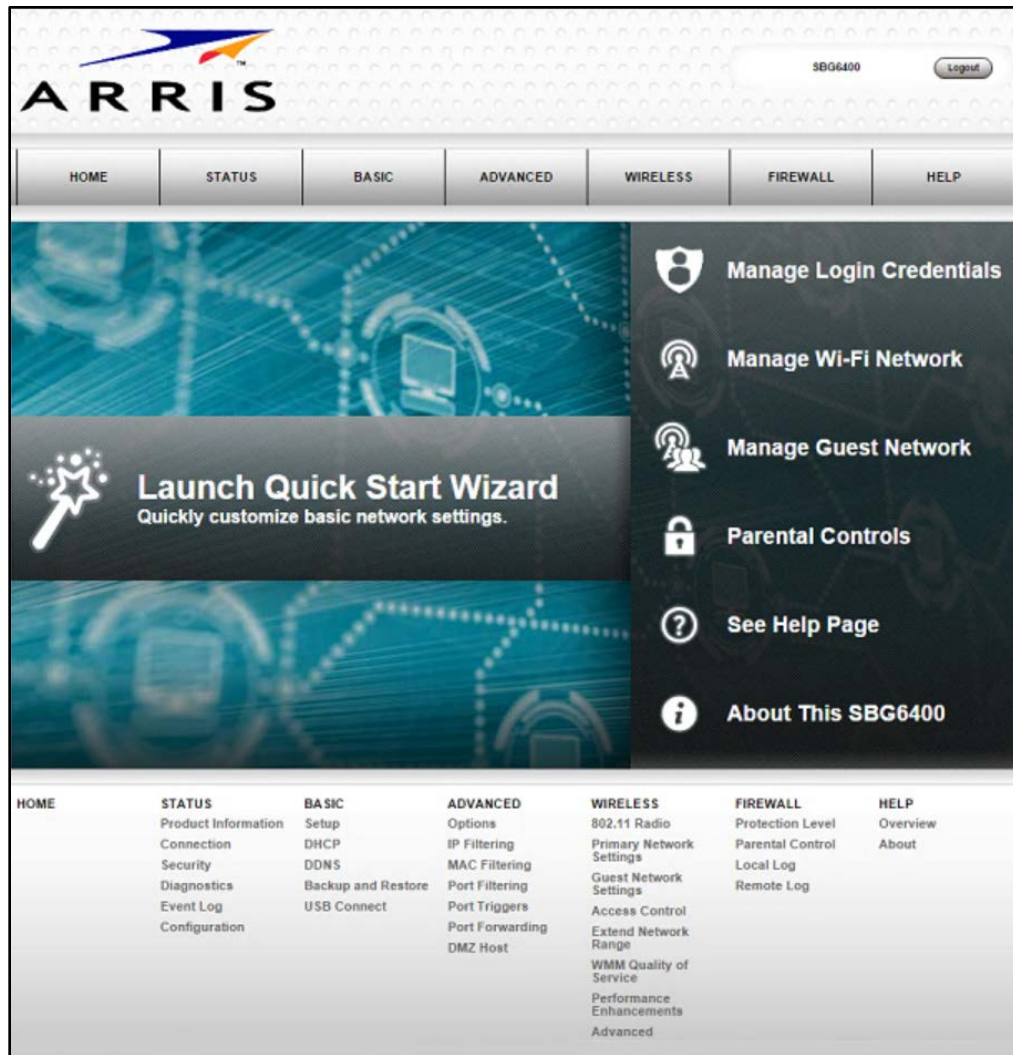


Figure 19 – SBG6400 Main Screen

## Gateway Web Manager Menu Options

### Main Menu Buttons

The SBG6400 main menu buttons are displayed along the top of the SBG6400 Web Manager screen. To display the drop-down submenu options, click the menu button.



Figure 20 – SBG6400 Web Manager Main Menu Buttons



## Main Menu Links

The SBG6400 main menu and related submenu option links are also displayed along the bottom of the SBG6400 Web Manager screen. To open a submenu option, click the link.

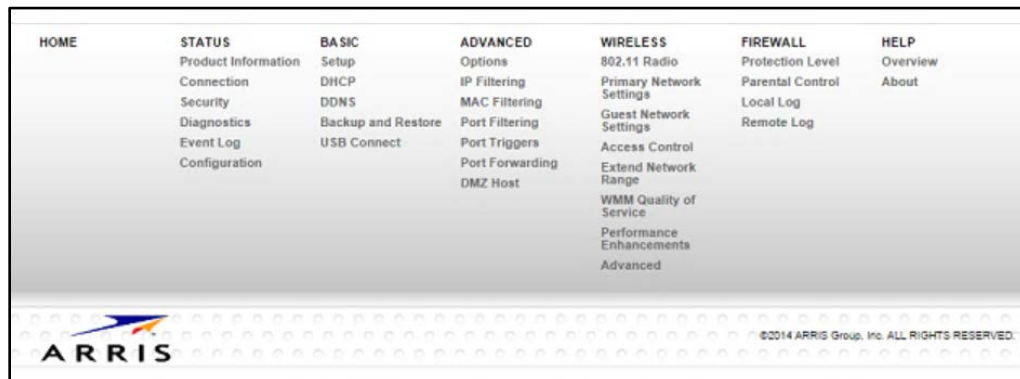


Figure 21 – SBG6400 Web Manager Main Menu Links

Table 4: SBG6400 Web Manager Main Menu Options

Menu Option	Function
<b>Home</b>	Displays the Quick Start Wizard main screen.
<b>Status</b>	Provides information about the gateway hardware and software, MAC address, gateway IP address, serial number, and related information. Additional screens provide diagnostic tools and also allow you to change your gateway user name and password.
<b>Basic</b>	Configures the gateway IP-related configuration data, including Network Configuration, WAN Connection Type, DHCPv6, and DDNS
<b>Advanced</b>	Controls Internet protocols which configure and monitor how the gateway routes IP traffic on the SBG6400.
<b>Wireless</b>	Configures and monitors the gateway wireless networking features.
<b>Firewall</b>	Configures and monitors the gateway firewall.
<b>Help</b>	Provides general information to help you set up your home network.
<b>Logout</b>	Closes the SBG6400 Web Manager.



## Get Help

You can choose any of the following three options to obtain help information for any SBG6400 Web Manager function. General help information is available for any SBG6400 menu option when you click the **Help** button on that page.

- [Overview Help](#)
- [Help Links](#)
- [Field Level Help](#)

## Overview Help

General help information is available when you click **Help, Overview** on the SBG6400 Main Menu.

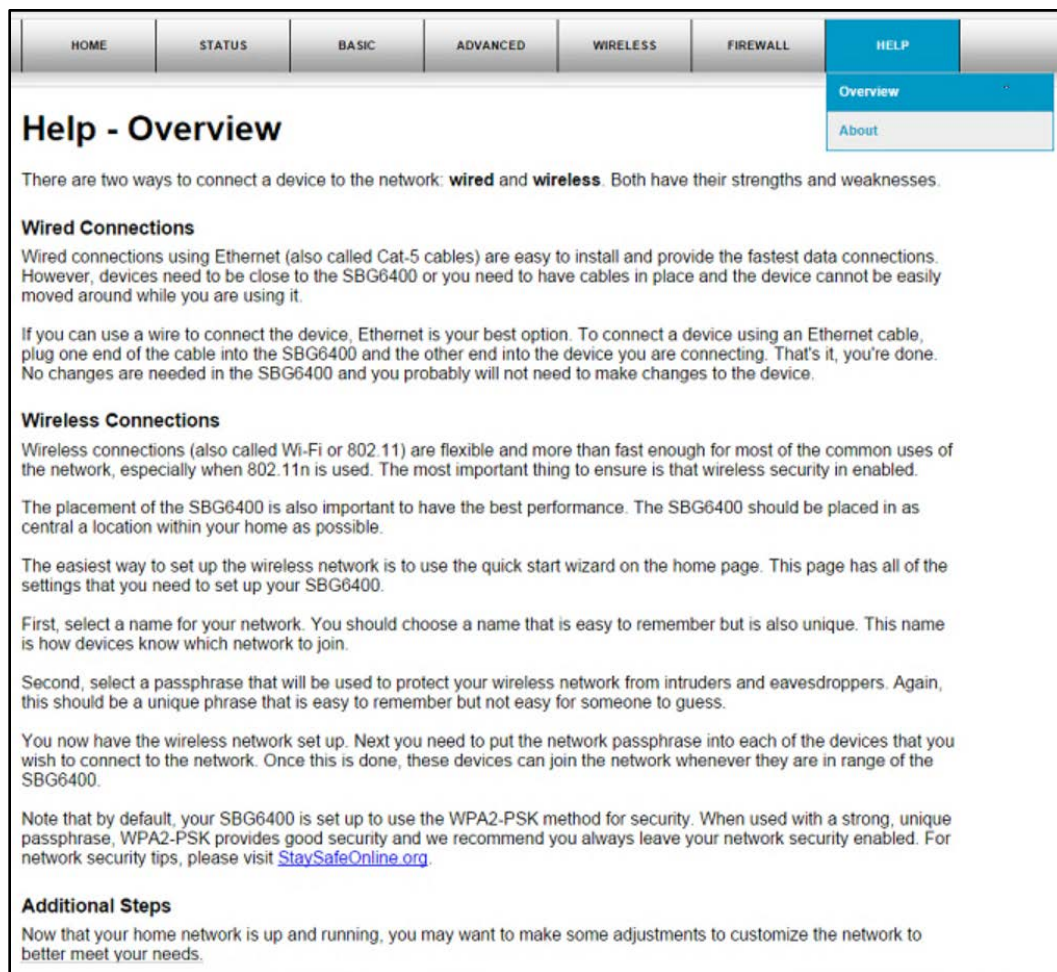


Figure 22 – Help Overview Screen

## Help Links

Provides a concise list of your gateway configuration settings with applicable links for easy access when you click **Help, About** on the SBG6400 Main Menu. The link opens the related configuration screen.

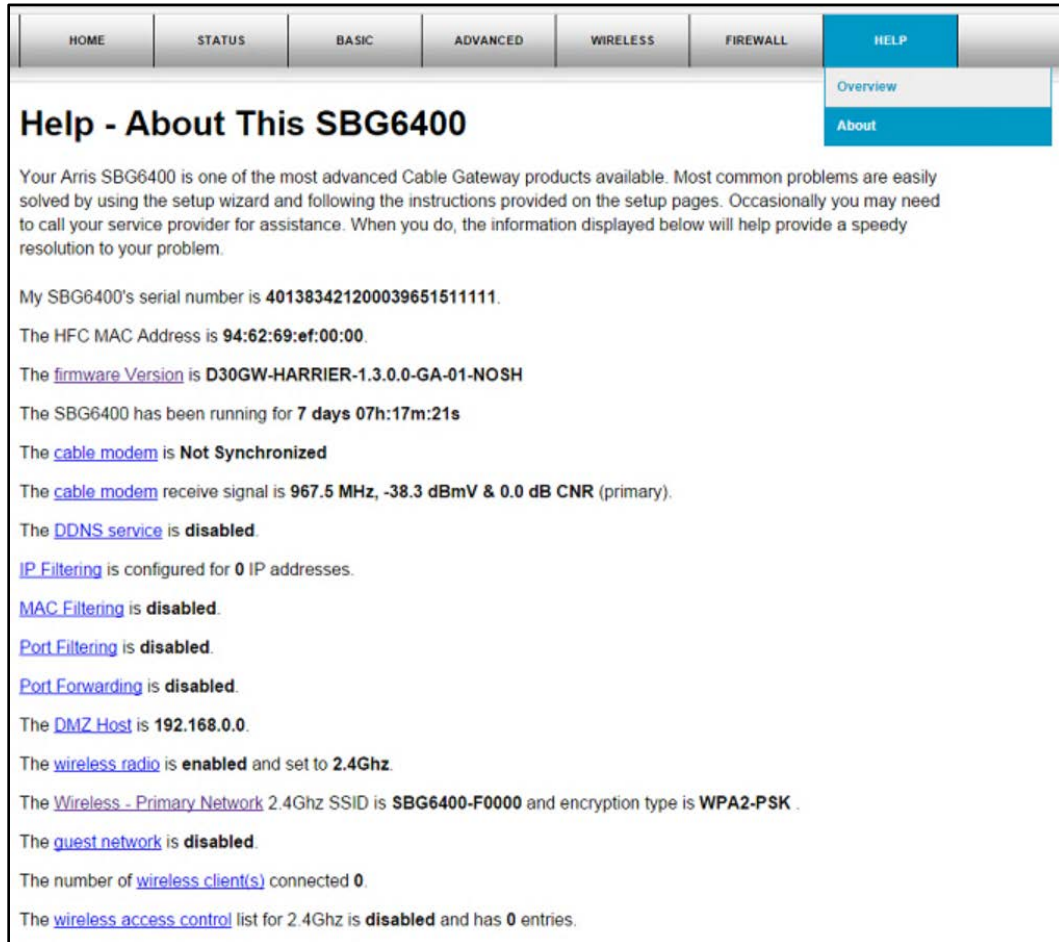


Figure 23 – Help Links Screen

## Field Level Help

More specific help information is available throughout the web manager for field level help when you click the **Help** link located to the right of the applicable field.



## View the Gateway Product Information

The Status Product Information screen displays general product information, including the firmware version and the current network connection status of the gateway.

To open the Status Product Information page:

1. Click **Status** on the SBG6400 Main Menu.
2. Click **Product Information** from the Status submenu options.
3. Click the **Refresh** button (**F5**) in your web browser to reload the information on the screen.

Information	
Standard Specification Compliant	DOCSIS 3.0
Hardware Version	1
Software Version	D30GW-HARRIER-1.3.0.0-GA-01-NOSH
Cable Modem MAC Address	94:62:69:ef:00:00
Serial Number	401383421200039651511111
Status	
Up Time	7 days 07h:29m:08s
Cable Modem IP Address	xxx.xxx.xxx.xxx

Figure 24 – SBG6400 Status – Product Information Screen

## View the Gateway Status

The Status Connection screen displays information about the RF upstream and downstream channels, including downstream channel frequency, upstream channel ID, and upstream and downstream signal power and modulation.

This screen also displays IP lease information including the current IP address of the cable modem, the duration of both leases, the expiration time of both leases, and the current system time from the DOCSIS time server.

To open the Status Connection screen:

1. Click **Status** on the SBG6400 Main Menu.
2. Click **Connection** from the Status submenu options.

Startup Procedure								
Procedure	Status	Comment						
Acquire Downstream Channel		Locked						
Connectivity State	OK	Operational						
Boot State	OK	Operational						
Configuration File	OK							
Security	Enabled	BPI+						

Downstream Bonded Channels								
Channel	Lock Status	Modulation	Channel ID	Frequency	Power	SNR	Corrected	Uncorrectables
1	Locked	QAM256	1	705000000 Hz	0.1 dBmV	46.4 dB	0	0
2	Locked	QAM256	2	711000000 Hz	0.2 dBmV	46.4 dB	0	0
3	Locked	QAM256	3	717000000 Hz	0.3 dBmV	46.9 dB	0	0
4	Locked	QAM256	4	723000000 Hz	0.3 dBmV	47.0 dB	0	0
5	Locked	QAM256	5	741000000 Hz	0.0 dBmV	46.1 dB	0	0
6	Locked	QAM256	6	747000000 Hz	0.3 dBmV	46.2 dB	0	0
7	Locked	QAM256	7	753000000 Hz	0.5 dBmV	46.4 dB	0	0
8	Locked	QAM256	8	759000000 Hz	0.4 dBmV	46.4 dB	0	0

Upstream Bonded Channels						
Channel	Lock Status	US Channel Type	Channel ID	Symbol Rate	Frequency	Power
1	Locked	ATDMA	49	5120 Ksym/sec	307000000 Hz	44.3 dBmV
2	Locked	TDMA and ATDMA	50	2560 Ksym/sec	185000000 Hz	44.3 dBmV
3	Locked	ATDMA	51	5120 Ksym/sec	233000000 Hz	43.8 dBmV
4	Locked	TDMA and ATDMA	52	2560 Ksym/sec	355000000 Hz	44.3 dBmV

Figure 25 – SBG6400 Status Connection Screen

## Back Up Your Gateway Configuration

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



**We highly recommend that you perform the gateway configuration backup using the SBG6400 default login username and password.**

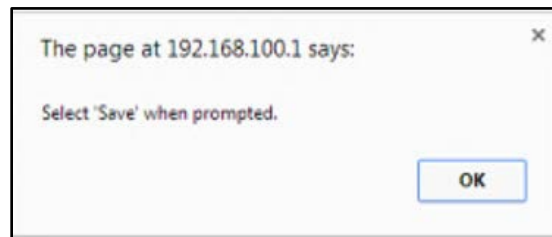
To create a back up copy of your gateway settings:

1. Click **Basic** on the SBG6400 Main Menu.
2. Click **Backup and Restore** from the Basic submenu options.



**Figure 26 – SBG6400 Backup and Restore Screen**

3. Click **Backup** and then click **OK** at the **Select 'Save'** prompt.



4. Click **Save** to create a backup file of your SBG6400 configuration in the File Download dialog box. A download is complete message will display.
5. Select **Desktop** from the pull-down list.  
*Note: GatewaySettings.bin is the default file name for your backup configuration file.*
6. Select the default **GatewaySettings.bin** file.
7. Select **bin Document** for the Save as document type.
8. Click **Save** and then **Close** to create a backup file of your SBG6400 configuration settings.

## Restore Your Gateway Settings

---

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

---

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

1. Click **Basic** on the SBG6400 Main Menu.
2. Click **Backup and Restore** from the Basic submenu options.
3. Click **Choose File** to search for a previously saved gateway configuration file from the Downloads folder on your computer.
4. Click **Open** and then **Restore**. The gateway will automatically reboot.

## Reset Your Gateway Settings

At any time, you can reset the SBG6400 gateway configuration settings and your user name and password back to the default factory settings. There are two methods available for resetting the gateway configuration settings on the SBG6400:

- Using the SBG6400 Reset button, see [Reset button](#)
- Using the SBG6400 Web Manager (this section)

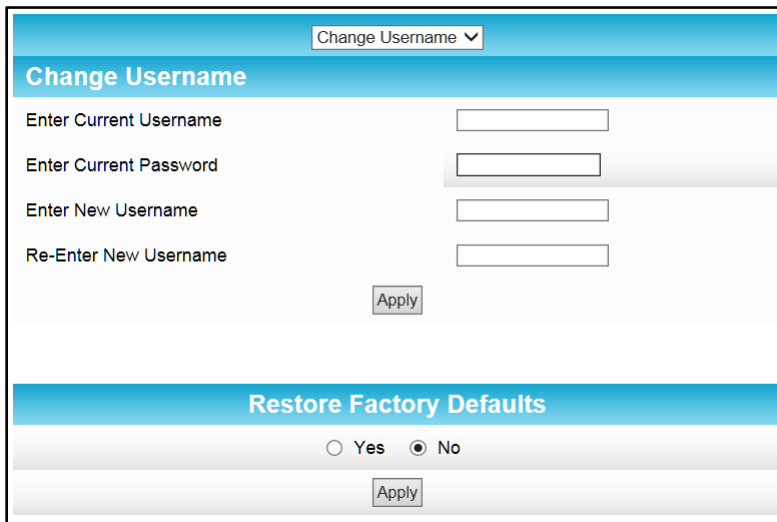
---

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

---

From the SBG6400 Web Manager, do the following to open the Status Security screen:

1. Click **Status** on the SBG6400 Main Menu.
2. Click **Security** from the Status submenu options.



**Figure 27 – Restore Factory Defaults Screen**

3. Select **Yes** under Restore Factory Defaults.
4. Click **Apply** to reset the default username and password, and restore the original gateway configuration.

The message, **This action will restore factory default settings. Please reboot the modem for new settings to take effect**, displays.

5. Click **OK**.
6. Click **Status** on the SBG6400 Main Menu.
7. Click **Configuration** from the Status submenu options to display the Status Configuration screen.

8. Click **Reboot**.
9. Log back in using the default username and password.
  - o Username: **admin**
  - o Password: **password**

## Exit the SBG6400 Web Manager

To log out and close the SBG6400 Web Manager:

- Click **Logout** located in the upper right corner of the screen above the SBG6400 Main Menu.



## 6

## Protecting & Monitoring Your Wireless Network

After you have successfully connected the SBG6400 and your wireless devices, you should configure the gateway to protect your wireless network from unwanted and unauthorized access by any wireless devices within range of your wireless network. Although security for the SBG6400 is already configured, you can use the SBG6400 Configuration Manager to tailor the level of security and access that you want to allow on your network.

### Prevent Unauthorized Access



**To prevent unauthorized access and configuration to your wireless network, we highly recommend that you immediately change the default user name and password after connecting to the Internet and logging on to the SBG6400 for the first time.**

One of the most important recommendations for securing your wireless home network is to change the default administrator password on your SBG6400 and other wireless devices as well. Default passwords are commonly used and shared on the Internet.

To ensure that your wireless home network is secure, it is recommended that you follow these best practices for user passwords:

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

**Note:** If your service provider supplied the SBG6400, you may not have the necessary user privileges to change the log in user name.

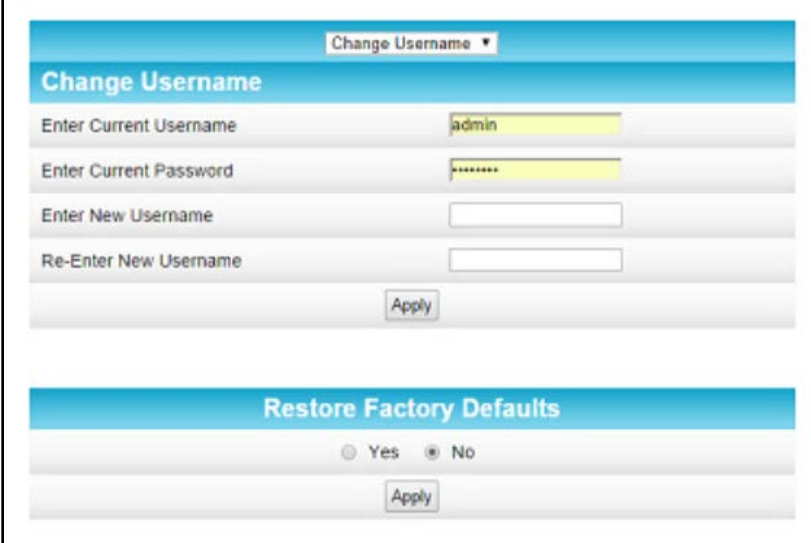
### Change the Default User Name and Password

To change the default user name:

1. Log in to the SBG6400 from any web browser on the computer connected to the SBG6400.
2. Type the Gateway Web Manager IP address, **http://192.168.0.1**, in the Address bar and then press **Enter**. The gateway Login screen displays.
3. Type the default username and password as they appear below:
  - o Username: **admin**
  - o Password: **password**
4. Click **Login** to open the SBG6400 Web Manager. The SBG6400 Status Connection screen displays.
5. Click the **Status** menu button and then click **Security** to display the Status Security screen.

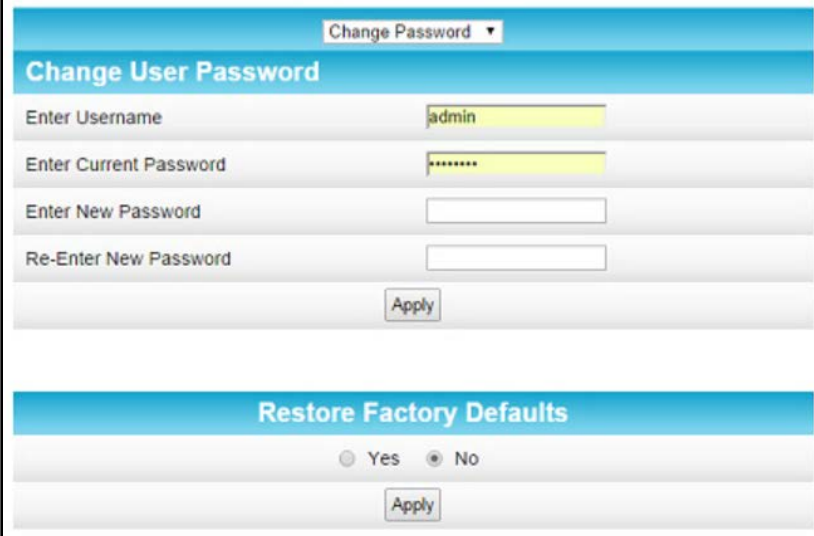


6. Confirm that **Change Username** is displayed in the drop-down selection box.
7. Complete each field entry, but note the following:
  - o All fields (for example, Current Username & Current Password) are case-sensitive.  
**Note:** For first time logons, the current username is **admin** and the current password is **password**.
  - o Make sure **No** is selected under **Restore Factory Defaults**.



**Figure 28 – Change User Name Screen**

8. Click **Apply** to update your user name.
9. Click **Change Username** drop-down arrow to display **Change Password**.



**Figure 29 – Change User Password Screen**

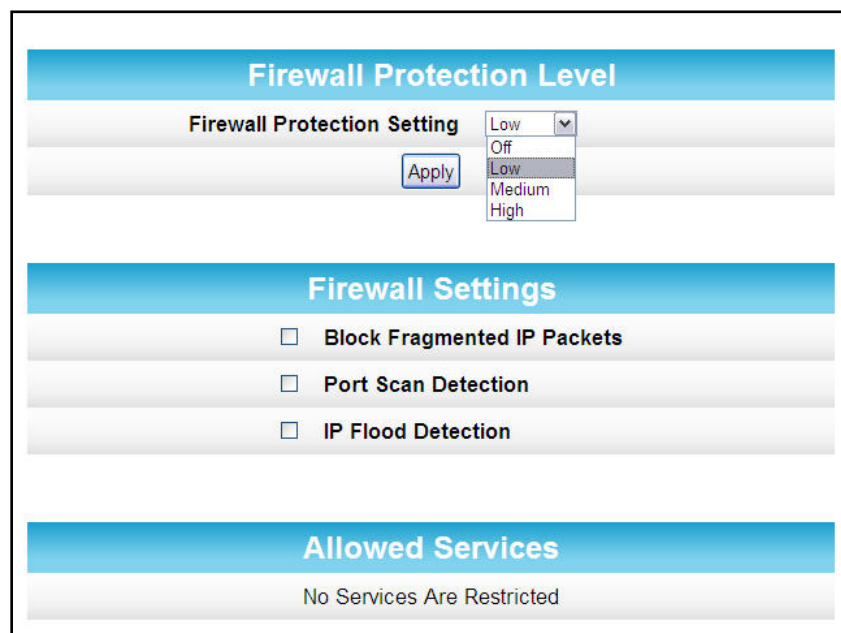
10. Complete each field entry, but note the following:
  - o All fields are case-sensitive.
  - o Username is your new user name, if you changed it.
  - o Make sure **No** is selected for **Restore Factory Defaults**.
  - o Find a secure place to write down and keep your new user name and password.
11. Click **Apply** to update your password.

## Set Up Firewall Protection

You can set up firewall filters and firewall alert notifications on your wireless home network. You can also block Java Applets, Cookies, ActiveX controls, popup windows, Proxies, and website access. See [Protection Level](#) for more information.

To set the firewall protection level:

1. From any screen, click the **Firewall-Protection Level** menu link or click the **Firewall** menu button on the SBG6400 Main Menu and then select **Protection Level**.



**Figure 30 – Firewall Protection Level Screen**

2. Click the Firewall Protection Setting drop-down button to select the firewall protection level.  
Possible values:
  - o **Off**
  - o **Low**
  - o **Medium**
  - o **High**

**Note:** Selecting **Off** will disable firewall protection on your home network. Your computer(s) and other Ethernet-enabled devices on your network will be at risk for possible attacks from viruses and hackers.

3. Select each Web filter that you want to set for the firewall and then click **Apply**.

## Set Up Parental Controls

You can set up the following Parental Controls on your home network:

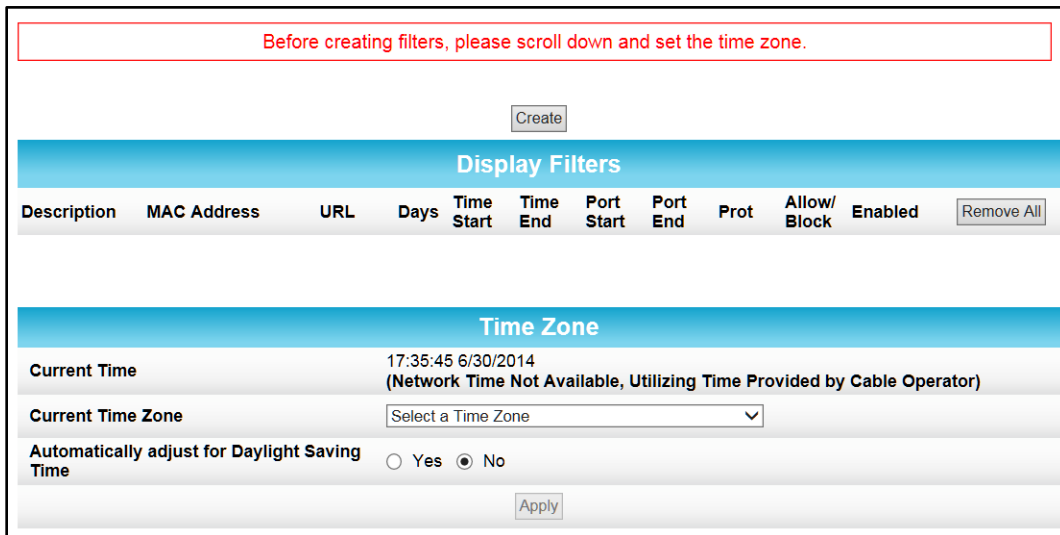
- Allow or block access to specific Internet sites.
- Allow or block access to specific MAC addresses.
- Set time limitations for computer usage or Internet access

**Note:** Any Parental Control filters that do not include assigned ports, will apply to all ports. This also applies to MAC addresses as well.

You can also link each user on your network to specified rules for login, time-access, and content filtering. See [Parental Control](#) for more information.

To set Parental Controls:

1. From any screen, click the **Firewall-Parental Control** menu link or click the **Firewall** menu button on the SBG6400 Main Menu and then select **Parental Control**.



Before creating filters, please scroll down and set the time zone.

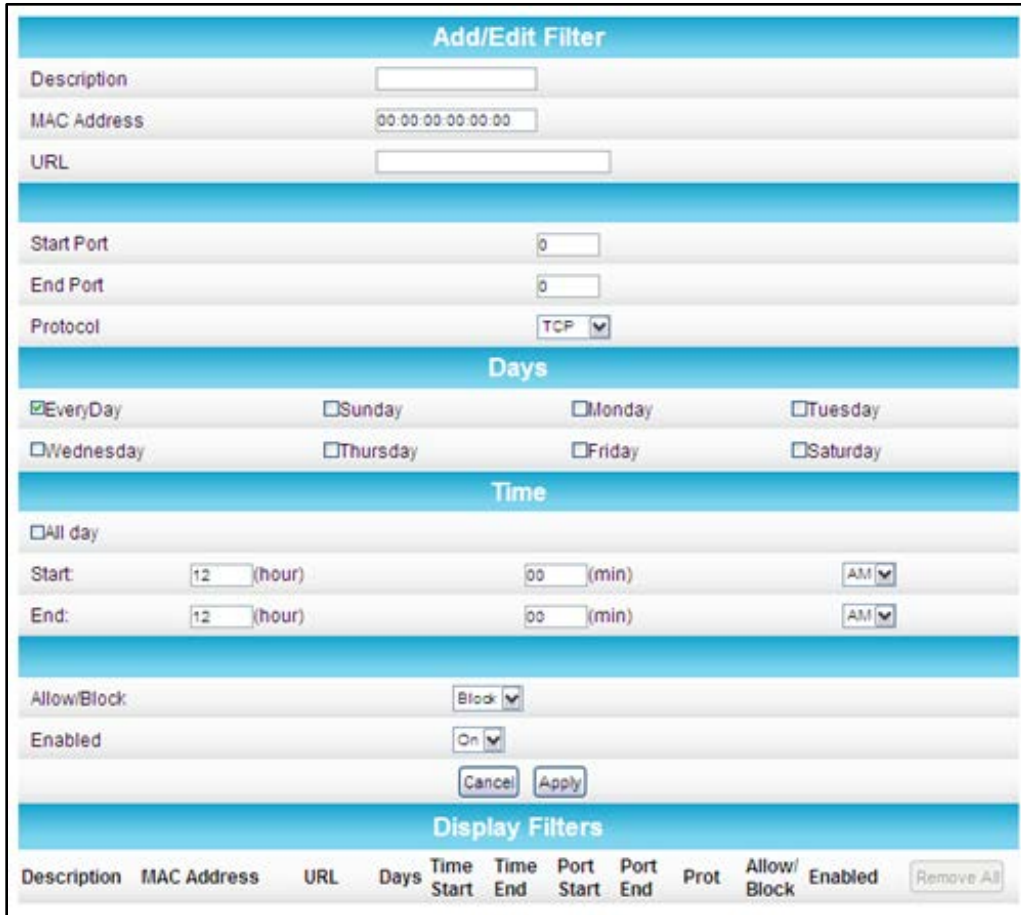
Create

Display Filters											
Description	MAC Address	URL	Days	Time Start	Time End	Port Start	Port End	Prot	Allow/Block	Enabled	Remove All
Time Zone											
Current Time			17:35:45 6/30/2014 (Network Time Not Available, Utilizing Time Provided by Cable Operator)								
Current Time Zone			Select a Time Zone								
Automatically adjust for Daylight Saving Time			<input type="radio"/> Yes <input checked="" type="radio"/> No								

Apply

**Figure 31 – Parental Control-Change Time Zone Screen**

2. Click **Current Time Zone** drop-down button to select your time zone.
3. Select **Yes** or **No** to automatically adjust the time for Daylight Saving Time.
4. Click **Create** to continue setting up Parental Controls (see Figure 22).
5. Enter a name for the user profile that you want to create in the Description field.
6. Enter the 12-digit (hexadecimal) MAC address of the device for which you are creating Parental Controls in the MAC Address field.



Description	MAC Address	URL	Start Port	End Port	Protocol	Days	Time	Allow/Block	Enabled
	00:00:00:00:00:00		0	0	TCP	<input checked="" type="checkbox"/> EveryDay <input type="checkbox"/> Sunday <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input type="checkbox"/> Saturday	<input type="checkbox"/> All day Start: 12 (hour) 00 (min) AM End: 12 (hour) 00 (min) AM	Block	On

Description	MAC Address	URL	Days	Time Start	Time End	Port Start	Port End	Prot	Allow/Block	Enabled	Remove All

**Figure 32 – Firewall Parental Control Screen**

7. Enter the web address of the Internet site that you want to block or access.
8. Enter the Starting port number of the in the Start Port field.
9. Enter the Ending port number of the in the End Port field.
10. Select **TCP**, **UDP**, or **BOTH** from the Internet Protocol drop-down list.
11. Select the days of the week that you want to allow the selected user to access the Internet.
12. Select the time range that you want to allow the selected user to access the Internet.
13. Select to **Allow** or **Block** Internet access for the time and days you set previously.
14. Select **On** or **Off** in the Enabled field to enable or disable this Parental Control restriction.
15. Click **Apply**, when done.

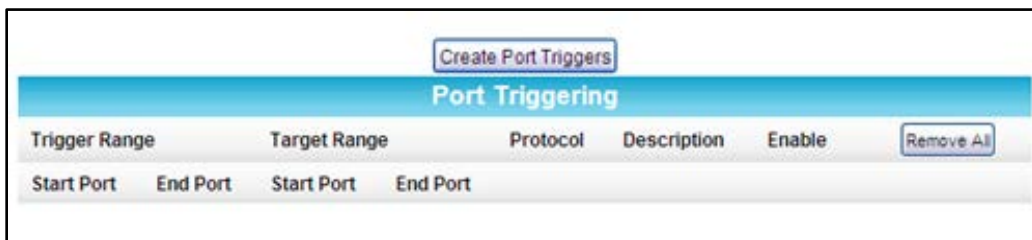
## Set Up Port Triggers

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

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

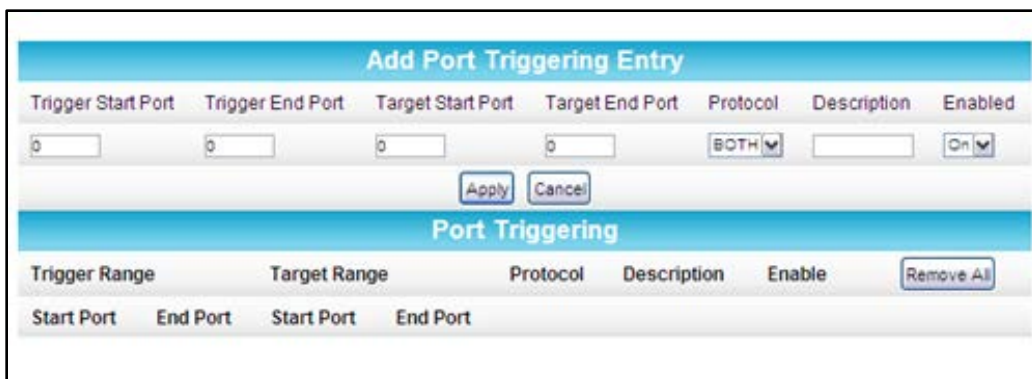
To configure Port Triggers:

1. Click **Advanced** on the SBG6400 Main Menu bar.
2. Click **Port Triggers** from the Advanced submenu options.



**Figure 33 – Advanced Port Triggers Screen**

3. Click **Create Port Triggers** button to open the Add Port Triggering Entry window.



**Figure 34 – Create Port Triggers Screen**

4. Enter the starting port number for the port to be triggered in the Trigger Start Port field.
5. Enter the ending port number for the port to be triggered in the Trigger End Port field.
6. Enter the starting port number of the Port Trigger range in the Target Start Port field.
7. Enter the ending port number of the Port Trigger range in the Target End Port field.
8. Select **TCP**, **UDP**, or **BOTH** from the Internet Protocol drop-down list.
9. Enter a unique name in the Description field.
10. Select **On** to enable IP port triggers or **Off** to disable them.

11. Click **Apply** to create your port triggers.
12. Repeat steps 3 thru 11 for each additional port trigger that you want to create.

## Set Up Port Forwarding

You can use Port Forwarding to set up a computer or other network device on your home network (LAN) to be accessible to computers or other remote network devices on the Internet. This allows you to open specific ports behind the firewall on your LAN to set up dedicated connections between your computer and other remote computers for online gaming or other online services. Some allowable services are predefined under the Commonly Forwarded Ports. See Figure 26 for a list of commonly used port numbers.

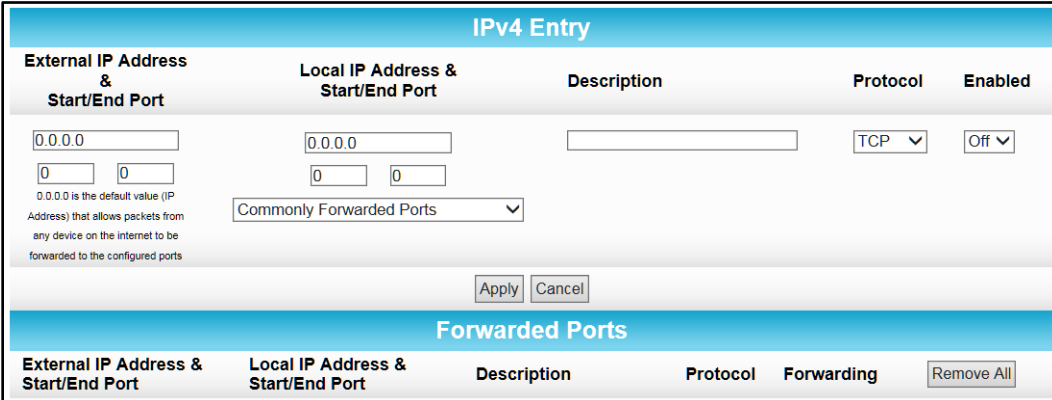
**Note:** It is recommended that you manually configure the TCP/IP settings listed below on the computer you are setting up for remote access. Otherwise, remote access to your computer will not be available on the Internet.

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

To set up Port Forwarding:

1. Click **Advanced** on the SBG6400 Main Menu bar.
2. Click **Port Forwarding** from the Advanced submenu options.

**Note:** To map a port, you would enter the range of port numbers that you want forwarded locally and the IP address for sending traffic to those ports. If you only want a single port specification, enter the same port number in the start and end locations for that IP address.



The screenshot shows the 'Advanced Port Forwarding Screen' with two main sections: 'IPv4 Entry' and 'Forwarded Ports'.

**IPv4 Entry Section:**

External IP Address & Start/End Port	Local IP Address & Start/End Port	Description	Protocol	Enabled
<input type="text" value="0.0.0.0"/> <input type="text" value="0"/> <input type="text" value="0"/> <small>0.0.0.0 is the default value (IP Address) that allows packets from any device on the internet to be forwarded to the configured ports</small>	<input type="text" value="0.0.0.0"/> <input type="text" value="0"/> <input type="text" value="0"/>	<input type="text"/>	TCP ▾	Off ▾
Commonly Forwarded Ports ▾				

Buttons: Apply, Cancel

**Forwarded Ports Section:**

External IP Address & Start/End Port	Local IP Address & Start/End Port	Description	Protocol	Forwarding	Remove All
					<input type="button" value="Remove All"/>

**Figure 35 – Advanced Port Forwarding Screen**

3. Do either of the following to set up the External IP Address:
  - o Keep the IP Address set at **0.0.0.0** in the External IP Address field and then enter the port number in the Start Port field. Repeat the same port number in the End Port field (select a specific port from the Commonly Forwarded Ports drop-down list or see Figure 26 for the list). This allows incoming data traffic on the specified ports from **any** remote IP address.

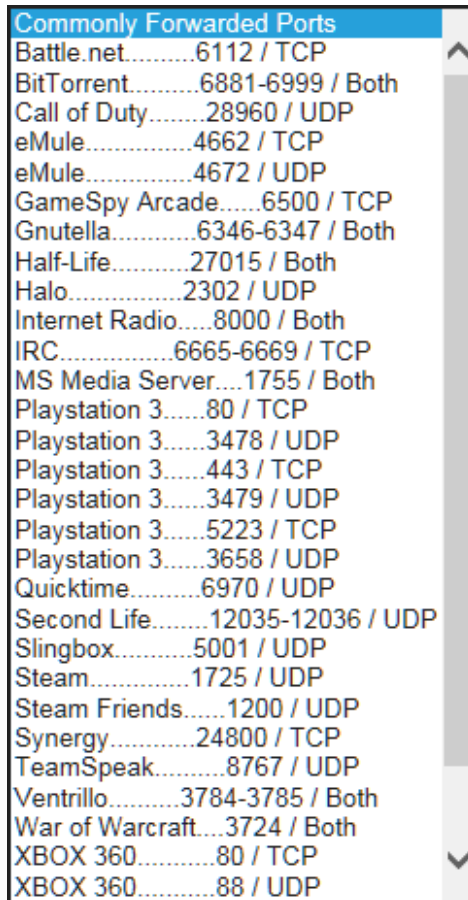
- o Enter a specific remote IP address of your choice in the External IP Address field and then enter the specific port numbers in the Start and End Port fields (select a specific port from the Commonly Forwarded Ports drop-down list or see Figure 26 for the list).

This allows incoming data traffic on the specified ports from only **one** remote IP address.

**Note:** To forward a range of ports, enter the first number of the port range in the Start Port field and the last number of the port range in the End Port field.

4. Do the following to set up your Local IP Address:
  - a. Enter the IP address of your local computer that you are setting up for port forwarding.
  - b. Enter the port number of your choice in the Start Port field. Repeat the same port number in the End Port field (select a specific port from the Commonly Forwarded Ports drop-down list or see Figure 26 for the list).

**Note:** To forward a range of ports, enter the first number of the port range in the Local Start Port field and the last number of the port range in the Local End Port field.
5. Enter a description to name the forwarded port you are creating.
6. Select **TCP**, **UDP**, or **BOTH** from the Internet Protocol drop-down list.
7. Select **On** to enable port forwarding or **Off** to disable it.
8. Click **Apply**.



Commonly Forwarded Ports		
Battle.net.....	6112 /	TCP
BitTorrent.....	6881-6999 /	Both
Call of Duty.....	28960 /	UDP
eMule.....	4662 /	TCP
eMule.....	4672 /	UDP
GameSpy Arcade.....	6500 /	TCP
Gnutella.....	6346-6347 /	Both
Half-Life.....	27015 /	Both
Halo.....	2302 /	UDP
Internet Radio.....	8000 /	Both
IRC.....	6665-6669 /	TCP
MS Media Server....	1755 /	Both
Playstation 3.....	80 /	TCP
Playstation 3.....	3478 /	UDP
Playstation 3.....	443 /	TCP
Playstation 3.....	3479 /	UDP
Playstation 3.....	5223 /	TCP
Playstation 3.....	3658 /	UDP
Quicktime.....	6970 /	UDP
Second Life.....	12035-12036 /	UDP
Slingbox.....	5001 /	UDP
Steam.....	1725 /	UDP
Steam Friends.....	1200 /	UDP
Synergy.....	24800 /	TCP
TeamSpeak.....	8767 /	UDP
Ventrillo.....	3784-3785 /	Both
War of Warcraft....	3724 /	Both
XBOX 360.....	80 /	TCP
XBOX 360.....	88 /	UDP

**Figure 36 – Commonly Used Forwarded Ports List**

## Set Up the DMZ Host

**WARNING!** The gaming DMZ host is not protected by the SBG6400 gateway firewall. It is exposed to the Internet and thus vulnerable to attacks or hacking from any computer on the Internet. Consider carefully before configuring a device to be in the DMZ.

You can configure one computer on your home network to be the DMZ Host. That computer will operate outside of the SBG6400 firewall and allow remote access from the Internet to your computer, gaming device, or other IP-enabled device. The DMZ Host feature will only allow outside users to have direct access to the designated DMZ Host device and not your home network. See [DMZ Host](#) for more information.

To create the DMZ Host:

1. Click **Advanced** on the SBG6400 Main Menu bar.
2. Click **DMZ Host** from the Advanced submenu options.



**Figure 37 – Advanced DMZ Host Screen**

3. Enter the last one to three digits (from **2** to **254**) of the IP address of the computer or gaming device that you are setting up as the DMZ host.
4. Click **Apply**.

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

## Store Remote Firewall Logs

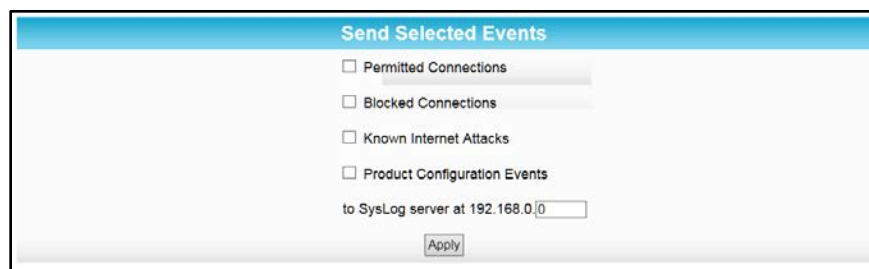
You can store firewall attack reports or logs on a computer in your home, so that multiple instances can be logged over a period of time. You can select individual attack or configuration items to send to the SysLog server, so that only the items of interest will be monitored.

**Note:** The SysLog server must be on the same network as the Private LAN behind the Configuration Manager (typically **192.168.0.x**).

To store remote Firewall logs:

1. Click the **Firewall-Remote Log** menu link or click the Firewall menu button on the SBG6400 Main Menu and then select **Remote Log**.





The screenshot shows a web interface titled "Send Selected Events". It contains four unchecked checkboxes: "Permitted Connections", "Blocked Connections", "Known Internet Attacks", and "Product Configuration Events". Below these is a text input field labeled "to SysLog server at 192.168.0.0" with a cursor in the last digit. An "Apply" button is located at the bottom of the form.

**Figure 38 – Firewall Remote Log Screen**

2. Select all desired event types that you want to monitor. This will activate the SysLog monitoring feature.
3. Enter the last digits from **10** to **254** of the SysLog server's IP address.  
***Note:** Normally, the IP address of this SysLog server is hard-coded so that the address always agrees with the entry on this page.*
4. Click **Apply**.

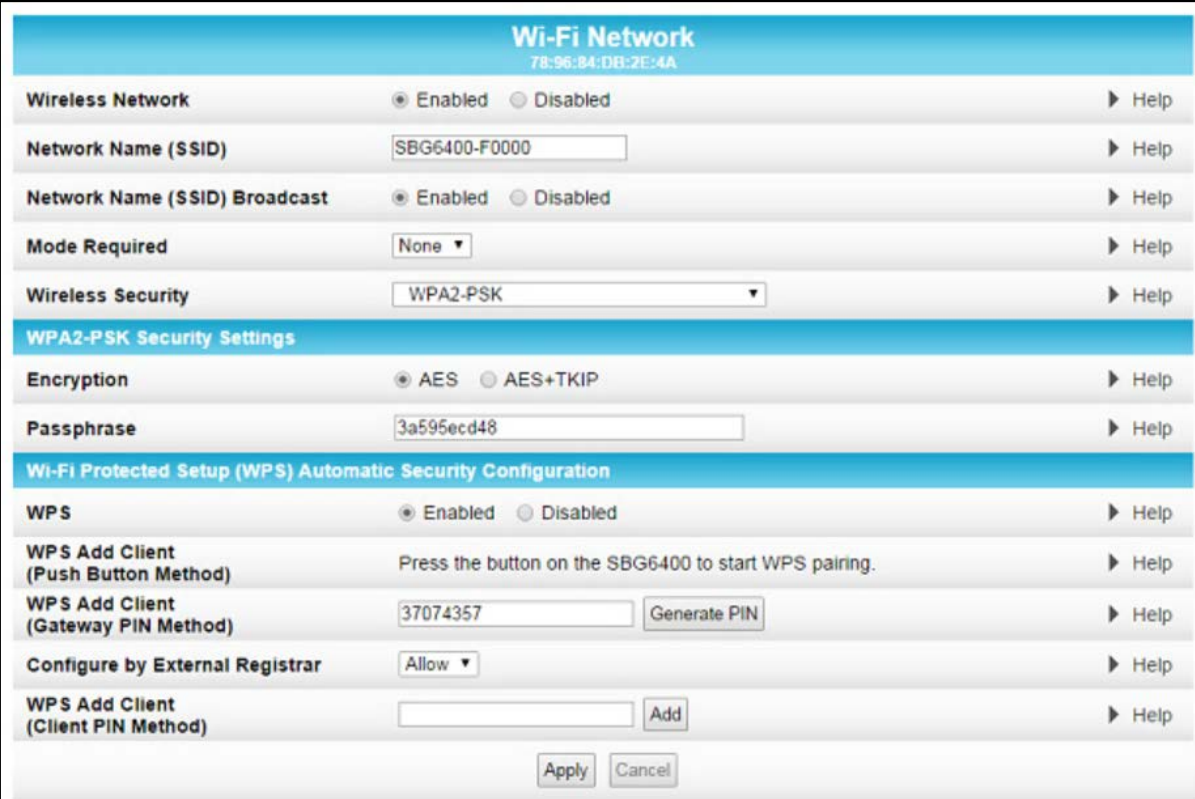
# 7

## Creating Wi-Fi Networks

The SBG6400 supports a secure method for setting up multiple access points on your wireless home network. This enables you to designate a guest network for visitors, friends, or other family members without giving them access to your files or other devices on your primary network. You have the option to create a PIN or pushbutton method for logging onto your wireless network.

### Set Up Your Wireless Primary Network

1. Open a web browser and log onto the SBG6400 to open the SBG6400 Web Manager. See [Start the Gateway Web Manager](#) for more information.
2. Click **Wireless** on the SBG6400 Main Menu bar.
3. Click **Primary Network Settings** from the Wireless submenu options.



Wi-Fi Network 78:96:B4:DB:2E:4A		
Wireless Network	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	▶ Help
Network Name (SSID)	<input type="text" value="SBG6400-F0000"/>	▶ Help
Network Name (SSID) Broadcast	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	▶ Help
Mode Required	<input type="text" value="None"/>	▶ Help
Wireless Security	<input type="text" value="WPA2-PSK"/>	▶ Help
<b>WPA2-PSK Security Settings</b>		
Encryption	<input checked="" type="radio"/> AES <input type="radio"/> AES+TKIP	▶ Help
Passphrase	<input type="text" value="3a595ecd48"/>	▶ Help
<b>Wi-Fi Protected Setup (WPS) Automatic Security Configuration</b>		
WPS	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	▶ Help
WPS Add Client (Push Button Method)	Press the button on the SBG6400 to start WPS pairing.	▶ Help
WPS Add Client (Gateway PIN Method)	<input type="text" value="37074357"/> <input type="button" value="Generate PIN"/>	▶ Help
Configure by External Registrar	<input type="text" value="Allow"/>	▶ Help
WPS Add Client (Client PIN Method)	<input type="text"/> <input type="button" value="Add"/>	▶ Help
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

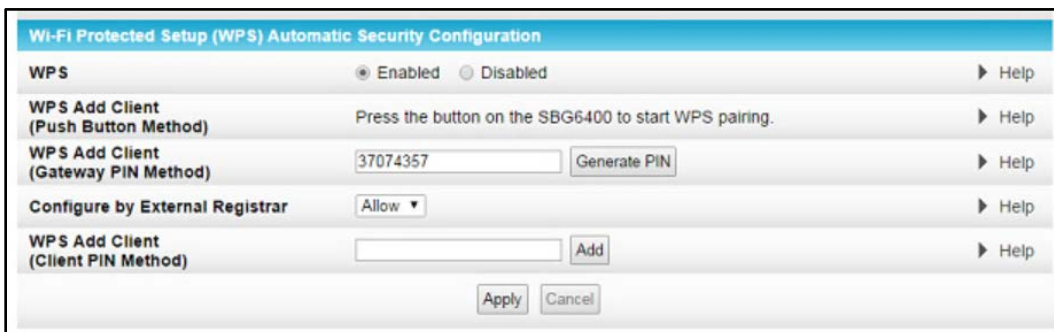
**Figure 39 – Wireless Primary Network Settings Screen**

4. Select **Enabled** or **Disabled** in the Wireless Network field to turn ON or OFF wireless networking on your wireless network.

5. Keep the default network name (also listed on the gateway label) or enter a name of your choice for your wireless primary network in the Network Name (SSID) field.  
The network name must consist of any combination of up to 32 ASCII characters. It cannot match any other SSID on your SBG6400.
6. Select **Enabled** or **Disabled** in the Network Name (SSID) Broadcast field to turn ON or OFF outside access to your wireless network.
7. Select one of the following wireless network security options for your wireless network from the Wireless Security drop-down list:
  - o **WPA2-PSK:** Wi-Fi Protected Access version 2 with Pre-Shared Key (recommended)
  - o **WPA2-PSK + WPA-PSK:** combination Wi-Fi Protected Access version 2 with Pre-Shared Key and Wi-Fi Protected Access with Pre-Shared Key
  - o **Unencrypted:** Allows access to the wireless network without a Wi-Fi Security Key
  - o **WPA-PSK:** Wi-Fi Protected Access with Pre-Shared Key, standard encryption
  - o **WPA2 (Enterprise):** Wi-Fi Protected Access version 2 provides additional network security and requires a user name and password for network logon
  - o **WPA2 + WPA (Enterprise):** combination Wi-Fi Protected Access version 2 and Wi-Fi Protected Access provides additional network security and requires a user name and password for network logon
  - o **WPA (Enterprise):** Wi-Fi Protected Access provides additional network security and requires a user name and password for network logon
8. Choose the wireless network encryption type in the Encryption field:
  - o **AES** – Advanced Encryption Standard: Provides the strongest encryption (recommended)
  - o **AES+TKIP** – Advanced Encryption Standard and Temporal Key Integrity Protocol  
Allows both AES and TKIP-capable clients to connect to your wireless network
9. Enter any combination of characters and words for your network password in the Passphrase field.
10. Click **Apply** if you are done or continue with [Enable or Disable WPS on Your Wireless Network](#) to set up WPS on your wireless network.

## Enable or Disable WPS on Your Wireless Network

From the Wireless Primary Network screen, go to the WPS Automatic Security Configuration section:



The screenshot shows the 'Wi-Fi Protected Setup (WPS) Automatic Security Configuration' screen. It includes the following sections:

- WPS:** Radio buttons for 'Enabled' (selected) and 'Disabled', with a 'Help' link.
- WPS Add Client (Push Button Method):** Instruction 'Press the button on the SBG6400 to start WPS pairing.' with a 'Help' link.
- WPS Add Client (Gateway PIN Method):** A text input field containing '37074357', a 'Generate PIN' button, and a 'Help' link.
- Configure by External Registrar:** A dropdown menu set to 'Allow' with a 'Help' link.
- WPS Add Client (Client PIN Method):** An empty text input field, an 'Add' button, and a 'Help' link.

At the bottom of the screen are 'Apply' and 'Cancel' buttons.

Figure 40 – WPS Setup Screen

1. Select **Enabled** in the WPS field to turn ON the Wi-Fi Protected Setup (WPS) network security on your home network. Continue with step 2.  
- or -  
Select **Disabled** in the WPS field to turn OFF the Wi-Fi Protected Setup (WPS) network security on your home network. Proceed to step 3 to finish.
2. Select one of the following WPS Pairing methods to add or pair your WPS-enabled wireless devices:
  - o **Push Button** – Press the WPS button on the SBG6400 to start the WPS pairing process with the WPS-enabled wireless device you want to connect to your wireless network.  
Repeat for each additional WPS-enabled device.
  - o **Gateway PIN** – Click **Generate PIN** to automatically create a new numeric password for logging onto your wireless home network.
  - o **Client PIN** – Enter a numeric password to log onto your wireless network and then click **Add**.
3. Click **Apply** when done.

## Set Up a Wireless Guest Network

**Note:** This feature may be disabled on your SBG6400. Some service providers or cable operators do not allow for secondary (or guest) wireless networks on their gateway devices.

1. Open a web browser and log onto the SBG6400 to open the SBG6400 Web Manager. See [Start the Gateway Web Manager](#) for more information.
2. Click **Wireless** on the SBG6400 Main Menu bar.
3. Click **Guest Network Settings** on the Wireless submenu options.

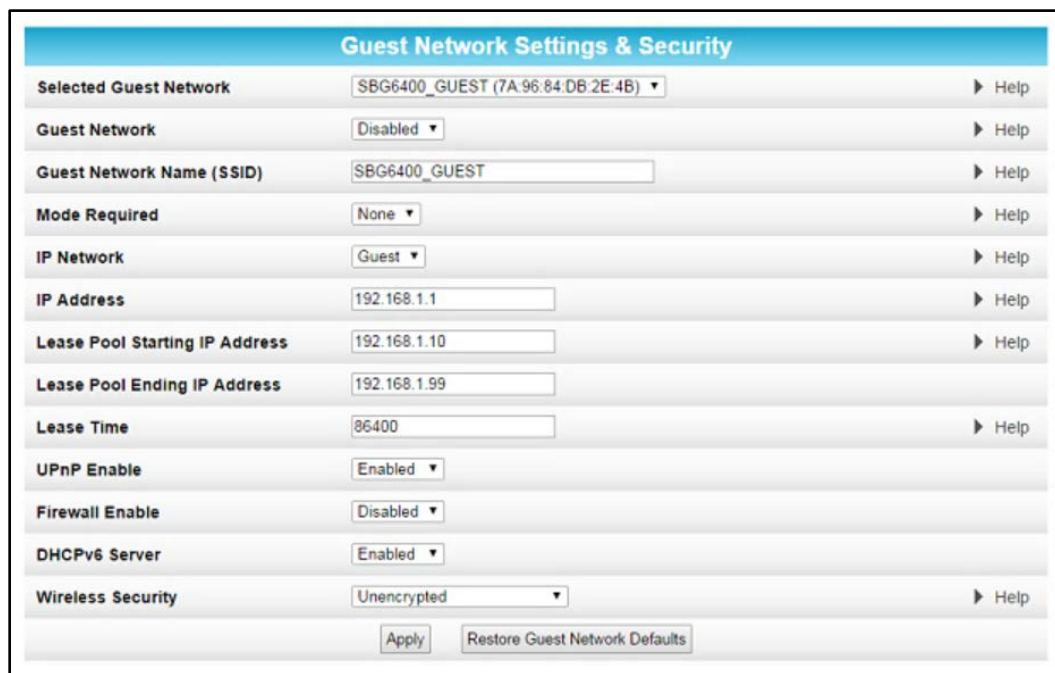


Figure 41 – Wireless Guest Network Screens

4. Select the frequency range for your wireless network.
5. Select the guest network from the Selected Guest Network drop-down list.
6. Select **Enabled** or **Disabled** in the Guest Network field to turn ON or OFF the selected wireless guest network.
7. Keep the default guest network name or enter a new name of your choice for your guest network in the Guest Network Name (SSID) field.
8. Select **LAN** or **Guest** from the IP Network drop-down list.
  - o **LAN** – Configures the guest network to be part of your primary network and allow guest users to connect to your primary network
  - o **Guest** – Configures the guest network to only allow access to a specific network and not your primary network
9. Enter the IP address for the SBG6400 on the Guest network in the IP Address field.
10. Enter the starting IP address for the guest network lease pool in the Lease Pool Starting IP Address field.
11. Enter the ending IP address for the guest network lease pool in the Lease Pool Ending IP Address field.
12. Enter the lease time for the guest network lease pool in the Lease Time field.
13. Select **Enabled** or **Disabled** in the UPnP (Universal Plug and Play) Enable field to allow or disallow any network devices, such as smart phones, tablets, gaming devices, or printers to automatically connect to your wireless home network.
14. Select **Enabled** or **Disabled** in the Firewall Enable field to turn ON or OFF the gateway firewall.
15. Select **Enabled** or **Disabled** in the DHCPv6 Server field to allow the DHCP server to send leases to the guest network clients from the guest network lease pool you specified earlier.

**Note:** *If the DHCP server is disabled, you must assign static IP addresses to the guest network STAs.*
16. Select one of the following wireless network security options for your wireless network from the Wireless Security drop-down list:
  - o **WPA2-PSK:** Wi-Fi Protected Access version 2 with Pre-Shared Key (recommended)
  - o **WPA2-PSK + WPA-PSK:** combination Wi-Fi Protected Access version 2 with Pre-Shared Key and Wi-Fi Protected Access with Pre-Shared Key
  - o **WPA-PSK:** Wi-Fi Protected Access with Pre-Shared Key, standard encryption
  - o **Unencrypted:** Turns off network security
  - o **WPA2 + WPA (Enterprise):** combination Wi-Fi Protected Access version 2 and Wi-Fi Protected Access provides additional network security and requires a user name and password for network logon
  - o **WPA2 (Enterprise):** Wi-Fi Protected Access version 2 provides additional network security and requires a user name and password for network logon
  - o **WPA (Enterprise):** Wi-Fi Protected Access provides additional network security and requires a user name and password for network logon
17. Click **Apply**, when done.

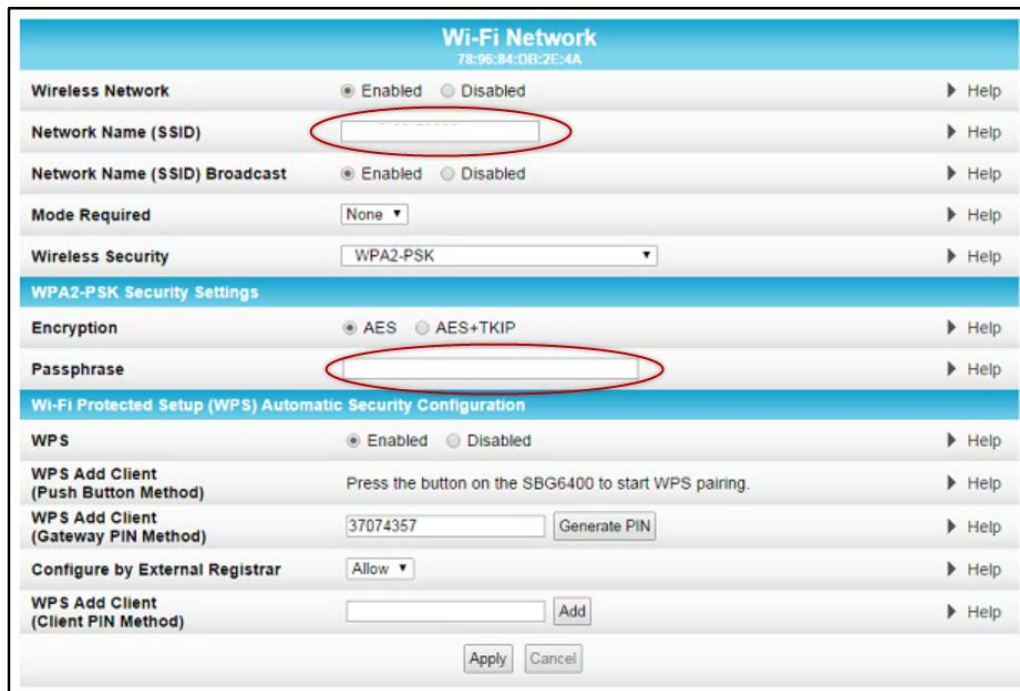
## Change Your Wireless Network Name (SSID)

The SSID (Service Set Identification) is the wireless network name assigned to your SBG6400 wireless primary and guest networks. The default SSID which is listed on the gateway label is automatically populated in the network configuration screens. A list of SSIDs of available wireless networks in close proximity of your home (for example, neighbors or local businesses) will display when you or someone else in your home attempt to establish a wireless network connection. For security purposes and quick recognition of your wireless network, it is recommended that you change the default SSID. You should also consider changing the default wireless password or passphrase (see [Prevent Unauthorized Access](#) for more information).

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

Do the following to change your wireless network name or SSID:

1. Open a web browser and log onto the SBG6400 to open the SBG6400 Web Manager. See [Start the Gateway Web Manager](#) for more information.
2. Click **Wireless** on the SBG6400 Main Menu bar.
3. Click **Primary Network Settings** from the Wireless submenu options to open the Wi-Fi Network screen.



The screenshot displays the 'Wi-Fi Network' configuration page. At the top, it shows the network name '78-96:84-0B:2E:4A'. The 'Wireless Network' section has 'Enabled' selected. The 'Network Name (SSID)' field is empty and circled in red. Below it, 'Network Name (SSID) Broadcast' is also 'Enabled'. The 'Mode Required' is set to 'None' and 'Wireless Security' is 'WPA2-PSK'. The 'WPA2-PSK Security Settings' section has 'Encryption' set to 'AES' and the 'Passphrase' field is empty and circled in red. The 'WPS' section is 'Enabled' and includes options for adding clients via push button, gateway PIN, or external registrar. At the bottom, there are 'Apply' and 'Cancel' buttons.

**Figure 42 – Change Your Network Name (SSID) and Password Screens**

4. Select the frequency range for your wireless network.
5. Make sure **Enabled** is selected in the Wireless Network field to turn ON wireless networking on your home network.

6. Delete the current network name in the Network Name (SSID) field and then enter a new name of your choice for your wireless network.

The network name can contain any combination of up to 32 alphanumeric characters.

7. Make sure **Enabled** is selected in the Network Name (SSID) Broadcast field.
8. Delete the current wireless password (passphrase) in the Passphrase field and enter a new passphrase for the wireless network password.

See [Prevent Unauthorized Access](#) for more information.

9. Click **Apply** at the bottom of the screen.

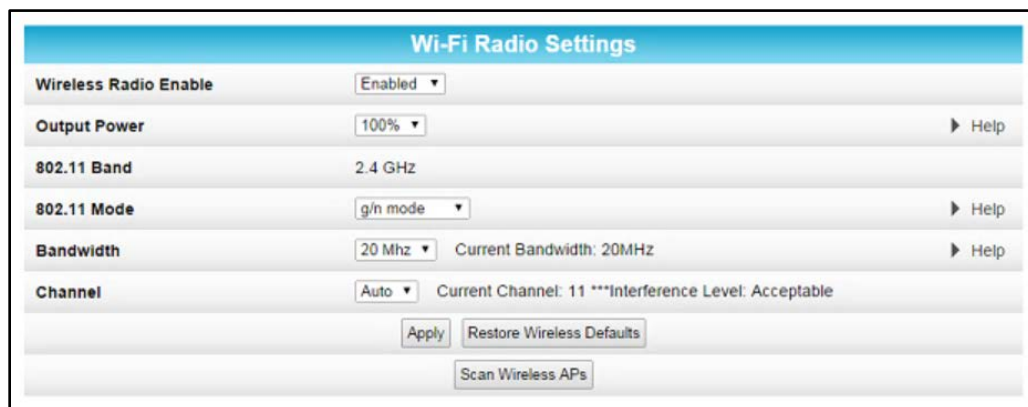
The new wireless network name should appear in the list of available wireless networks when you reconnect your wireless devices.

## Change the Wireless Channel

Network interference may occur at any time when using a wireless network connection. This may be caused by other wireless access points that are using the same wireless channel as your SBG6400 and are also operating within close proximity in your home. When experiencing wireless network interference, changing the wireless channel on the SBG6400 can improve network connectivity (or signal strength) and avoid network interference. By default, the SBG6400 is set on Channel 1.

Do the following to change the wireless channel on the SBG6400:

1. Open a web browser and log onto the SBG6400 to open the SBG6400 Web Manager. See [Start the Gateway Web Manager](#) for more information.
2. Click **Wireless** on the SBG6400 Main Menu bar.
3. Click **802.11 Radio** from the Wireless submenu options to open the Wireless 802.11 Radio screen.



**Figure 43 – Wireless 802.11 Radio Screens**

4. Select the frequency range for your wireless network.
5. Select a channel number from the Channel drop-down list that is different from the channel number listed as the Current Channel.

**Note:** It is recommended to use Channel 6 or 11, if it is not listed as the Current Channel. In the Wi-Fi spectrum, there are multiple channels that overlap and thus degrade wireless network performance. Channels 1, 6, and 11 are used for better network performance and stability because they do not overlap.

6. Click **Apply**.





# Troubleshooting Tips

If the solutions listed in this section do not solve your problem, contact your service provider for assistance.

Your service provider may ask for the status of the LEDs as described in [Front Panel LED Icons and Error Conditions](#).

You may have to reset the SBG6400 gateway configuration to its original factory settings if the gateway is not functioning properly.

## Solutions

**Table 5: Troubleshooting Solutions**

Gateway Problem	Possible Solution
<b>POWER LED Icon is OFF</b>	<ul style="list-style-type: none"> <li>• Check the power connection on the gateway and to the electrical outlet.</li> <li>• Check that the electrical outlet is working. Is the outlet controlled by a light switch? If so, disconnect the gateway power cord and connect it to another electrical outlet that is not controlled by a light switch.</li> </ul>
<b>Cannot Send or Receive Data</b>	<ul style="list-style-type: none"> <li>• Check each end of the coaxial cable connection on the gateway and cable outlet. Hand tighten each connector, if necessary.</li> <li>• Check the Ethernet cable to make sure it is properly connected to the gateway and computer.</li> <li>• On the front panel, check the status of the LED icons and refer to <a href="#">Front Panel LED Icons and Error Conditions</a> to identify the problem.</li> <li>• If you have cable television service, check your television to ensure your cable service is operating properly.</li> <li>• If none of the above solutions resolves the problem, contact your service provider or call ARRIS Technical Support at <b>1-877-466-8646</b> for assistance.</li> </ul>
<b>Cannot Access the Internet</b>	<ul style="list-style-type: none"> <li>• Check that all cable and power connections on your gateway and computer are properly connected.</li> <li>• Check that the Power, Online, and Wireless LED icons on the front panel are lit up solid.</li> <li>• Contact your service provider for assistance.</li> </ul>








Gateway Problem	Possible Solution
Wireless devices cannot send or receive data	<ul style="list-style-type: none"> <li>If the problem still persists after checking the coaxial cable and Ethernet connections and your IP address, check the <b>Wireless Security Mode</b> setting on the Wireless Primary Network screen.</li> <li>If you enabled <b>WPA</b> and configured a passphrase on the gateway, be sure each affected wireless client has the identical passphrase. If this does not solve the problem, check if the wireless client supports WPA.</li> <li>If you enabled <b>WEP</b> and configured a key on the gateway, be sure each affected wireless client has the identical WEP key. If this does not solve the problem, check whether the client’s wireless adapter supports the type of WEP key configured on the gateway.</li> </ul>

## Front Panel LED Icons and Error Conditions

The SBG6400 front panel LED icons provide status information for the following error conditions:

**Table 6: Front Panel LED Icons and Error Conditions**

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

# B

## Gateway Configuration Screen Definitions

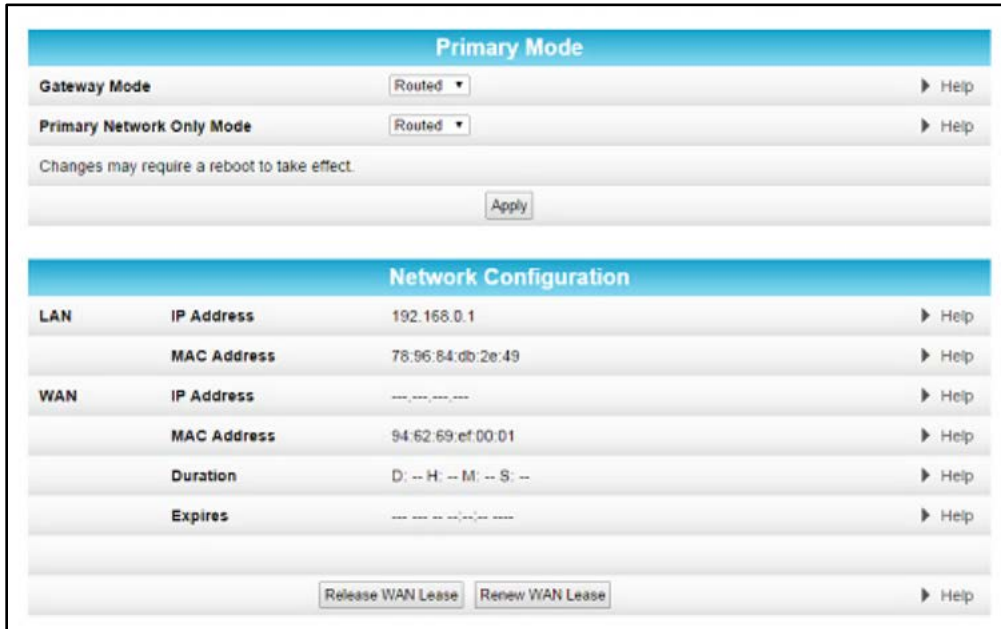
This section provides detailed field definitions for the following ARRIS SBG6400 network configuration screens:

- [Basic](#)
- [Advanced](#)
- [Firewall](#)

### Basic Screens

#### Setup

You can use the SBG6400 Basic Setup screen to configure basic SBG6400 IP-related configuration data, including your local network configuration, and WAN connection type.



The screenshot displays the 'Basic Setup' screen for the SBG6400 gateway. It is divided into two main sections: 'Primary Mode' and 'Network Configuration'.

**Primary Mode Section:**

- Gateway Mode:** Set to 'Routed' (dropdown menu). A 'Help' link is visible to the right.
- Primary Network Only Mode:** Set to 'Routed' (dropdown menu). A 'Help' link is visible to the right.
- A note states: 'Changes may require a reboot to take effect.'
- An 'Apply' button is located below the note.

**Network Configuration Section:**

<b>LAN</b>	<b>IP Address</b>	192.168.0.1	▶ Help
	<b>MAC Address</b>	78:96:84:db:2e:49	▶ Help
<b>WAN</b>	<b>IP Address</b>	---:---:---:---	▶ Help
	<b>MAC Address</b>	94:62:69:ef:00:01	▶ Help
	<b>Duration</b>	D: -- H: -- M: -- S: --	▶ Help
	<b>Expires</b>	---:---:---:---	▶ Help
	<input type="button" value="Release WAN Lease"/> <input type="button" value="Renew WAN Lease"/>		▶ Help

**Figure 44 – Basic Setup Screen**

**Table 7: Basic Setup Screen-Field Descriptions**

Field	Description
<b>Gateway Mode</b>	Sets the device mode: <b>Routed:</b> Allows the internal network devices to use IP addresses from the WAN subnet. <b>Bridged:</b> Disables the network address and port translation settings on the gateway.
<b>Primary Network Only Mode</b>	Sets the device mode for the primary network only: <b>Routed:</b> Allows the internal network devices to use IP addresses from the WAN subnet. <b>Bridged:</b> Disables the network address and port translation settings on the gateway.
<b>LAN</b>	
<b>IP Address</b>	The IP address of the SBG6400 on your home network (LAN).
<b>MAC Address</b>	Media Access Control address is set of 12 hexadecimal digits that are assigned during manufacturing to uniquely identify the hardware address of the SBG6400 access point.
<b>WAN</b>	
<b>IP Address</b>	The public WAN IP address of your SBG6400, which is either dynamically or statically assigned by the cable operator
<b>MAC Address</b>	Media Access Control address — a set of 12 hexadecimal digits assigned during manufacturing that uniquely identifies the hardware address of the SBG6400 access point.
<b>Duration</b>	Describes how long before your Internet connection expires, The WAN lease will automatically renew itself when it expires.
<b>Expires</b>	Displays the exact time and date the WAN lease expires
<b>Release WAN Lease</b>	Click to release the WAN lease
<b>Renew WAN Lease</b>	Click to renew the WAN lease

## DHCP

You can use the Basic DHCP (Dynamic Host Configuration Protocol) screen to configure the IP settings of your SBG6400 gateway and the DHCP server on your home network. You can also view the status of the optional internal SBG6400 DHCP server.

---

**WARNING!** Do not modify these setting unless you are an experienced network administrator with a strong understanding of IP addressing, sub-netting, and DHCP.

---

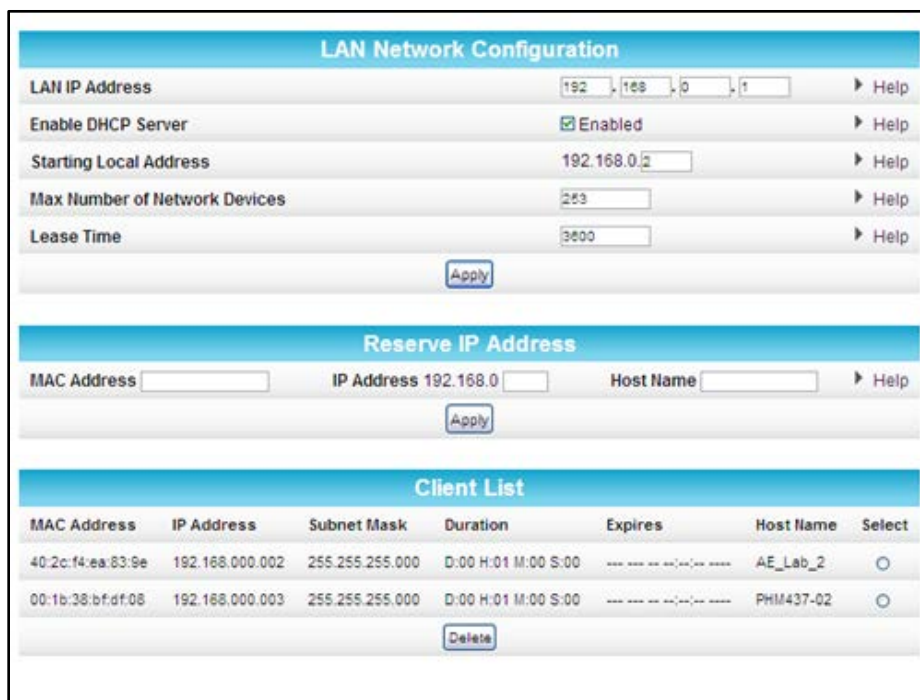



Figure 45 – Basic DHCP Screen

Table 8: Basic DHCP Screen-Field Descriptions

Field	Description
<b>LAN Network Configuration</b>	
<b>LAN IP Address</b>	The IP address of the SBG6400 on your home network (LAN).
<b>Enable DHCP Server</b>	Checkmark <b>Enabled</b> to enable the SBG6400 DHCP Server. Uncheck <b>Enabled</b> to disable the SBG6400 DHCP Server.
<b>Starting Local Address</b>	Enter the starting IP address to be assigned by the SBG6400 DHCP server to clients in dotted-decimal format. Default is <b>192.168.0.2</b> .
<b>Max Number of Network Devices</b>	Sets the maximum number of clients for the SBG6400 DHCP server to assign a private IP address.
<b>Lease Time</b>	Sets the time in seconds that the SBG6400 DHCP server leases an IP address to a client. The default is 3600 seconds (60 minutes).
<b>Reserve IP Address</b>	
	Lists clients in which the DHCP server reserves a specific IP address on the home network (LAN)
<b>Client List</b>	
	Lists the DHCP client device information.

## DDNS

You can use the Basic DDNS (Dynamic Domain Name System) screen to set up the DDNS service to assign a static Internet domain name to a dynamic IP address. This allows various servers on the Internet to access your computer for processing your requests when you are visiting various Internet sites.



DDNS		
DDNS Service	Disabled	▶ Help
Username		▶ Help
Password		▶ Help
Host Name		▶ Help
IP Address	206.18.87.27	▶ Help
Status	DDNS service is not enabled.	▶ Help
Apply		

**Figure 46 – Basic DDNS Screen**

**Table 9: Basic DDNS Screen-Field Descriptions**

Field	Description
<b>DDNS Service</b>	Select <b>Disabled</b> or select <b>wwwDynDNS.org</b> to enable the DDNS service
<b>Username</b>	Enter your user name for the Dynamic Domain Name system
<b>Password</b>	Enter your password for the Dynamic Domain Name system
<b>Host Name</b>	Enter the host name for the Dynamic Domain Name system
<b>IP Address</b>	Displays the IP address
<b>Status</b>	Shows if the DDNS service is <b>Enabled</b> or <b>Disabled</b>

## Backup and Restore

You can use the Basic Backup and Restore screen to save a backup copy of the current SBG6400 gateway configuration settings locally on your computer or restore previously saved gateway configurations.



**Figure 47 – Basic Backup & Restore Screen**

**Table 10: Basic Backup & Restore -Field Descriptions**

Field	Description
<b>Choose File</b>	Allows you to search for a file on your computer to retrieve or save the gateway configuration.
<b>Restore</b>	Restores a previously saved gateway configuration.
<b>Backup</b>	Creates a back up copy of the current gateway configuration.

## Advanced Screens

### Options

You can use the Advanced Options to set the operating modes for adjusting how the SBG6400 routes IP traffic on your home network.



Advanced Options	
WAN Blocking	<input checked="" type="checkbox"/> Enable
IPsec Pass-through	<input type="checkbox"/> Enable
PPTP Pass-through	<input type="checkbox"/> Enable
Remote Config Management	<input type="checkbox"/> Enable
Multicast Enable	<input checked="" type="checkbox"/> Enable
UPnP Enable	<input type="checkbox"/> Enable
NAT ALG Status	
FTP	<input checked="" type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable
Kerb88	<input checked="" type="checkbox"/> Enable
Kerb1293	<input checked="" type="checkbox"/> Enable
ICQ	<input checked="" type="checkbox"/> Enable
ICQTalk	<input checked="" type="checkbox"/> Enable
IRC666x	<input checked="" type="checkbox"/> Enable
IRC7000	<input checked="" type="checkbox"/> Enable
IRC8000	<input checked="" type="checkbox"/> Enable
H225	<input checked="" type="checkbox"/> Enable
RSVP	<input checked="" type="checkbox"/> Enable
NetBios	<input checked="" type="checkbox"/> Enable
MSN	<input checked="" type="checkbox"/> Enable
PPTP	<input checked="" type="checkbox"/> Enable
Net2Phone	<input checked="" type="checkbox"/> Enable
RTSP	<input checked="" type="checkbox"/> Enable
IKE	<input checked="" type="checkbox"/> Enable
SIP	<input checked="" type="checkbox"/> Enable
<input type="button" value="Apply"/>	
Pass-through MAC Addresses	
<input type="text"/>	<input type="button" value="Add MAC Address"/> (example: 01:23:45:67:89:AB)
<input type="text"/> MAC Addresses entered: 0/32	
<input type="button" value="Remove MAC Address"/> <input type="button" value="Clear All"/>	

**Figure 48 – Advanced Options Screen**

**Table 11: Advanced Options-Field Descriptions**

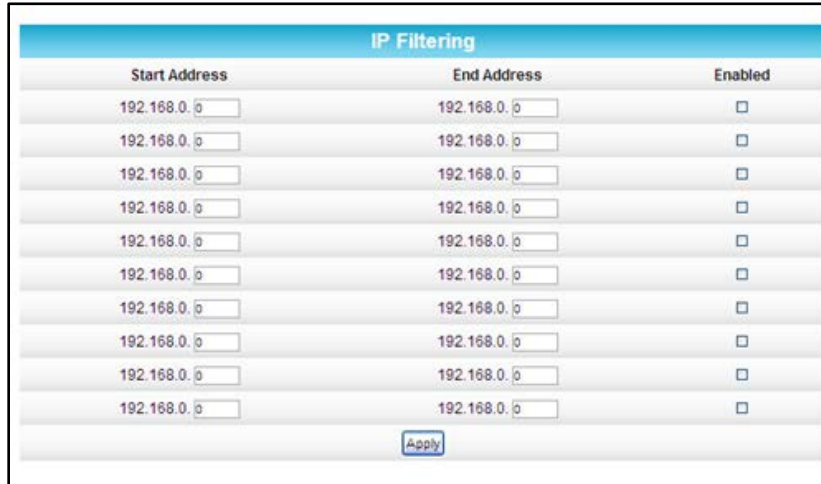
Field	Description
<b>WAN Blocking</b>	Prevents the SBG6400 Web Manager or the computers behind it from being visible to other computers on the SBG6400 WAN.
<b>IPsec Pass-through</b>	Enables the IPsec Pass-through protocol to be used through the SBG6400 Web Manager so that a VPN device (or software) may communicate properly with the WAN.
<b>PPTP Pass-through</b>	Enables the Point-to-Point Tunneling Protocol (PPTP) Pass-through protocol to be used through the SBG6400 Web Manager so that a VPN device (or software) may communicate properly with the WAN.
<b>Remote Config Management</b>	<p>Allows remote access to the SBG6400 Web Manager. This enables you to configure the SBG6400 WAN by accessing the WAN IP address at Port 8080 of the SBG6400 Web Manager from anywhere on the Internet.</p> <p>For example, in the Internet browser URL window, type <b>http://WanIPAddress:8080/</b> to access the SBG6400 Web Manager remotely.</p>
<b>Multicast Enable</b>	Allows multicast-specific traffic (denoted by a multicast specific address) to be passed to and from the computers on the home network (LAN) behind the SBG6400 Web Manager.
<b>UPnP Enable</b>	<p>Turns on the Universal Plug and Play protocol (UPnP) agent in the SBG6400 Web Manager.</p> <p>Select this option, if you are running a CPE (client) application that requires UPnP.</p>
<b>NAT ALG Status</b>	Turn ON or OFF the various Network Address Translation (NAT) and Application Level Gateway (ALG) status options on your wireless network
<b>Add MAC Address</b>	<p>Enter the MAC address for the computer you want to block and click <b>Add MAC Address</b> button.</p> <p>Repeat for up to 20 MAC addresses.</p>
<b>Remove MAC Address</b>	Enter the MAC address filter that you want to delete or block, then click <b>Remove MAC Address</b> button.
<b>Clear All button</b>	Deletes all of your MAC Address filters.



## IP Filtering

IP filtering allows you to define which local computers will be denied access to the SBG6400 WAN. You can configure IP address filters to block Internet traffic to specific network devices on your home network by entering the starting and ending IP address ranges.

**Note:** You only have to enter the LSB (Least-significant byte) of the IP address; the upper bytes of the IP address are set automatically from the SBG6400 Web Manager's IP address.



Start Address	End Address	Enabled
192.168.0. <input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>
192.168.0. <input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>
192.168.0. <input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>
192.168.0. <input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>
192.168.0. <input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>
192.168.0. <input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>
192.168.0. <input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>
192.168.0. <input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>
192.168.0. <input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>
192.168.0. <input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>

Figure 49 – Advanced IP Filtering Screen

Table 12: Advanced IP Filtering -Field Descriptions

Field	Description
<b>Start Address</b>	Enter the starting IP address range of the computers for which you want to deny access to the SBG6400 WAN. Be sure to only enter the least significant byte of the IP address.
<b>End Address</b>	Enter the ending IP address range of the computers you want to deny access to the SBG6400 WAN. Be sure to only enter the least significant byte of the IP address.
<b>Enabled</b>	Activates the IP address filter, when selected. Select <b>Enabled</b> for each range of IP addresses you want to deny access to the SBG6400 WAN. When done, click <b>Apply</b> to activate and save your settings.

## MAC Filtering

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



Figure 50 – Advanced MAC Filtering Screen

Table 13: Advanced MAC Filtering -Field Descriptions

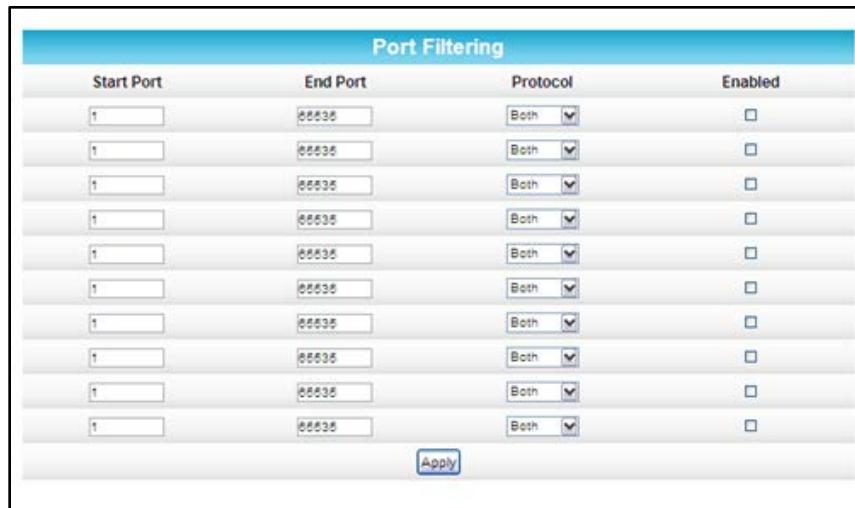
Field	Description
<b>Add MAC Address</b>	Enter the MAC address for the computer you want to block and click <b>Add MAC Address</b> button. Repeat for up to 20 MAC addresses.
<b>Remove MAC Address</b>	Enter the MAC address filter that you want to delete block and click <b>Remove MAC Address</b> button.
<b>Clear All button</b>	Deletes all of your MAC Address filters.

## Port Filtering

Port filtering allows you to define port filters to prevent all devices from sending outgoing TCP/UDP traffic to the WAN on specific IP port numbers. By specifying a starting and ending port range, you can determine what TCP/UDP traffic is allowed out to the WAN on a per-port basis.

**Note:** The specified port ranges are blocked for ALL computers, and this setting is not IP address or MAC address specific. For example, if you wanted to block all computers on your home network from accessing HTTP sites (or web surfing), you would create the following port filter and then click **Apply** when done:

- Set **Start Port** to **80**
- Set **End Port** to **80**
- Set **Protocol** to **TCP**
- Select **Enabled**



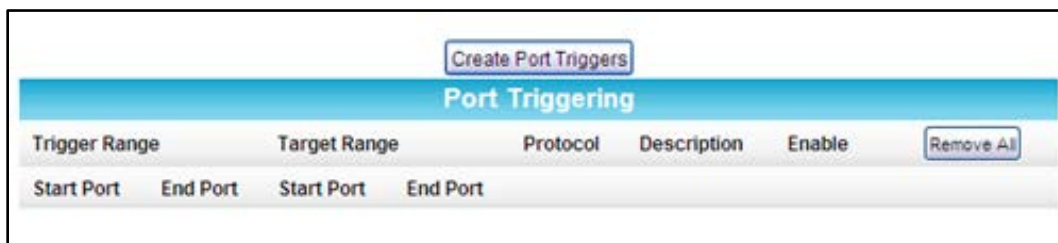
**Figure 51 – Advanced Port Filtering Screen**

**Table 14: Advanced Port Filtering -Field Descriptions**

Field	Description
<b>Start Port</b>	The starting port number of the Port Filtering range.
<b>End Port</b>	The ending port number of the Port Filtering range.
<b>Protocol</b>	Select <b>TCP</b> , <b>UDP</b> , or <b>BOTH</b> from the drop-down list.
<b>Enabled</b>	Select to activate or deselect to deactivate the selected IP port triggers.

## Port Triggers

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



**Figure 52 – Advanced Create Port Triggers Screen**

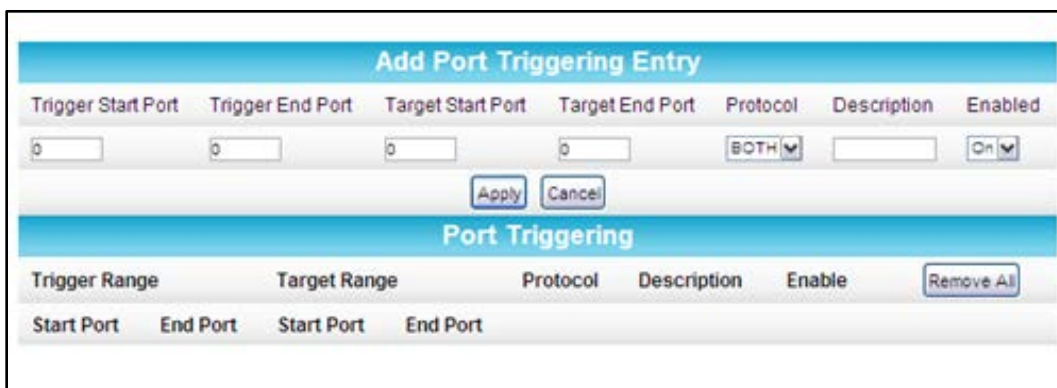


Figure 53 – Advanced Port Triggers Screen

Table 15: Advanced Port Triggers -Field Descriptions

Field	Description
<b>Trigger Start Port</b>	The starting port number of the Port Trigger range.
<b>Trigger End Port</b>	The ending port number of the Port Trigger range.
<b>Target Start Port</b>	The starting port number of the Port Target range.
<b>Target End Port</b>	The ending port number of the Port Target range.
<b>Protocol</b>	Select <b>TCP</b> , <b>UDP</b> , or <b>BOTH</b> from the drop-down list.
<b>Description</b>	Name the port trigger.
<b>Enabled</b>	Select <b>On</b> or <b>Off</b> to activate or deactivate the selected IP port triggers.

## Port Forwarding

Port forwarding allows you to run a publicly accessible server on your home network by specifying the mapping of TCP/UDP ports to a local computer. This enables incoming requests on specific port numbers to reach web servers, FTP servers, mail servers, etc. so that they can be accessible from the Internet.

To map a port, you must enter the range of port numbers that want forwarded locally and the IP address to which traffic to those ports should be sent. If you only want a single port specification, enter the same port number in the start and end locations for that IP address.

A table of commonly used port numbers is also displayed on the page for your convenience. These are some of the ports used by common applications:

Commonly Forwarded Ports	
Battle.net.....	6112 / TCP
BitTorrent.....	6881-6999 / Both
Call of Duty.....	28960 / UDP
eMule.....	4662 / TCP
eMule.....	4672 / UDP
GameSpy Arcade.....	6500 / TCP
Gnutella.....	6346-6347 / Both
Half-Life.....	27015 / Both
Halo.....	2302 / UDP
Internet Radio.....	8000 / Both
IRC.....	6665-6669 / TCP
MS Media Server....	1755 / Both
Playstation 3.....	80 / TCP
Playstation 3.....	3478 / UDP
Playstation 3.....	443 / TCP
Playstation 3.....	3479 / UDP
Playstation 3.....	5223 / TCP
Playstation 3.....	3658 / UDP
Quicktime.....	6970 / UDP
Second Life.....	12035-12036 / UDP
Slingbox.....	5001 / UDP
Steam.....	1725 / UDP
Steam Friends.....	1200 / UDP
Synergy.....	24800 / TCP
TeamSpeak.....	8767 / UDP
Ventrillo.....	3784-3785 / Both
War of Warcraft....	3724 / Both
XBOX 360.....	80 / TCP
XBOX 360.....	88 / UDP

Figure 54 – Commonly Used Port Forwarding Port Numbers List

IPv4 Entry

External IP Address & Start/End Port	Local IP Address & Start/End Port	Description	Protocol	Enabled
<input style="width: 100%;" type="text" value="0.0.0.0"/> <input style="width: 20px;" type="text" value="0"/> <input style="width: 20px;" type="text" value="0"/> <small>0.0.0.0 is the default value (IP Address) that allows packets from any device on the internet to be forwarded to the configured ports</small>	<input style="width: 100%;" type="text" value="0.0.0.0"/> <input style="width: 20px;" type="text" value="0"/> <input style="width: 20px;" type="text" value="0"/> <input style="width: 100%;" type="text" value="Commonly Forwarded Ports"/>	<input style="width: 100%;" type="text"/>	TCP ▾	Off ▾
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

Forwarded Ports

External IP Address & Start/End Port	Local IP Address & Start/End Port	Description	Protocol	Forwarding
				<input type="button" value="Remove All"/>

Figure 55 – Advanced Port Forwarding Screen

**Table 16: Advanced Port Forwarding-Field Descriptions**

Field	Description
<b>External IP Address &amp; Start/End Port</b>	Single port: Remote IP address and a specific port number (enter the same port number in the Start and End Port fields). Range of ports: Remote IP address and a specific range of port numbers (enter the first and last port numbers of the desired port range in the Start and End Port fields).
<b>Local IP Address &amp; Start/End Port</b>	Single port: IP address of the local computer or device and a specific port number (enter the same port number in the Start and End Port fields). Range of ports: IP address of the local computer or device and a specific range of port numbers (enter the first and last port numbers of the desired port range in the Start and End Port fields).
<b>Description</b>	Name of the forwarded port.
<b>Protocol</b>	Select <b>TCP</b> , <b>UDP</b> , or <b>Both</b> for the Internet protocol.
<b>Enabled</b>	Select <b>On</b> or <b>Off</b> to enable or disable port forwarding on the selected port(s).
<b>Commonly Forwarded Ports</b>	List of port numbers used by common applications.

## DMZ Host

You can configure one computer on your home network as the DMZ Host. That computer will operate outside of the SBG6400 firewall. This feature allows you to set up a separate subnetwork for remote access from the Internet to your computer, gaming devices, or other IP-enabled device so that your home network is not exposed to hackers or other external attacks from the Internet. Outside users will only have direct access to the designated DMZ Host device and not your home network.

If you set up a computer as the DMZ Host, remember to set the IP address back to zero (0) when you are finished with the needed application, since this computer will be exposed to the Internet. Although the computer is protected from Denial of Service (DoS) attacks via the SBG6400 firewall, it is still exposed to the Internet.

**Figure 56 – Advanced DMZ Host Screen****Table 17: Advanced DMZ Host-Field Descriptions**

Field	Description
<b>DMZ Host</b>	Enter the IP address of the selected computer you are setting up as the DMZ host.

## Firewall Screens

You can configure firewall filters and alert notifications for your home network. The SBG6400 firewall protects the SBG6400 LAN from unwanted attacks and other intrusions on the Internet. Firewall protection also provides the following benefits:

- Advanced, integrated stateful-inspection firewall supporting intrusion detection, session tracking, and denial-of-service attack prevention.
- Maintains state data for every TCP/IP session on the OSI network and transport layers.
- Monitors all incoming and outgoing packets, applies the firewall policy to each one, and screens for improper packets and intrusion attempts.
- Generates comprehensive notifications for the following:
  - User authentications
  - Rejected internal and external connection requests
  - Session creation and termination
  - Outside attacks (intrusion detection)

## Protection Level

The Firewall Protection Level screen has various settings related to blocking or exclusively allowing different types of data through the SBG6400 from the WAN to the LAN. There are three security firewall protection levels which correspond to how many services are allowed:

- **Off** - No security, highest risk
- **Low** - Minimum security, higher risk
- **Medium** - Common configuration, modest risk
- **High** - Safest configuration, highest security

Firewall protection enables the Stateful Packet Inspection (SPI) firewall features. Block Fragmented IP packets prevent all fragmented IP packets from passing through the firewall. Port Scan Detection detects and blocks port scan activity originating on both the LAN and WAN. IP Flood Detection detects and blocks packet floods originating on both the LAN and WAN.

You can block Java Applets, Cookies, ActiveX controls, pop up windows, and Proxies.

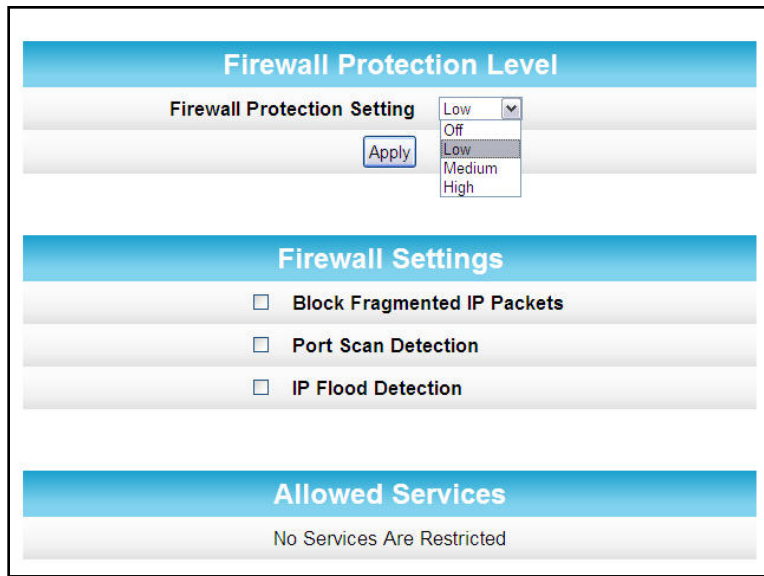


Figure 57 – Firewall Protection Level Screen

Table 18: Firewall Protection Level -Field Descriptions

Field	Description
<b>Firewall Protection Level</b>	<ul style="list-style-type: none"> <li>Select <b>Low</b>, <b>Medium</b>, or <b>High</b> to set the level of firewall protection that you want for your gateway.</li> <li>Select <b>Off</b> to disable firewall protection.</li> </ul> <p><b>Note:</b> If you choose to disable firewall protection, your computer(s) and other Ethernet-enabled devices on your home network will be at risk for possible attacks from viruses and hackers.</p>
<b>Firewall Settings</b>	<ul style="list-style-type: none"> <li>Checkmark to enable each filter that you want to set for the firewall.</li> <li>Click <b>Apply</b>, when done.</li> </ul>
<b>Allowed Services</b>	Listing of the websites you selected to allow access to from your home network.



## Parental Control

You can use the Parental Control screen to set up user access restrictions on a specific device connected to your SBG6400 network. You can set up the following Parental Controls:

- Allow or block access to specific Internet sites.
- Allow or block access to specific MAC addresses.
- Allow or block Internet access based on specific day and time settings.
- Enable or disable Internet session duration timers to limit the amount of time for Internet access.

**Note:** When creating Parental Control access filters, remember to assign the Start and End ports. Otherwise, any filters without assigned ports will apply to all ports. This also applies to MAC addresses.

Before creating filters, please scroll down and set the time zone.

**Display Filters**

Description	MAC Address	URL	Days	Time Start	Time End	Port Start	Port End	Prot	Allow/Block	Enabled	<input type="button" value="Remove All"/>

**Time Zone**

Current Time	17:35:45 6/30/2014 <small>(Network Time Not Available, Utilizing Time Provided by Cable Operator)</small>
Current Time Zone	<input type="text" value="Select a Time Zone"/>
Automatically adjust for Daylight Saving Time	<input type="radio"/> Yes <input checked="" type="radio"/> No

**Figure 58 – Firewall Parental Control-Set Time Zone Screen**

**Table 19: Firewall Parental Control-Set Time Zone-Field Descriptions**

Field	Description
<b>Current Time</b>	Enter the current time.
<b>Current Time Zone</b>	Select your time zone.
<b>Automatically adjust for Daylight Saving Time</b>	Select <b>Yes</b> or <b>No</b> if you want the time to change for Daylight Saving Time.

Figure 59 – Firewall Parental Control Screen

Table 20: Firewall Parental Control -Field Descriptions

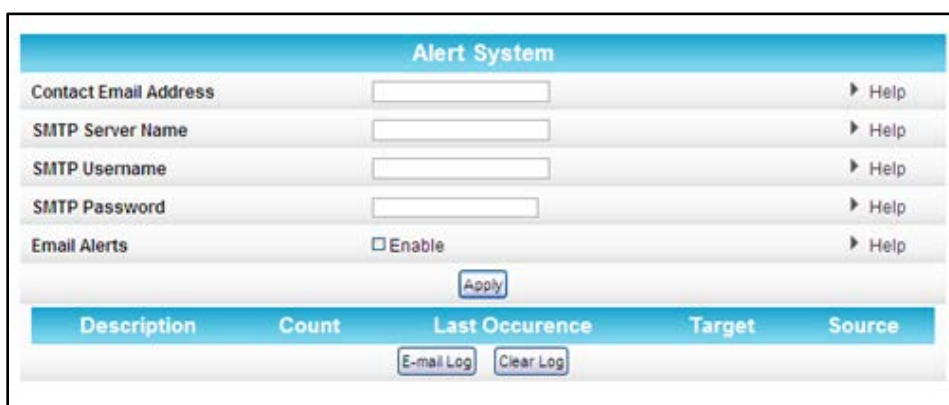
Field	Description
<b>Description</b>	Enter a name to create a new user profile.
<b>MAC Address</b>	Enter the 12-digit (hexadecimal) hardware address of the device that you are setting up for parental controls. The MAC address is assigned by the hardware manufacturer and should be located on the device label.
<b>URL</b>	Enter the web address of the Internet site that you want to block or access.
<b>Start Port</b>	Enter the starting port number of the range of ports for which you want to block incoming or outgoing access. Default port is 0.

Field	Description
<b>End Port</b>	Enter the ending port number of the range of ports for which you want to block incoming or outgoing access. Default port is 0.
<b>Protocol</b>	Select <b>TCP</b> , <b>UDP</b> , or <b>Both</b> for the Internet protocol.
<b>Days</b>	Select the days of the week that the selected user can access the Internet.
<b>Time</b>	Set the start and end time of day that the selected user can access the Internet.
<b>Allow/Block</b>	Set to allow or block Internet access for the time defined above.
<b>Enabled</b>	Turn ON or OFF this Parental Control restriction.
<b>Time Zone</b>	Update the related time information for your location.

## Local Log

You can use either of the following two formats to send your firewall event log notifications:

- Individual e-mail alerts sent out automatically each time the firewall is under attack
- Local log stored within the gateway and displayed in table form on the Local Log page



**Figure 60 – Firewall Local Log Screen**

**Table 21: Firewall Local Log -Field Descriptions**

Field	Description
<b>Contact Email Address</b>	Your email address
<b>SMTP Server Name</b>	Name of the email Simple Mail Transfer Protocol (SMTP) server  The firewall page requires the name of your email server for sending a firewall log to your email address. You can obtain the SMTP server name from your service provider.

Field	Description
<b>SMTP Username</b>	Your user name for your email account. Check with your email service provider.
<b>SMTP Password</b>	Your user password for your email account. Check with your email service provider.
<b>Email Alerts</b>	Enable or disable emailing firewall alerts.

## Remote Log

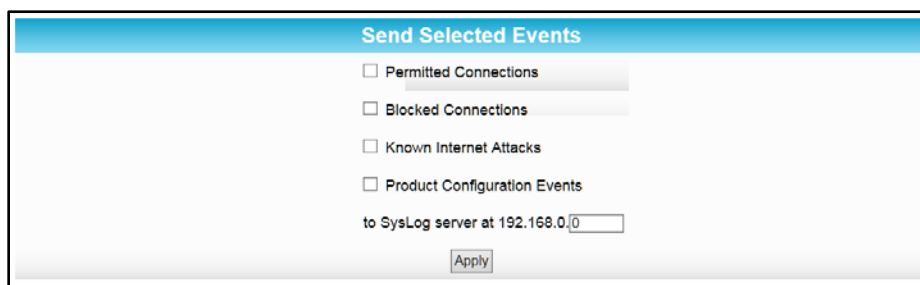
You can send firewall attack reports out to a standard SysLog server, so that many instances can be logged over a long period of time. You can select individual attack or configuration items to send to the SysLog server so that only the items of interest will be monitored.

There are four types of Firewall reports that you can monitor and log:

- **Permitted Connections** – Select to notify the server to send you email logs identifying who is connecting to your network.
- **Blocked Connections** – Select to notify the server to send you email logs identifying who was blocked from connecting to your network.
- **Known Internet Attacks** – Select to notify the server to send you email logs of known Internet attacks against your network.
- **Product Configuration Events** – Select to notify the server to send you email logs of the basic product configuration events logs.

The SysLog server must be on the same network as the Private LAN behind the Configuration Manager (typically 192.168.0.x).

To activate the SysLog monitoring feature, check all desired event types to monitor and enter the last byte of the IP address of the SysLog server. Normally, the IP address of this SysLog server is hard coded so that the address always agrees with the entry on this page.



**Figure 61 – Firewall Remote Log Screen**

**Table 22: Firewall Remote Log -Field Descriptions**

<b>Field</b>	<b>Description</b>
<b>Permitted Connections</b>	Select if you want email notification of who is connecting to your network.
<b>Blocked Connections</b>	Select if you want email notification of who is blocked from connecting to your network.
<b>Known Internet Attacks</b>	Select if you want email notification of known Internet attacks against your network.
<b>Product Configuration Events</b>	Select if you want email notification of the basic product configuration events.
<b>to Syslog server at 192.168.0.x</b>	Enter the last digit(s) of your SysLog server's IP address. Possible values: <b>10</b> to <b>254</b>



# Warranty Information

SURFboard SBG6400 Wireless Cable Modem Gateway  
ARRIS Enterprises, Inc. ("ARRIS")

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

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

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

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

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

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

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

These matters are governed by the laws of the Commonwealth of Pennsylvania, without regard to conflict of laws principles and excluding the provisions of the United Nations Convention on Contracts for the International Sale of Goods.

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



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

[www.arrisi.com](http://www.arrisi.com)

365-095-26377 x.1 09/14

