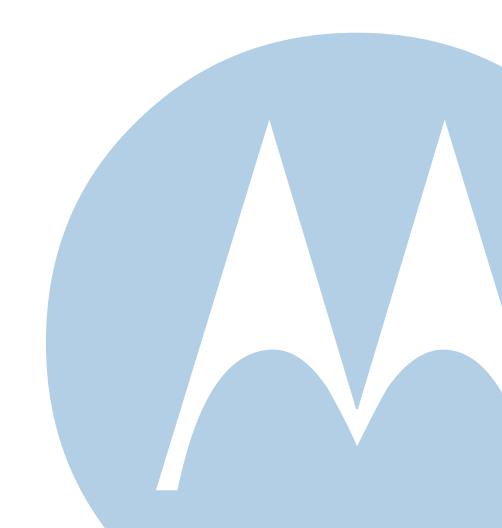**MOTOROLA**

User Guide

Motorola SURFboard®

SBG941 Series Wireless Cable Modem Gateways*

*SBG941
SBG941U
SBG941E
SBG941UE

i 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 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.

- Postpone installation until there is no risk of thunderstorm or lightning activity in the area.

- 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.

- 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.
- 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.
- 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 40° C.

SAVE THESE INSTRUCTIONS

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

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 and Revision G), as defined and approved by the Institute of Electrical and 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 Setting Up Your Wireless LAN or visit the Motorola website.

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 Motorola 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.

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.

This device is designed to operate with two internal antennas as part of the printed wiring board. The top facing antenna has a maximum gain of 2dBi and the front facing antenna has a maximum gain of 4dBi.

To reduce potential radio interference to other users, the antenna types and their gains were so chosen that the equivalent isotropically radiated power (e.i.r.p) is not more than that permitted for successful communications.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

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 (8 inches) between the radiator and your body.

Caring for the Environment by Recycling

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

Recycling your Motorola 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. If collection systems are not available, call Motorola Customer Service for assistance. Please visit www.motorola.com/recycle for instructions on recycling.

International Declaration of Conformity

We, Motorola, Inc., 101 Tournament Drive, Horsham, PA 19044, U.S.A., declare under our sole responsibility that the SBG941 SURFboard Wireless Cable Modem Gateway Series to which this declaration relates is in conformity with one or more of the following standards:

EN60950-1	EN 300 328	EN 301 489-1/-17
EN61000-3-2	EN61000-3-3	EN50385

The following provisions of the Directive(s) of the Council of the European Union:

- EMC Directive 2004/108/EC
- Low Voltage Directive 2006/95/EC
- R&TTE 1999/5/EC

Contents

Tables

Figures

1   Introduction

The Motorola SBG941 Wireless Cable Modem Gateway can be used in households with one or more computers capable of wireless and/or wired connectivity.

This guide provides product overview and setup information for the SBG941. It also provides instructions for installing the cable modem and configuring the wireless, Ethernet, router, DHCP, and security settings.

Note: All references to the SBG941 used throughout this guide also apply to the SBG941U, SBG941E, and SBG941UE, unless noted otherwise. All SBG941U references also apply to the SBG941UE unless noted otherwise.

Inside the Box

Before installing the SBG941, verify that the following items are included in the box. If you obtained the modem from your service provider, some of the included items may be different.

Item		Description
Power supply		Provides power via an AC electrical outlet
10/100Base-T Ethernet cable		Standard Cat 5, or higher, cable for connecting to the network
Software License & Regulatory Card		Contains software license, warranty, and safety information for the SBG941
SBG941U Installation CD-ROM		Contains the SBG941U Installation Assistant, and this user guide *Included with SBG941U models only.*
SBG941 Install Sheet		Provides basic information for setting up the SBG941

You will need a 75-ohm coaxial cable with F-type connectors to connect the SBG941 to the nearest cable outlet. If a TV is connected to the cable outlet, you may need a 5 to 900 MHz RF splitter and two additional coaxial cables to use the TV and SBG941.

Note: *This product is also designed for IT power systems with phase to phase voltage 230VAC input.*

Minimum System Requirements

The SBG941 is compatible with the following operating systems:

- Windows XP Service Pack 2 or later
- Windows Vista Service Pack 1 or later
- MAC 10.4

Contact Information

For information about Motorola consumer cable products, education, and support, visit the Motorola support website at: http://broadband.motorola.com/consumers/support

2 Product Overview

Front Panel Overview

The SBG941 front panel contains indicator lights and the **WPS** button, which is used to configure a Wi-Fi Protected Security (WPS)-enabled device so that it automatically connects to the SBG941 wireless network.
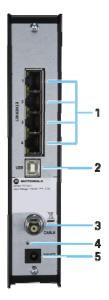
The SBG941 front panel LED indicators provide the following status information for power, communications, and errors:

	LED	Flashing	On
1	POWER	Not applicable — LED does not flash	**Green**: Power is properly connected
2	RECEIVE	Scanning for a downstream (receive) channel connection	**Green**: Downstream channel is connected
3	SEND	Scanning for an upstream (send) channel connection	**Green**: Upstream channel is connected
4	ONLINE	Scanning for Internet connection	**Green**: Startup process completed
5	LINK	Not applicable — LED does not flash	**Green**: A device is connected to the Ethernet (10Base-T) or Fast Ethernet (100Base-T), and/or USB port.

6	WIRELESS	**Green**: Wi-Fi enabled with encrypted wireless data activity. Long/short flash indicates mobile pairing in progress. **Amber**: Wi-Fi enabled with unencrypted wireless data activity.	**Green**: Wireless pairing successfully established between the SBG941 and another Wi-Fi enabled device on your network — printer, PDA, laptop, etc. **Amber**: Mobile pairing was successful. LED turns green after five minutes.
7	WPS START	Not applicable — LED does not flash	**Green**: WPS button is pressed and Wi-Fi Protected Security is activated. LED will remain on until WPS button is released.

Rear Panel Overview

Both the SBG941 and SBG941U (shown above) rear panels contain the following cabling port and connectors:

	Item	Description
1	**ETHERNET** **1 2 3 4**	Ethernet-ports: **Activity LED** — Green LED defines the activity of the Ethernet connector • LED is ON — Indicates a 100Base-T negotiated data rate • LED is FLASHING — Indicates activity is detected on the port • LED is OFF — Indicates the unit is not powered or there is no 100Base-T Ethernet connection

	ETHERNET **1 2 3 4** **(continued)**	**10/100 LED** — Indicates the connection data rate • Green LED is ON — Indicates a 100Base-T data connection • Amber LED is ON — Indicates a 10Base-T negotiated data rate • Amber LED is FLASHING — Indicates there is activity on the Ethernet connection when in 10Base-T rate • Amber LED is OFF— Indicates the device is not powered on or there is no 10Base-T connection
2	**USB**	For Windows only, used for connecting a PC to the SBG941U. You cannot connect a Macintosh or UNIX® computer to the USB port on the SBG941U. Front panel **LINK LED** will turn ON when a USB device is connected and a link is established *USB connector is available on SBG941U models only.*
3	**CABLE**	Coaxial cable connector
4	**RESET**	Resets the cable modem which may take from five to 30 minutes
5	**POWER**	+12VDC power connector

MAC Label Overview

The SBG941 Media Access Control (MAC) label contains the MAC address which is a unique, 48-bit value that identifies each Ethernet network device. To receive data service, you need to provide the MAC address marked **HFC MAC ID** to your Internet Service provider.

3 Installing the Modem

This section provides information on setting up and installing the SBG941 wireless gateway. For information on the WLAN setup, see Setting Up Your Wireless LAN.

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

Cabling the SBG941

Before starting, power on your computer and check that the SBG941 is unplugged.

1. Connect the coaxial cable to the cable outlet or splitter.
2. Connect the other end of the coaxial cable to the cable connector on the modem. Hand-tighten the connectors to avoid damaging them.
3. Plug the power cord into the Power port on the modem.
4. Plug the other end of the power cord into an electrical wall outlet.
   The first time you plug in the modem, allow 5 to 30 minutes to find and lock on the appropriate communications channels.
5. Connect the Ethernet cable to the Ethernet port on the computer.
6. Connect the other end of the Ethernet cable to the Ethernet port on the modem.
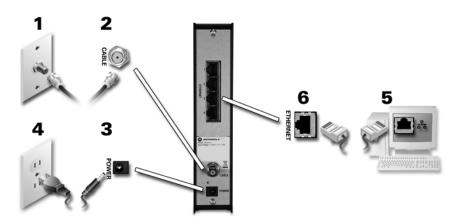
Figure 1 – Cabling the SBG941

7. Check that the LEDs on the front panel cycle through the following sequence:

Table 1 – SBG941 LED Activity During Startup

LED	Description
POWER	Turns on when AC power is connected to the modem. Indicates that the power is connected properly.
RECEIVE	Flashes while scanning for the downstream receive channel. Changes to solid green when the receive channel is locked.
SEND	Flashes while scanning for the upstream send channel. Changes to solid green when the send channel is locked.
ONLINE	Flashes during the modem registration and configuration. Changes to solid green when the modem is registered.

Cabling the SBG941U

CAUTION	*Before plugging in the USB cable on the SBG941U, load the SBG941U Installation CD-ROM in the CD-ROM drive.* *Do not connect the Ethernet and USB cables on the same computer at any time.*

Before starting, power on your computer and check that the SBG941U power cord is unplugged.

1. Load and run the SBG941U Installation CD-ROM and install the applicable USB driver.
2. Connect one end of the coaxial cable to the cable outlet or splitter.
3. Connect the other end of the coaxial cable to the cable connector on the modem. Hand-tighten the connectors to avoid damaging them.
4. Plug the power cord into the power port on the modem.
5. Plug the other end of the power cord into an electrical wall outlet.

   The first time you plug in the modem, allow it 5- to 30 minutes to find and lock on the appropriate communications channels.
6. Connect the USB or Ethernet cable to the appropriate port on your computer.
7. Connect the other end of the USB or Ethernet cable to the appropriate port on the modem.
8. Check that the LEDs on the front panel cycle through the proper sequence, see Table 1 – SBG941 LED Activity During Startup.
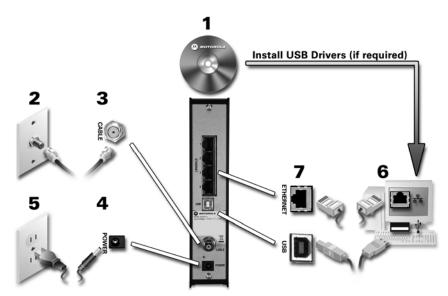
Figure 2 – Cabling the SBG941U

Connecting to the Internet

After installing the modem, check that you can connect to the Internet. You can retrieve an IP address for your computer's network interface using one of the following options:

- Retrieve the statically-defined IP address and DNS address

- Automatically retrieve the IP address using the Network DHCP server

The modem provides a DHCP server on its LAN. Motorola recommends that you configure your LAN to obtain the IPs for the LAN and DNS server automatically.

Make sure all computers on your LAN are configured for TCP/IP. After configuring TCP/IP on your computer, you should verify the IP address.

Note*: For UNIX or Linux systems, follow the instructions in the applicable user documentation.*

Configuring TCP/IP in Windows XP

1. Open the **Control Panel**.
2. Double-click **Network Connections** to list the Dial-up and LAN or High-Speed Internet connections.
3. Right-click the network connection for your network interface.

4. Select **Properties** from the drop-down menu to display the Local Area Connection Properties window. Be sure Internet Protocol (TCP/IP) is checked.
5. Select **Internet Protocol (TCP/IP)** and click **Properties** to display the Internet Protocol (TCP/IP) Properties window.
6. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
7. Click **OK** to save the TCP/IP settings and exit the TCP/IP Properties window.
8. Close the Local Area Connection Properties window and then exit the Control Panel.
9. When you complete the TCP/IP configuration, go to Verifying the IP Address in Windows XP.

Configuring TCP/IP in Windows Vista

1. Open the **Control Panel**.
2. Double-click **Network and Internet** to display the Network and Internet window.
3. Double-click **Network and Sharing Center** to display the Network and Sharing Center window.
4. Click **Manage network connections** to display the LAN or High-Speed Internet connections window.
5. Right-click the network connection for your network interface.
6. Select **Properties** to display the Local Area Connection Properties window.

    Vista may prompt you to allow access to the Network Properties Options. If you see the prompt, `User Account Control -- Windows needs your permission to continue`, click **Continue**.
7. Select **Internet Protocol Version 4 or 6 (TCP/IPv4** or **v6)** and click **Properties** to display the Internet Protocol Properties window.
8. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
9. Click **OK** to save the TCP/IP settings and close the Internet Protocol Version 4 (TCP/IPv4) Properties window.
10. Click **OK** to close the Local Area Connection Properties window.
11. Close the remaining windows and exit the Control Panel.
12. When you complete the TCP/IP configuration, go to Verifying the IP Address in Windows Vista.

Verifying the IP Address in Windows XP

To check the IP address:

1. On the Windows Desktop, click **Start**.
2. Select **Run**. The Run window is displayed.
3. Type **cmd** and click **OK.**
4. Type **ipconfig** and press **ENTER** to display your IP configuration.

If an Autoconfiguration IP address is displayed, that indicates possible broadband network problems or an improper connection between your computer and the SBG941. The Autoconfiguration IP address, ranging from **169.254.0.0** to **169.254.255.255**, is reserved for Automatic Private IP Addressing (APIPA).

This can occur if the modem is configured to automatically obtain an IP address from a Dynamic Host Configuration Protocol (DHCP) server. When Auto-configuration is enabled, Windows will automatically assign an IP address if the cable modem gateway is unable to obtain one. Because this automatically assigned IP address is not valid, you will not be able to access the Internet using the cable modem gateway.

Check the following:

- Your cable connections
- Whether you can see cable-TV channels on your television

After successfully verifying your cable connections and proper cable-TV operation, you can renew your IP address.

Verifying the IP Address in Windows Vista

Do the following to verify the IP address:

1. On the Windows Desktop, click **Start**.
2. Click **All Programs**.
3. Click **Accessories**.
4. Click **Run** to display the Run window.
5. Type **cmd** and click **OK** to open a command prompt window.
6. Type **ipconfig** and press **ENTER** to display the IP Configuration.

If an Auto-configuration IP address is displayed, that indicates possible broadband network problems or an improper connection between your computer and the SBG941. The Auto-configuration IP address, ranging from **169.254.0.0** to **169.254.255.255**, is reserved for Automatic Private IP Addressing (APIPA).

Renewing Your IP Address in Windows XP or Windows Vista

1. Open a command prompt window.
    A. From the Windows Taskbar, click **Start** to open the Start menu.
    B. Select **Run** to open the Run window.
    C. Type `cmd` in the Open entry box and click **OK**.
2. Type `ipconfig /renew` and press `ENTER`. A valid IP address should appear indicating that Internet access is available.
3. Type `exit` and press `ENTER` to close the command prompt window.

If, after performing this procedure, your computer cannot access the Internet, call your cable provider for help.

Setting Up a Wi-Fi Network

Do the following to set up a Wi-Fi network using the WPS button on the modem:

1. If necessary, power on the modem.
2. Power on the WPS-enabled devices you want to have access to the network, such as a PC or router.

    The Wi-Fi network will automatically detect the WPS devices.
3. Press **WPS** button on the modem.
4. If applicable, press **WPS** button on the other WPS devices.
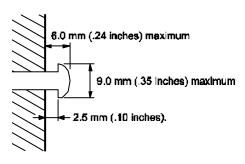
Wall Mounting the Modem

If you choose to wall mount the modem, do the following before starting:

*   Locate the unit as specified by the local or national codes governing residential or business cable TV and communications services.
*   Follow all local standards for installing a network interface unit/network interface device (NIU/NID).
*   Make sure the AC power plug is disconnected from the wall outlet and all cables are removed from the back of the modem before starting the installation.
*   Determine if you are mounting the modem horizontally or vertically.
*   Use M3.5 x 38 mm (#6 x 1½ inch) screws with a flat underside and maximum screw head diameter of 9.0 mm to mount the modem.

    See the screw mounting dimensions below to properly mount the modem:

6.0 mm (.24 inches) maximum

9.0 mm (.35 inches) maximum

2.5 mm (.10 inches).

If possible, mount the modem to concrete, masonry, a wooden stud, or some other solid wall material. Use anchors if necessary (for example, if you must mount the unit on drywall).

CAUTION	Before drilling holes, check the structure for potential damage to water, gas, or electrical lines.

1. Drill the holes to a depth of at least 1½ inches (3.8 cm).
   There must be .10 inches (2.5 mm) between the wall and the underside of the screw head.
2. After mounting, reconnect the coaxial cable and re-plug the power cord.
3. Properly route the cables to avoid any safety hazards.
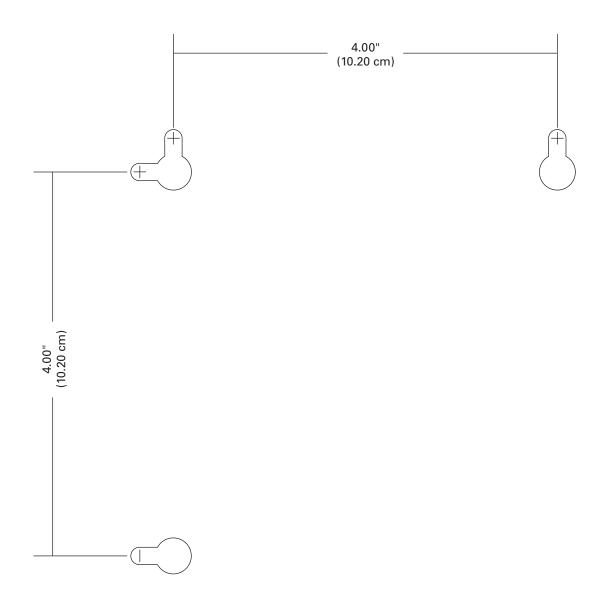
Wall Mounting Template

You can print the following page to use as a wall mounting template.

After mounting the modem, do the following:

1. Reconnect the coaxial cable input and Ethernet connection.
2. Plug the power cord into the +12VDC Power connector on the modem and the electrical outlet.
3. Arrange the cables appropriately to prevent any safety hazards.

4.00"
(10.20 cm)

4.00"
(10.20 cm)

4 Basic Configuration

For more advanced configuration information, see Connecting to the Internet and Setting Up Your Wireless LAN.

For normal operation, you do not need to change most default settings. The following caution statements summarize the issues you must be aware of:

CAUTION   *To prevent unauthorized configuration, change the default password immediately when you first configure the SBG941. See Changing the SBG941 Default Password.*
Firewalls are not foolproof. Choose the most secure firewall policy you can. See Firewall Pages.

Starting the SBG941 Configuration Manager (CMGR)

Note: *Do not attempt to configure the SBG941 over a wireless connection.*

Use the SBG941 Configuration Manager (CMGR) to change and view settings on your SBG941.
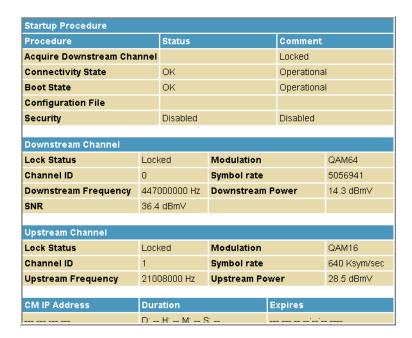
If the modem was obtained as part of a service package, your service provider may have alternative configuration methods. If you cannot access any of the SBG941 HTML pages, please contact your service provider.

1. Open the web browser on a computer connected to the modem over an Ethernet connection.
2. In the Address or Location field of your browser, type **http://192.168.0.1** and press **ENTER**.
3. Type **admin** in the Username field (this field is case-sensitive).
4. Type **motorola** in the Password field (this field is case-sensitive).

Login

Login
Please enter username and password to login.

Username ●●●●●
Password ●●●●●●●
[Login]

---

5. Click **Login** to display the SBG941 Status Connection page.

Startup Procedure		
Procedure	**Status**	**Comment**
Acquire Downstream Channel		Locked
Connectivity State	OK	Operational
Boot State	OK	Operational
Configuration File		
Security	Disabled	Disabled

Downstream Channel			
Lock Status	Locked	**Modulation**	QAM64
Channel ID	0	**Symbol rate**	5056941
Downstream Frequency	447000000 Hz	**Downstream Power**	14.3 dBmV
SNR	36.4 dBmV		

Upstream Channel			
Lock Status	Locked	**Modulation**	QAM16
Channel ID	1	**Symbol rate**	640 Ksym/sec
Upstream Frequency	21008000 Hz	**Upstream Power**	28.5 dBmV

CM IP Address	Duration	Expires
--- --- --- ---	D: -- H: -- M: -- S: --	--- --- -- --:--:-- ----

The Status Connection page provides the following status information on the network connection of the SBG941:

o RF Downstream Channel, which uses lower cable frequencies to transmit data

o RF Upstream Channel, which uses higher cable frequencies to receive data

6. Click the **Refresh** button in your web browser any time you want to refresh the information on this page.

If you have any problems starting the SBG941 Configuration Manager (CMGR), see Troubleshooting for more information.

Changing the SBG941 Default Password

From the SBG941 Status page, click **Security** submenu option to change the default password. Complete each field, then click **Apply** when done to save your changes.
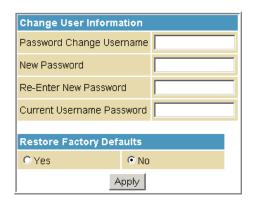
• For the password change username, type a new user name.

• The password is case-sensitive.

• For the current username password, type your old password.

- Select **Yes** or **No** to reset the user name and password to the default factory settings.

  Note: *You must login with the default user name,* `admin`*, and password,* `motorola,` *after applying this change. All entries are case-sensitive.*

SBG941 Menu Options Bar

The SBG941 Menu Options bar is displayed along the top of the SBG941 Configuration Manager window. When a menu option is selected, a top-level page for that option is displayed.

Configuration Manager Menu Options Bar

Menu Option Pages	Function
Status	Provides information about the SBG941 hardware and software, MAC address, cable modem IP address, serial number, and related information. Additional pages provide diagnostic tools and allow you to change your SBG941 user name and password.
Basic	Views and configures SBG941 IP-related configuration data, including Network Configuration, WAN Connection Type, DHCP, and DDNS. The Backup option allows you to save your SBG941 configuration on your computer.
Advanced	Configures and monitors how the SBG941 routes IP traffic
Firewall	Configures and monitors the SBG941 firewall

Parental Control	Configures and monitors the SBG941 parental control feature
Wireless	Configures and monitors SBG941 wireless networking features
Logout	Exits the SBG941 Configuration Manager

CAUTION   *To prevent unauthorized configuration, immediately change the default password when you first configure your Motorola SBG941.*

Getting Help

To retrieve help information for any menu option, click **help** on that page. You can use the Windows scroll bar to view additional items on the help screens. See the sample Firewall help page shown below.

Gaming Configuration Guidelines

The following provides information about configuring the SBG941 firewall and DMZ for gaming.

Configuring the Firewall for Gaming

By default, the SBG941 firewall is enabled. As recommended, if you keep the firewall enabled, refer to the game's documentation to ensure that the necessary ports are open for use by that game.

The pre-defined SBG941 firewall policies affect Xbox LIVE® as follows:

- On the Firewall Web Content Filter Page, you may need to disable Firewall Protection and IP Flood Detection.

Configuring Port Triggers

Because the SBG941 has pre-defined port triggers for games using any of the following applications, no user action is required to enable them:

- ALG for MSN
- MSN Games by Zone.com

You may need to create custom port triggers to enable other games to operate properly. To create custom port triggers, see the Advanced Port Triggers Page.

Configuring a Gaming DMZ Host

CAUTION   *The gaming DMZ host is not protected by the firewall. It is open to communication or hacking from any computer on the Internet. Consider carefully before configuring a device to be in the DMZ.*

Some games and game devices require:

- The use of random ports
- The forwarding of unsolicited traffic

For example, to connect a PlayStation®2 for PS2® online gaming, designate it as the gaming DMZ host because the ports required vary from game to game. For these games, Motorola recommends configuring the gaming computer or device as a gaming DMZ device.

To configure a gaming DMZ device, on the Basic DHCP Page:

1. Reserve a private IP address for the computer or game device MAC address.
2. Designate the device as a DMZ device.

You can reserve IP addresses for multiple devices, but only one device at a time can be designated as the gaming DMZ.

Exiting the SBG941 Configuration Manager

To logoff and close the SBG941 Configuration Manager, click **Logout** on the SBG941 Menu Options bar.

5   Status Pages

The SBG941 Status pages provide information about the SBG941 hardware and software, MAC address, cable modem IP address, serial number, and related information. You can also monitor your cable system connection. Additional pages provide diagnostic tools and allow you to change your SBG941 user name and password.

You can click any Status submenu option to view or change the status information for that option.

Status Software Page

This page displays information about the hardware version, software version, MAC address, cable modem IP address, serial number, system "up" time, and network registration status.

Information	
Standard Specification Compliant	DOCSIS 2.0
Hardware Version	1
Software Version	SBG941-2.0.0.0-BETA-00-128-DIAG
Cable Modem MAC Address	00:22:10:46:a7:86
Cable Modem Serial Number	307201835100260201028105
CM certificate	Installed
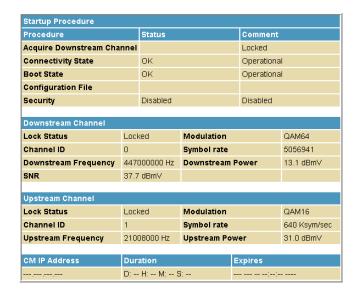
Status	
System Up Time	10 days 05h:44m:05s
Network Access	Denied
Cable Modem IP Address	---.---.---.---

Status Connection Page

This page provides the HFC and IP network connectivity status of the SBG941 cable modem.

You can click the **Refresh** button in your web browser to refresh the information on this page at any time.

Startup Procedure			
Procedure	**Status**	**Comment**	
Acquire Downstream Channel		Locked	
Connectivity State	OK	Operational	
Boot State	OK	Operational	
Configuration File			
Security	Disabled	Disabled	

Downstream Channel			
Lock Status	Locked	**Modulation**	QAM64
Channel ID	0	**Symbol rate**	5056941
Downstream Frequency	447000000 Hz	**Downstream Power**	13.1 dBmV
SNR	37.7 dBmV		

Upstream Channel			
Lock Status	Locked	**Modulation**	QAM16
Channel ID	1	**Symbol rate**	640 Ksym/sec
Upstream Frequency	21008000 Hz	**Upstream Power**	31.0 dBmV

CM IP Address	Duration	Expires
---.---.---.---	D: -- H: -- M: -- S: --	--- --- -- --:--:-- ----

Field Descriptions for the Status Connection Page

Field	Description
Startup Procedure	Startup status information about the cable modem.
Downstream Channel	Status information about the RF downstream channels, including downstream channel frequency and downstream signal power and modulation.
Upstream Channel	Status information about the RF upstream channels, including upstream channel ID and upstream signal power and modulation.

Status Security Page

This page allows you to define administrator access privileges by changing your SBG941 user name and password. It also allows you to reset your user name and password to the default setting.

Field Descriptions for the Status Security Page

Field	Description
Password Change Username	Type a new user name
New Password	Type a new password. The password is case-sensitive.
Re-Enter New Password	Type the new password again. The password is case-sensitive.
Current Username Password	Type your old password
Restore Factory Defaults	Select **Yes** or **No** to reset the user name and password to the default factory settings After restoring the factory defaults, you must login using the default user name, **admin**, and password, **motorola**.
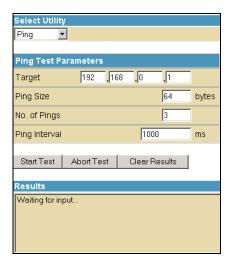
Status Diagnostics Page

This page provides the following diagnostic tools for troubleshooting IP connectivity problems:

- Ping (LAN)
- Traceroute (WAN)

Ping Utility

Ping (Packet InterNet Groper) allows you to check connectivity between the SBG941 and other devices on the SBG941 LAN. This utility sends a small packet of data and then waits for a reply. When you Ping a computer IP address and receive a reply, it confirms that the computer is connected to the SBG941.

Testing Network Connectivity with the SBG941

To check connectivity between the SBG941 and other devices on the SBG941 LAN, perform the following test:

1. Select **Ping** from the Select Utility drop-down list.
2. Enter the IP address of the computer you want to Ping in the Target field.
3. Enter the data packet size in bytes in the Ping Size field.
4. Enter the number of ping attempts in the No. of Pings field.
5. Enter the time (in milliseconds) between Ping send operations in the Ping Interval field.
6. Click **Start Test** to begin the Ping operation. Ping results display in the Results pane.
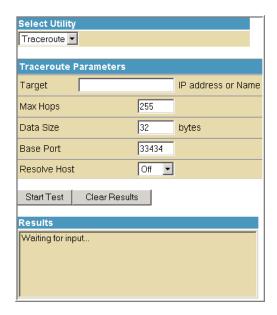
7. You can click **Abort Test** at any time during the test to stop the Ping operation.
8. Repeat steps 2 through 6 for each device you want to ping.

When done, click **Clear Results** to delete the Ping results in the Results pane.

Traceroute Utility

Traceroute allows you to map the network path from the SBG941 Configuration Manager to a public host. Selecting Traceroute from the Select Utility drop-down list presents alternate controls for the Traceroute utility.

Select Utility
Traceroute ▾

Traceroute Parameters		
Target		IP address or Name
Max Hops	255	
Data Size	32	bytes
Base Port	33434	
Resolve Host	Off ▾	

Start Test   Clear Results

Results
Waiting for input...
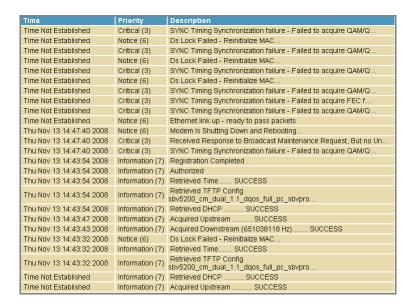
1. Enter the IP address or Host Name of the computer you want to target for the Traceroute operation in the Target field.
2. Enter the maximum number of hops that the Traceroute operation performs before stopping in the Max Hops field.
3. Enter the data packet size in bytes in the Data Size field.
4. Set the base UDP port number used by Traceroute in the Base Port field. The default is **33434**. If a UDP port is not available, this field can be used to specify an unused port range.
5. In the Resolve Host field, select **On** to list the names of hosts found during the Traceroute operation, or select **Off** to list only the hosts IP addresses.
6. After entering the Traceroute parameters, click **Start Test** to begin the Traceroute operation. The Traceroute results will display in the Results pane.

When done, click **Clear Results** to delete the Traceroute results in the Results pane.

Status Event Log Page

This page lists the critical system events in chronological order. A sample Event log is shown below:

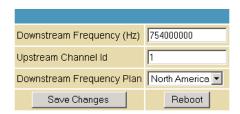| Time	Priority	Description
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...
Time Not Established	Notice (6)	Ds Lock Failed - Reinitialize MAC...
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...
Time Not Established	Notice (6)	Ds Lock Failed - Reinitialize MAC...
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...
Time Not Established	Notice (6)	Ds Lock Failed - Reinitialize MAC...
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire FEC f...
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...
Time Not Established	Notice (6)	Ethernet link up - ready to pass packets
Thu Nov 13 14:47:40 2008	Notice (6)	Modem Is Shutting Down and Rebooting...
Thu Nov 13 14:47:40 2008	Critical (3)	Received Response to Broadcast Maintenance Request, But no Un...
Thu Nov 13 14:47:40 2008	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...
Thu Nov 13 14:43:54 2008	Information (7)	Registration Completed
Thu Nov 13 14:43:54 2008	Information (7)	Authorized
Thu Nov 13 14:43:54 2008	Information (7)	Retrieved Time....... SUCCESS
Thu Nov 13 14:43:54 2008	Information (7)	Retrieved TFTP Config sbv5200_cm_dual_1.1_dqos_full_pc_sbvpro...
Thu Nov 13 14:43:54 2008	Information (7)	Retrieved DHCP .... SUCCESS
Thu Nov 13 14:43:47 2008	Information (7)	Acquired Upstream .... SUCCESS
Thu Nov 13 14:43:43 2008	Information (7)	Acquired Downstream (651038118 Hz)........ SUCCESS
Thu Nov 13 14:43:32 2008	Notice (6)	Ds Lock Failed - Reinitialize MAC...
Thu Nov 13 14:43:32 2008	Information (7)	Retrieved Time....... SUCCESS
Thu Nov 13 14:43:32 2008	Information (7)	Retrieved TFTP Config sbv5200_cm_dual_1.1_dqos_full_pc_sbvpro...
Time Not Established	Information (7)	Retrieved DHCP .... SUCCESS
Time Not Established	Information (7)	Acquired Upstream .... SUCCESS

Status Configuration Page

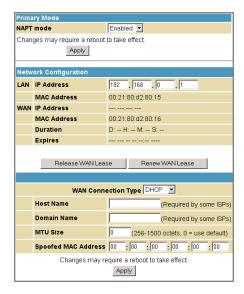|	
Downstream Frequency (Hz)	754000000
Upstream Channel Id	1
Downstream Frequency Plan	North America
Save Changes	Reboot

6

Basic Pages

The SBG941 Basic Pages allow you to view and configure SBG941 IP-related configuration data, including Network Configuration, WAN Connection Type, DHCP, and DDNS. The Backup option allows you to save a copy of your SBG941 configuration on your computer. You can click any Basic submenu option to view or change the configuration information for that option.

Basic Setup Page

This page allows you to configure the basic features of your SBG941 gateway related to your ISP connection.

Field Descriptions for the Basic Setup Page

Field	Description
NAPT mode	NAPT is a special case of NAT, where many IP numbers are hidden behind a number of addresses. In contrast to the original NAT, however, this does not mean there can be only that number of connections at a time.

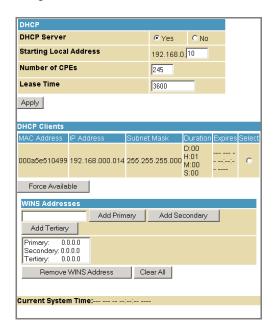|	
NAPT mode (continued)	In NAPT mode, an almost arbitrary number of connections are multiplexed using TCP port information. The number of simultaneous connections is limited by the number of addresses multiplied by the number of available TCP ports.
LAN	
IP Address	Enter the IP address of the SBG941 on your private LAN.
MAC Address	Media Access Control address — a set of 12 hexadecimal digits assigned during manufacturing that uniquely identifies the hardware address of the SBG941 Access Point.
WAN	
IP Address	The public WAN IP address of your SBG941 device, which is either dynamically or statically assigned by your ISP.
MAC Address	Media Access Control address — a set of 12 hexadecimal digits assigned during manufacturing that uniquely identifies the hardware address of the SBG941 Access Point.
Duration	Describes how long before your Internet connection expires. The WAN lease will automatically renew itself when it expires.
Expires	Displays the exact time and date the WAN lease expires.
Release WAN Lease	Click to release WAN lease.
Renew WAN Lease	Click to renew WAN lease.
WAN Connection Type	DHCP or Static IP. If your ISP uses DHCP, select **DHCP** and enter a Host Name and Domain name, if required. If your ISP uses static IP addressing, select **Static IP** and enter the information provided by your ISP for Static IP Address, Static IP Mask, Default Gateway, Primary DNS, and Secondary DNS.
Host Name	If WAN Connection Type is DHCP, enter a Host Name, if required.
Domain Name	If WAN Connection Type is DHCP, enter a Domain Name, if required.
MTU Size	Maximum Transmission Unit (MTU) is the largest size packet or frame that can be sent. The default value is suitable for most users.
Spoofed MAC Address	If WAN Connection Type is Static IP, enter the information provided by your ISP for Static IP Address, Static IP Mask, Default Gateway, Primary DNS, and Secondary DNS.

When done, click **Apply** to save your changes.

Basic DHCP Page

This page allows you to configure and view the status of the optional internal SBG941 DHCP (Dynamic Host Configuration Protocol) server for the LAN.

CAUTION	*Do not modify these settings unless you are an experienced network administrator with strong knowledge of IP addressing, subnetting, and DHCP.*

Field Descriptions for the Basic DHCP Page

| Field	Description
DHCP Server	Select **Yes** to enable the SBG941 DHCP Server. Select **No** to disable the SBG941 DHCP Server.
Starting Local Address	Enter the starting IP address to be assigned by the SBG941 DHCP server to clients in dotted-decimal format. The default is 192.168.0.2.
Number of CPEs	Sets the number of clients for the SBG941 DHCP server to assign a private IP address. There are 245 possible client addresses. The default is **245**.
Lease Time	Sets the time in seconds that the SBG941 DHCP server leases an IP address to a client. The default is 3600 seconds (60 minutes).
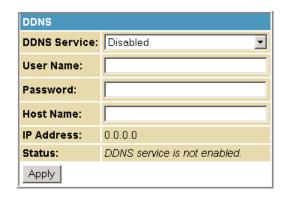
DHCP Clients	Displays DHCP client device information.
WINS Addresses	Specifies up to three Windows Internet Name Service (WINS) Server Addresses.

When done, click **Apply** to save your changes.

To renew a DHCP client IP address, choose **Select** and then click **Force Available**.

Basic DDNS Page

This page allows you to set up the Dynamic Domain Name System (DDNS) service. The DDNS service allows you to assign a static Internet domain name to a dynamic IP address, which allows your SBG941 to be more easily accessed from various locations on the Internet.

DDNS	
DDNS Service:	Disabled
User Name:	
Password:	
Host Name:	
IP Address:	0.0.0.0
Status:	*DDNS service is not enabled.*
Apply	

Field Descriptions for Basic DDNS Page

Field	Description
DDNS Service	Select **Disable** or **wwwDynDNS.org** to enable the DDNS Service.
User Name	Enter your DynDNS user name.
Password	Enter your DynDNS password.
Host Name	Enter your DDNS host name.
IP Address	Lists IP information.
Status	Displays the DDNS service status: **enabled** or **disabled**

When done, click **Apply** to save your changes.

Basic Backup Page

This page allows you to save your current SBG941 configuration settings locally on your computer or restore previously saved configurations.

Field Descriptions for the Basic Backup Page

Field	Description
Restore	Lets you restore a previously saved configuration.
Backup	Lets you create a backup copy of the current configuration.

Restoring Your SBG941 Configuration

1. Type the path with the file name where the backup file is located on your computer, or click **Browse** to locate the file.
2. Click **Restore** to recreate your previously saved SBG941 settings.

Backing Up Your SBG941 Configuration

1. Type the path with the file name where you want to store your backup file on your computer, or click **Browse** to locate the file.
2. Click **Backup** to create a backup of your SBG941 settings.

<table>
<tr><td></td><td>**7**</td><td></td><td>**Advanced Pages**</td></tr>
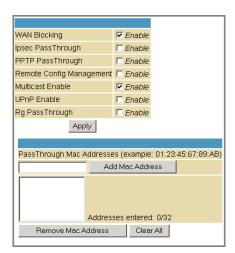</table>

The SBG941 Advanced Pages allow you to configure the advanced features of the SBG941:

- IP Filtering
- MAC Filtering
- Port Filtering
- Port Forwarding
- Port Triggers
- DMZ Host
- Routing Information Protocol (RIP) Setup

You can click any Advanced submenu option to view or change the advanced configuration information for that option.

Advanced Options Page

This page allows you to set the operating modes for adjusting how the SBG941 device routes IP traffic.

Field Descriptions for the Advanced Options Page

Field	Description
WAN Blocking	Prevents the SBG941 Configuration Manager or the PCs behind it from being visible to other computers on the SBG941 WAN. Select **Enable** to turn on this option.
IPsec PassThrough	Enables the IPsec Pass-Through protocol to be used through the SBG941 Configuration Manager so that a VPN device (or software) may communicate properly with the WAN. Select **Enable** to turn on this option.
PPTP PassThrough	Enables the Point-to-Point Tunneling Protocol (PPTP) Pass-Through protocol to be used through the SBG941 Configuration Manager so that a VPN device (or software) may communicate properly with the WAN. Select **Enable** to turn on this option.
Remote Config Management	Allows remote access to the SBG941 Configuration Manager. For example, in the browser URL window, type **http://WanIPAddress:8080/** to access the SBG941 Configuration Manager remotely. Select **Enable** to turn on this option.
Multicast Enable	Allows multicast-specific traffic (denoted by a specific address) to be passed to and from the PCs on the private network behind the configuration manager. Select **Enable** to turn on this option.
UPnP Enable	Turns on the Universal Plug and Play protocol (UPnP) agent in the configuration manager. If you are running a CPE (client) application that requires UPnP, select this box. Select **Enable** to turn on this option.
Rg PassThrough	Disables NAT operation allowing all client computers to act as passthrough clients. Select **Enable** to turn on this option.
PassThrough Mac Addresses	Specifies up to 32 computers as passthrough clients not subject to NAT, using their MAC addresses. To enable this feature, your cable operator may need to provide additional public IP addresses.

When done, click **Apply** to save your changes.

Advanced IP Filtering Page

This page allows you to define which local PCs will be denied access to the SBG941 WAN. You can configure IP address filters to block Internet traffic to specific network devices on the LAN by entering starting and ending IP address ranges.

Note: Only enter the LSB (Least-significant byte) of the IP address; the upper bytes of the IP address are set automatically from the IP address for the SBG941 Configuration Manager.

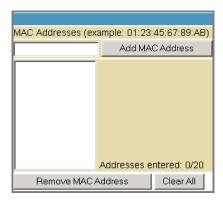**Field Descriptions for the Advanced IP Filtering Page**

Field	Description
Start Address	Enter the starting IP address range of the computers for which you want to deny access to the SBG941 WAN. Only enter the least significant byte of the IP address.
End Address	Enter the ending IP address range of the computers you want to deny access to the SBG941 WAN. Only enter the least significant byte of the IP address.
Enabled	Activates the IP address filter, when selected. Select **Enabled** for each range of IP addresses you want to deny access to the SBG941 WAN.

When done, click **Apply** to activate and save your settings.

Advanced MAC Filtering Page

This page allows you to define up to twenty Media Access Control (MAC) address filters to prevent PCs 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.

Field Descriptions for the Advanced MAC Filtering Page

Field	Description
MAC Addresses	Media Access Control address — a unique set of 12 hexadecimal digits assigned to a PC during manufacturing.

Setting a MAC Address Filter

1. Enter the MAC address in the MAC Addresses field for the PC you want to block.
2. Click **Add MAC Address**.
3. Repeat above steps for up to twenty MAC addresses.

Advanced Port Filtering Page

This page 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 PCs, and this setting is not IP address or MAC address specific. For example, to block all PCs on the private LAN from accessing HTTP sites (or "web surfing"), set the "Start Port" to 80, "End Port" to 80, "Protocol" to TCP, select **Enabled**, and then click **Apply.***
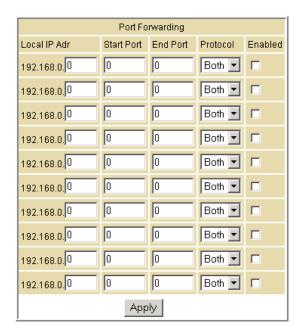
Port Filtering			
Start Port	End Port	Protocol	Enabled
1	65535	Both	☐
1	65535	Both	☐
1	65535	Both	☐
1	65535	Both	☐
1	65535	Both	☐
1	65535	Both	☐
1	65535	Both	☐
1	65535	Both	☐
1	65535	Both	☐
1	65535	Both	☐
Apply			

Field Descriptions for the Advanced Port Filtering Page

Field	Description
Start Port	Enter the starting port number.
End Port	Enter the ending port number.
Protocol	Select **TCP**, **UDP**, or **Both** from the drop-down list.
Enabled	Select for each port that you want to activate the IP port filters.

Advanced Port Forwarding Page

This page allows you to run a publicly accessible server on the LAN by specifying the mapping of TCP/UDP ports to a local PC. 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 public Internet.

	Port Forwarding			
Local IP Adr	Start Port	End Port	Protocol	Enabled
192.168.0.[0]	[0]	[0]	Both ▾	☐
192.168.0.[0]	[0]	[0]	Both ▾	☐
192.168.0.[0]	[0]	[0]	Both ▾	☐
192.168.0.[0]	[0]	[0]	Both ▾	☐
192.168.0.[0]	[0]	[0]	Both ▾	☐
192.168.0.[0]	[0]	[0]	Both ▾	☐
192.168.0.[0]	[0]	[0]	Both ▾	☐
192.168.0.[0]	[0]	[0]	Both ▾	☐
192.168.0.[0]	[0]	[0]	Both ▾	☐
192.168.0.[0]	[0]	[0]	Both ▾	☐
		Apply		

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

- HTTP: 80
- FTP: 20, 21
- Secure Shell: 22
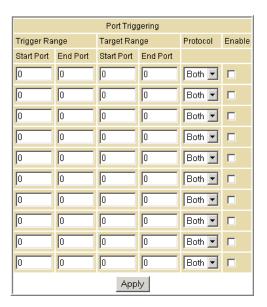- Telnet: 23
- SMTP e-mail: 25
- SNMP: 161

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

Advanced Port Triggers Page

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

The Advanced Port Triggers are similar to Advanced Port Forwarding except that they are not static ports held open all the time. When the Configuration Manager detects outgoing data on a specific IP port number set in the "Trigger Range," the resulting ports set in the "Target Range" are opened for incoming (sometimes referred to as bi-directional ports) data. If no outgoing traffic is detected on the "Trigger Range" ports for 10 minutes, the "Target Range" ports will close. This is a safer method for opening specific ports for special applications (e.g. video conferencing programs, interactive gaming, file transfer in chat programs, etc.) because they are dynamically triggered and not held open constantly or erroneously left open via the router administrator and exposed for potential hackers to discover.

Field Descriptions for the Advanced Port Triggers Page

Field	Description
Trigger Range Start Port	The starting port number of the Port Trigger range.

End Port	The ending port number of the Port Trigger range.
Target Range Start Port	The starting port number of the Port Trigger range.
End Port	The ending port number of the Port Trigger range.
Protocol	Select **TCP**, **UDP**, or **Both** from the drop-down list.
Enable	Select to activate the IP port triggers.

Advanced DMZ Host Page

This page allows you to specify the default recipient of WAN traffic that NAT is unable to translate to a known local PC. The DMZ (De-militarized Zone) hosting (also commonly referred to as "Exposed Host") can also be described as a computer or small sub-network that is located outside the firewall between the trusted internal private LAN and the untrusted public Internet. It prevents direct access by outside users to private data.

For example, you can set up a web server on a DMZ computer to enable outside users to access your website without exposing confidential data on your network.

A DMZ can also be useful to play interactive games that may have a problem running through a firewall. You can leave a computer used for gaming only exposed to the Internet while protecting the rest of your network. For more information, see Gaming Configuration Guidelines.

Setting Up the DMZ Host

1. Enter the computer's IP address.
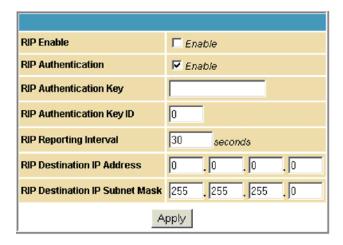2. Click **Apply** to activate the selected computer as the DMZ host.

Advanced Routing Information Protocol Setup Page

This page allows you to configure Routing Information Protocol (RIP) parameters related to authentication, destination IP address/subnet mask, and reporting intervals. RIP automatically identifies and uses the best known and quickest route to any given destination address. To help reduce network congestion and delays, the Advanced RIP setup is used in WAN networks to identify and use the best known and quickest route to given destination addresses.

RIP is a protocol that requires negotiation from both sides of the network (i.e., CMRG and CMTS). The ISP would normally set this up to match their CMTS settings with the configuration in the CMRG.

Note: RIP messaging will only be sent upstream when running in Static IP Addressing mode on the Basic Setup page. You must enable Static IP Addressing and then set the WAN IP network information!

RIP Enable	☐ Enable
RIP Authentication	☑ Enable
RIP Authentication Key	
RIP Authentication Key ID	0
RIP Reporting Interval	30 *seconds*
RIP Destination IP Address	0 . 0 . 0 . 0
RIP Destination IP Subnet Mask	255 . 255 . 255 . 0

Apply

Field Descriptions for the Advanced RIP Setup Page

Field	Description
RIP Enable	Enables or disables the RIP protocol. This protocol helps the router dynamically adapt to the changes in the network. RIP is obsolete since newer routing protocols, such as OSPF and ISIS, have been introduced.
RIP Authentication	If enabled, a plain text password or a shared key authentication is added to the RIP packet in order for the CPE and the wireless router to authenticate each other.

RIP Authentication Key	Used to encrypt the plain text password that is enclosed in each RIP packet. If you are using the shared key authentication in RIP, you will need to provide a key.
RIP Authentication Key ID	An unsigned 8-bit field in the RIP packet. This field identifies the key used to create the authentication data for the RIP packet, and it also indicates the authentication algorithm.
RIP Reporting Interval	Determines how long before a RIP packet is sent to the CPE.
RIP Destination IP Address	Location where the RIP packet is sent to update the routing table in your CPE.
RIP Destination IP Subnet Mask	Specifies which CPE you want to receive the RIP packet.

8   Firewall Pages

The SBG941 Firewall Pages allow you to configure the SBG941 firewall filters and firewall alert notifications. The SBG941 firewall protects the SBG941 LAN from undesired attacks and other intrusions from the Internet. It provides an advanced, integrated stateful-inspection firewall supporting intrusion detection, session tracking, and denial-of-service attack prevention. The firewall:

- 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.

- Provides comprehensive logging for all:

    - User authentications

    - Rejected internal and external connection requests

    - Session creation and termination

    - Outside attacks (intrusion detection)

You can configure the firewall filters to set rules for port usage. For information about choosing a predefined firewall policy template, see the Firewall Pages.

You can click any Firewall submenu option to view or change the firewall configuration information for that option.

For information about how the firewall can affect gaming, see Gaming Configuration Guidelines.

The predefined policies provide outbound Internet access for computers on the SBG941 LAN. The SBG941 firewall uses stateful-inspection to allow inbound responses when there already is an outbound session running that corresponds to the data flow. For example, if you use a web browser, outbound HTTP connections are permitted on port 80. Inbound responses from the Internet are allowed because an outbound session is established.

When required, you can configure the SBG941 firewall to allow inbound packets without first establishing an outbound session. You also need to configure a port forwarding entry on the Advanced Port Forwarding Page or a DMZ client on the Advanced DMZ Host Page.

Firewall Web Content Filter Page

This page allows you to configure the firewall by enabling or disabling various Web filters related to blocking or exclusively allowing different types of data through the Configuration Manager from the WAN to the LAN.

Java Applets, Cookies, ActiveX controls, popup windows, and Proxies can be blocked from this page. Firewall Protection turns on 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.

Web Features	
Filter Proxy	☐ Enable
Filter Cookies	☐ Enable
Filter Java Applets	☐ Enable
Filter ActiveX	☐ Enable
Filter Popup Windows	☐ Enable
Block Fragmented IP Packets	☑ Enable
Port Scan Detection	☐ Enable
IP Flood Detection	☑ Enable
Firewall Protection	☑ Enable
Apply	

Select each Web filter you want to enable for the firewall and then click **Apply**. The Web filters activate without having to reboot the SBG941 Configuration Manager.

Note: At least one Web filter or feature must be enabled for the firewall to be active. Make sure the firewall is not disabled.

Firewall Local Log Page

This page allows you to set up how to send notification of the firewall event log in either of the following formats:

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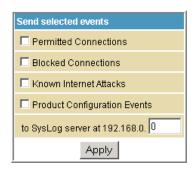- Local log is stored within the modem and displayed in table form on the Local Log page

Field Descriptions for the Firewall Local Log Page

Field	Description
Contact Email Address	Your email address.
SMTP Server Name	Name of the e-mail (Simple Mail Transfer Protocol) server. The firewall page needs your email server name to send a firewall log to your email address. You can obtain the SMTP server name from your Internet service provider.
E-mail Alerts	Enable or disable e-mailing firewall alerts.

Firewall Remote Log Page

This page allows you to send firewall attack reports out to a standard SysLog server so 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. You can log permitted connections, blocked connections, known Internet attack types, and CMRG configuration events. 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.

Field Description for the Firewall Remote Log Page

Field	Description
Permitted Connections	Select for the server to e-mail you logs of who is connecting to your network.
Blocked Connections	Select for the server to e-mail you logs of who is blocked from connecting to your network.
Known Internet Attacks	Select for the server to e-mail you logs of known Internet attacks against your network.
Product Configuration Events	Select for the server to e-mail you logs of the basic product configuration events logs.
To SysLog server at 192.168.0.	Enter the last digits from 10 to 254 of your SysLog server's IP address.

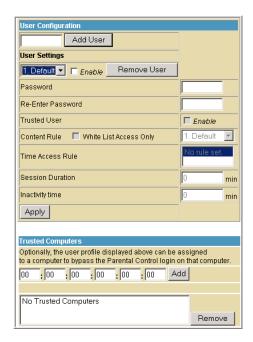When done, click **Apply**.

9 Parental Control Pages

The SBG941 Parental Control Pages allow you to configure access restrictions to a specific device connected to the SBG941 LAN.

You can click any Parental Control submenu option to view or change the configuration information for that option.

Parental Control User Setup Page

Each user is linked to a specified time access rule, content filtering rule, and login password to get to the filtered content. You may also specify a user as a "trusted user," which means that person will have access to all Internet content regardless of the filters that you define. You can use the Trusted User checkbox as a simple override to grant a user full access, while storing all of the filtering settings for easy availability.

You can also enable Internet session duration timers, which set a limited amount of time for Internet access from the rules you select. Each user must enter their password the first time to access the Internet. In addition, there is a password inactivity timer. If there is no Internet access for the specified time in minutes, the user must login again.

Field Descriptions for the Parental Control User Setup Page

| Field	Description
Add User	Adds a user to set the parental controls for a specific user.
User Settings	Select the user for whom you want to modify access restrictions. Select **Enable** to select the user. Click **Remove User** to delete the user from Parental Controls.
Password	Enter a user password to log onto the Internet.
Re-Enter Password	Enter the password again for confirmation.
Trusted User	The selected user will have full access to Internet content, thus overriding any set filters. Select **Enable** to override set filters without having to turn off filter settings.
Content Rule	Used to specify which websites a selected user is allowed to access. Select **White List Access Only** and choose a user from the drop-down list.
Time Access Rule	You can choose a rule that restricts when a selected user can use the Internet.
Session Duration	You can set the amount of time a selected user can use the Internet.
Inactivity time	You can set the amount of inactivity time before the Internet automatically closes for a selected user.
Trusted Computers	You can enter a selected user's CPE MAC address so that CPE can access the Internet without being censored by the Parental Control. When done entering the MAC address, click **Add.**
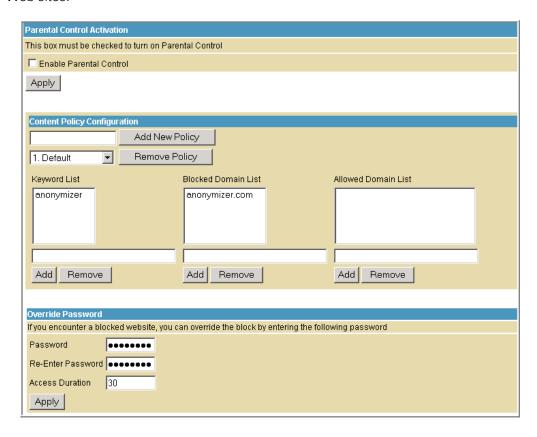
When done, click **Apply** to activate and save any changes you made.

Parental Control Basic Setup Page

This page allows you to set rules to block certain kinds of Internet content and certain Web sites.

After you have changed your Parental Control settings, click the appropriate **Apply**, **Add**, or **Remove** button.
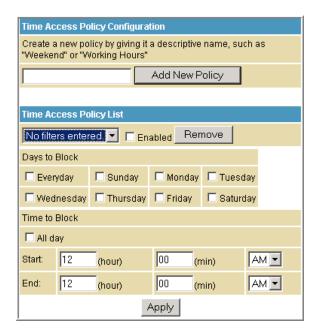
Click **Refresh** in your web browser window to view your current settings.

Parental Control Time of Day Access Policy Page

This page allows you to block all Internet traffic to and from specified devices on your SBG941 network based on the day and time settings you specify. You can set policies to block Internet traffic for the entire day or just certain time periods within each day for specific users. You can add up to 30 eight-character categories (filter names) with different day and time settings. You enter a name for each time filter in the **Add New Policy** field. Any time filter for Internet access can be enabled or disabled at any time.

The time filters for limited Internet access are applied for each user in the **Time Access Rule** field on the Parental Control User Setup Page.

After each category change is made, click **Apply** at the bottom of the page to store and activate the settings. These same category names for blocking profiles show up in the Parental Control section on the User Setup page in the "Time Access Rules" section. On that page, each user is assigned up to four of these categories simultaneously.

Parental Control Event Log Page

This page displays the Parental Control event log report. The event log is a running list of the last 30 Parental Control access violations, which include the following items on Internet traffic:

- If the user's Internet access is blocked (time filter)
- If a blocked keyword is detected in the URL
- If a blocked domain is detected in the URL
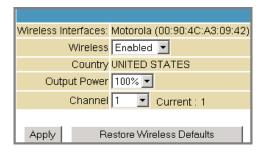- If the online lookup service detects that the URL falls under a blocked category

Last Occurence	Action	Target	User	Source

Clear Log

10 Wireless Pages

The SBG941 Wireless Pages allow you to configure your wireless LAN (WLAN). WPA or WPA2 encryption provides higher security than WEP encryption, but older wireless client cards may not support the newer WPA or WPA2 encryption methods.

Wireless 802.11 Radio Page

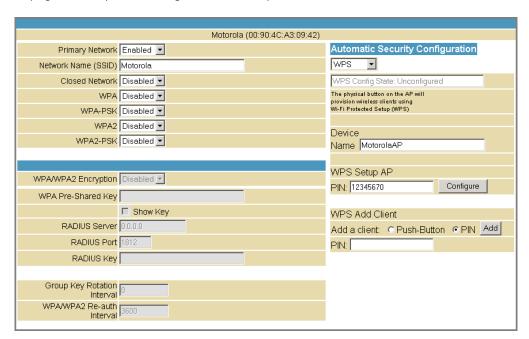This page allows you to configure the Wireless Radio parameters, including the current country and channel number.

Field Descriptions for the Wireless 802.11 Radio Page

Field	Description
Wireless Interfaces	Shows the MAC address of the installed wireless card (not configurable).
Wireless	Shows if the wireless network is enabled or disabled.
Country	Restricts the channel set based on the country's regulatory requirements. This is a display-only field.
Output Power	Sets a percentage of the output power of the hardware's maximum capability.
Channel	Selects the channel for access point (AP) operation. The list of available channels depends on the designated country. For this field, the channel selected on the wireless clients on your WLAN must be the same as the one selected on the SBG941.

Wireless 802.11 Primary Network Page

This page allows you to configure the Primary wireless network.

Field Descriptions for the Wireless 802.11 Primary Network Page

Field	Description
Primary Network	When **Enabled**, beacon frames are transmitted with the Primary Network SSID.
Network Name (SSID)	Sets the Network Name (also known as SSID) of the Primary wireless network. This is a 1-32 ASCII character string.
Closed Network	With a closed network, users type the SSID into the client application instead of selecting the SSID from a list. This feature makes it slightly more difficult for the user to gain access.
WPA	Enables or disables Wi-Fi Protected Access encryption.
WPA-PSK	Enables or disables a local WPA pre-shared key passphrase.
WPA2	Enables or disables Wi-Fi Protected Access 2 encryption.
WPA2-PSK	Enables or disables a local WPA2 pre-shared key passphrase.

|	
WPA/WPA2 Encryption	When using WPA or WPA2 authentication, these WPA encryption modes can be set: TKIP, AES, or TKIP + AES. AES (Advanced Encryption Standard) provides the strongest encryption, while TKIP (Temporal Key Integrity Protocol) provides strong encryption with improved compatibility. The TKIP + AES mode allows both TKIP and AES-capable clients to connect.
WPA Pre-Shared Key **Show Key**	Sets the WPA Pre-Shared Key (PSK). This is either an 8-63 ASCII character string or a 64-digit hex number. This is specified when the Network Authentication method is WPA-PSK. **Show Key** - When selected, the WPA Pre-Shared Key is displayed.
RADIUS Server	Sets the RADIUS server IP address to use for client authentication using the dotted-decimal format (xxx.xxx.xxx.xxx).
RADIUS Port	Sets the UDP port number of the RADIUS server. The default is 1812.
RADIUS Key	Sets the shared secret for the RADIUS connection. The key is a 0 to 255 character ASCII string.
Group Key Rotation Interval	Sets the WPA Group Rekey Interval in seconds. Set to zero to disable periodic rekeying.
WPA/WPA2 Re-auth Interval	The re-authentication interval is the amount of time the wireless router can wait before re-establishing authentication with the CPE.
WEP Encryption	WEP Encryption enables or disables Wired Equivalent Privacy encryption.
Shared Key Authentication	The WEP protocol uses the Shared Key Authentication protocol where the CPE sends an authentication request to the access point. Then the access point sends a challenge text to the CPE. The CPE uses either the 64-bit or 128-bit key to encrypt the challenge text and sends the encrypted text to the access point. The access point decrypts the encrypted text and then compares the decrypted message with the original challenge text. If they are the same, the access point lets the CPE connect; if it doesn't match, then the access point does not let the CPE connect.
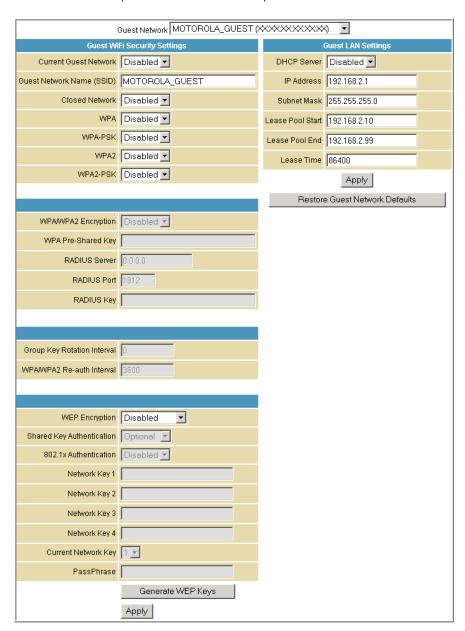
802.1x Authentication	This authentication is used in addition to WEP. 802.1x Authentication. It is a much stronger type of authentication than WEP.
Network Key 1 – 4	Sets the static WEP keys when WEP encryption is enabled. • Enter five ASCII characters or 10 hexadecimal digits for a 64-bit key. • Enter 13 ASCII characters or 26 hexadecimal digits for a 128-bit key. When both WPA encryption and WEP encryption are enabled, only keys 2 and 3 are available for WEP encryption.
Current Network Key	Selects the encryption (transmit) key when WEP encryption is enabled.
PassPhrase	Sets the text to use for WEP key generation.

Wireless 802.11 Guest Network Page

This page allows you to configure a secondary guest network on the wireless interface. This network is isolated from the LAN. Any clients that associate with the guest network SSID is isolated from the private LAN and can only communicate with WAN hosts.
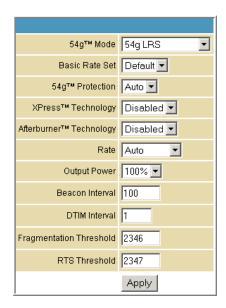
Field Descriptions for the Wireless 802.11 Guest Network Page

Field	Description
Guest Network	You may have several different wireless Guest Networks running with different options. You can select which wireless Guest Network to modify.
Current Guest Network	When set to **Enabled**, beacon frames are transmitted with the Guest SSID
Guest Network Name (SSID)	Assigns a unique network name (SSID) for the guest network, which appears in the beacon frames.
Closed Network	With a closed network, users type the SSID into the client application instead of selecting the SSID from a list. This feature makes it more difficult for the user to gain access.
DHCP Server	Enables the DHCP server to give out leases to guest network clients from the specified lease pool. If the DHCP server is disabled, guest network stations (STAs) need to be assigned static IP addresses.
IP Address	Specifies the gateway IP relayed to guest clients in DHCP lease offers.
Subnet Mask	Specifies the subnet mask for the guest network.
Lease Pool Start	Specifies the starting IP address for the guest network lease pool.
Lease Pool End	Specifies the ending IP address for the guest network lease pool.
Lease Time	Specifies the lease time for the guest network lease pool once the Configuration Manager completes the WAN provisioning.

Wireless 802.11 Advanced Page

This page allows you to configure data rates and Wi-Fi thresholds.

54g™ Mode	54g LRS
Basic Rate Set	Default
54g™ Protection	Auto
XPress™ Technology	Disabled
Afterburner™ Technology	Disabled
Rate	Auto
Output Power	100%
Beacon Interval	100
DTIM Interval	1
Fragmentation Threshold	2346
RTS Threshold	2347
	Apply

Field Descriptions for the Wireless 802.11 Advanced Page

| Field	Description
54g™ Mode	Sets these network modes: • 54g Auto • 54g Performance • 54g LRS • 802.11b only 54g Auto accepts 54g, 802.11g, and 802.11b clients, but optimizes performance based on the type of connected clients. 54g Performance accepts only 54g clients and provides the highest performance throughout; nearby 802.11b networks may have degraded performance. 54g LRS interoperates with the widest variety of 54g, 802.11g, and 802.11b clients. 80211b. accepts only 802.11b clients.
Basic Rate Set	Determines which rates are advertised as basic rates. Default uses the driver defaults. All sets all available rates as basic rates.
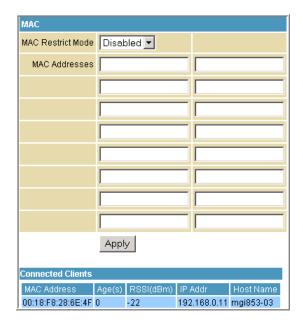
54g™ Protection	In Auto mode, the AP uses RTS/CTS protection to improve 802.11g performance in mixed 802.11g + 802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.
XPress™ Technology	A performance-enhancing Wi-Fi technology designed for increasing throughput and efficiency. Use it when there are mixed wireless networks in the surrounding area from 802.11a/b/g networks.
Afterburner™ Technology	A performance-enhancing Wi-Fi technology that enhances the existing 802.11g standard by increasing throughput by 40 percent.
Rate	Forces the transmission rate for the AP to a particular speed. Auto will provide the best performance in nearly all situations.
Output Power	Sets the output power as a percentage of the hardware's maximum capability.
Beacon Interval	Sets the beacon interval for the AP. The default is 100, which is fine for nearly all applications.
DTIM Interval	Sets the wakeup interval for clients in Power Save mode. When a client is running in Power Save mode, lower values provide higher performance, while higher values provide lower performance.
Fragmentation Threshold	Sets the fragmentation threshold. Packets exceeding this threshold are fragmented into packets no larger than the threshold before packet transmission.
RTS Threshold	Sets the RTS threshold. Packets exceeding this threshold cause the AP to perform an RTS/CTS exchange to reserve the wireless medium before packet transmission.

Wireless 802.11 Access Control Page

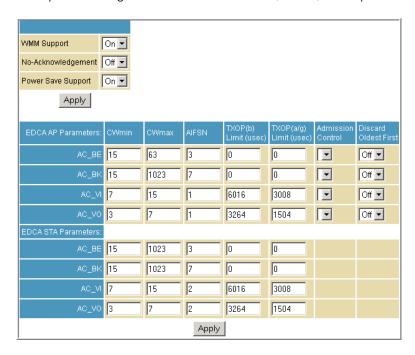This page allows you to configure the Access Control to the AP as well as status on the connected clients.

MAC		
MAC Restrict Mode	Disabled ▼	
MAC Addresses	[ ]	[ ]
	[ ]	[ ]
	[ ]	[ ]
	[ ]	[ ]
	[ ]	[ ]
	[ ]	[ ]
	[ ]	[ ]
	[ ]	[ ]
	Apply	

Connected Clients				
MAC Address	Age(s)	RSSI(dBm)	IP Addr	Host Name
00:18:F8:28:6E:4F	0	-22	192.168.0.11	mgi853-03

Field Descriptions for the Wireless 802.11 Access Control Page

Field	Description
MAC Restrict Mode	Selects whether wireless clients with the specified MAC address are allowed or denied wireless access. Select **Disabled** to allow all clients.
MAC Address	A list of wireless client MAC addresses to allow or deny based on the Restrict Mode setting. Valid input MAC address formats are XX:XX:XX:XX:XX:XX and XX-XX-XX-XX-XX-XX.
Connected Clients	Lists connected wireless clients. When a client connects (associates) to the network, the client is added to the list; when a client leaves (disassociates) from the network, the client is removed from the list. For each client, the age (in seconds), estimated average receive signal strength (in dBm), IP address, and host name are presented. The age is the amount of time elapsed since data was transmitted to or received from the client.

Wireless 802.11 Wi-Fi Multimedia Page

This page allows you to configure the Wi-Fi Multimedia (WMM) Quality of Service (QoS).

Field Descriptions for the Wireless 802.11 Wi-Fi Multimedia Page

Field	Description
WMM Support	Sets WMM support to Auto, On, or Off. If enabled (Auto or On), the WME Information Element is included in beacon frame.
No-Acknowledgement	Sets No-Acknowledgement support to On or Off. When enabled, acknowledgments for data are not transmitted.
Power Save Support	Sets Power Save support to On or Off. When Power Save is enabled, the AP queues packets for STAs are in Power Save mode. Queued packets are transmitted when the station (STA) notifies the AP that it has left Power-Save mode.
EDCA AP Parameters	Specifies the transmit parameters for traffic transmitted from the AP to the STA in four Access Categories: • Best Effort (AC_BE) • Background (AC_BK)

	• Video (AC_VI) • Voice (AC_VO)
EDCA AP Parameters (continued)	Transmit parameters include Contention Window (CWmin and CWmax), Arbitration Inter Frame Spacing Number (AIFSN), and Transmit Opportunity Limit (TXOP Limit). There are also two AP-specific settings: Admission Control and Discard Oldest First. Admission control specifies if admission control is enforced for the Access Categories. Discard Oldest First specifies the discard policy for the queues. On discards the oldest first; Off discards the newest first.
EDCA STA Parameters	Specifies the transmit parameters for traffic transmitted from the STA to the AP in four Access Categories: • Best Effort (AC_BE) • Background (AC_BK) • Video (AC_VI) • Voice (AC_VO) Transmit parameters include Contention Window (CWmin and CWmax), Arbitration Inter Frame Spacing Number (AIFSN), and Transmit Opportunity Limit (TXOP Limit).

Wireless 802.11 Bridging Page

This page allows you to configure the WDS features.

Wireless Bridging	Disabled ▼
Remote Bridges	
	Apply

Field Descriptions for the Wireless 802.11 Bridging Page

Field	Description
Wireless Bridging	Enables or disables wireless bridging.
Remote Bridges	Table of remote bridge MAC addresses authorized to establish a wireless bridge. Up to four remote bridges may be connected. Typically, you will also have to enter your AP's MAC address on the remote bridge.

Setting Up Your Wireless LAN

You can use the SBG941 as an access point for a wireless LAN (WLAN) without changing its default settings.

To enable security for your WLAN, you can do the following on the SBG941:

- Encrypt wireless LAN transmissions
- Restrict wireless LAN access to further prevent unauthorized WLAN intrusions using the Wireless 802.11 Access Control Page.

CAUTION	*Never provide your SSID, WPA or WEP passphrase, or WEP key to anyone who is not authorized to use your WLAN.*

Connect at least one computer to the SBG941 Ethernet port to perform configuration. Do not attempt to configure the SBG941 over a wireless connection.

You need to configure each wireless client (station) to access the SBG941 LAN as described in Installing Wireless Clients.

Another step to improve wireless security is to place wireless components away from windows. This decreases the signal strength outside the intended area.

Encrypting Wireless LAN Transmissions

To prevent unauthorized viewing of data transmitted over your WLAN, you must encrypt your wireless transmissions. Choose one:

Encrypting Wireless LAN Transmissions

Configure on the SBG941	Required on Each Wireless Client
If all of your wireless clients support Wi-Fi Protected Access (WPA), Motorola recommends configuring WPA on the SBG941	If you use a local, pre-shared key (WPA-PSK) passphrase, you must configure the identical passphrase to the SBG941 on each wireless client. Home and small-office settings typically use a local passphrase.
Otherwise, configure WEP on the SBG941	You must configure the identical WEP key to the SBG941 on each wireless client.

If all of your wireless clients support WPA encryption, Motorola recommends using WPA instead of WEP.

For new wireless LANs, Motorola recommends purchasing client adapters that support WPA encryption.

Installing Wireless Clients

Note: *Use the SBG941 Installation CD-ROM to set the client security. The passcode is located on the* MAC Label.

For each wireless client computer (station), install the wireless adapter by following the instructions supplied with the adapter. Be sure to:

1. Insert the CD-ROM for the adapter in the CD-ROM drive on the client.
2. Install the device software from the CD or the modem.
3. Insert the adapter in the PCMCIA or PCI slot or connect it to the USB port.
4. Configure the adapter to obtain an IP address automatically.

You may need to do the following to use a wireless client computer to access the Internet:

Installing Wireless Clients

If You Performed:	On Each Client, You Need to Perform:
Configuring WPA on the SBG941	Configuring a Wireless Client for WPA or WPA2
Configuring WEP on the SBG941	Configuring a Wireless Client for WEP
Configuring the Wireless Network Name on the SBG941	Configuring a Wireless Client with the Network Name (SSID)
Configuring a MAC Access Control List on the SBG941	No configuration on client required

Configuring a Wireless Client for WPA

If you enabled WPA and set a PSK Passphrase by configuring WPA on the SBG941, you must configure the same passphrase (key) on each wireless client. The SBG941 cannot authenticate a client if:

• WPA is enabled on the SBG941, but not on the client

• The client passphrase does not match the SBG941 PSK Passphrase

CAUTION　　*Never provide the PSK Passphrase to anyone who is not authorized to use your WLAN.*

Configuring a Wireless Client for WEP

If you enabled WEP and set a key by configuring WEP on the SBG941, you must configure the same WEP key on each wireless client. The SBG941 cannot authenticate a client if:

- Shared Key Authentication is enabled on the SBG941 but not on the client
- The client WEP key does not match the SBG941 WEP key

For all wireless adapters, you must enter the 64-bit or 128-bit WEP key generated by the SBG941.

CAUTION   *Never provide the WEP key to anyone who is not authorized to use your WLAN.*

Configuring a Wireless Client with the Network Name (SSID)

After you specify the network name on the Wireless Primary Network Page, many wireless cards or adapters automatically scan for an access point, such as the SBG941 and the proper channel and data rate. If your card requires you to manually start scanning for an access point, do so following the instructions in the documentation supplied with the card. You must enter the same SSID in the wireless configuration setup for the device to communicate with the SBG941.

A Troubleshooting

If the solutions listed here do not solve your problem, contact your service provider.

Before calling your service provider, try pressing the Reset button on the rear panel of the SBG941.

Note: *Press **RESET** to restore the default settings. You will lose your custom configuration settings, including Parental Control, Firewall, and Advanced settings.*

Resetting the SBG941 may take 5- to 30 minutes. Your service provider may ask for the status of the lights as described in Front-Panel LEDs and Error Conditions.

Solutions

Table 2 – Troubleshooting Solutions

Problem	Possible Solution
Power light is off	Check that the SBG941 is properly plugged into the electrical outlet.
	Check that the electrical outlet is working.
	Press the Reset button.
Cannot send or receive data	On the front panel, note the status of the LEDs and refer to Table 3 – Front Panel LEDs and Error Conditions to identify the error. If you have cable TV, check that the TV is working and the picture is clear. If you cannot receive regular TV channels, the data service will not function.
	Check the coaxial cable at the SBG941 and wall outlet. Hand-tighten if necessary.
	Check the IP address. Follow the steps for verifying the IP address for your system, see Verifying the IP Address in Windows XP or Verifying the IP Address in Windows Vista. Call your service provider if you need an IP address.
	Check that the Ethernet cable is properly connected to the SBG941 and the computer.
	If a device is connected via the Ethernet port, verify connectivity by checking the LINK LEDs on the rear panel.

Wireless client(s) cannot send or receive data	Perform the first four checks in "Cannot send or receive data."
	Check the Security Mode setting on the Wireless Primary Network Page:
	• If you enabled WPA and configured a passphrase on the SBG941, be sure each affected wireless client has the identical passphrase. If this does not solve the problem, check whether the wireless client supports WPA.
	• If you enabled WEP and configured a key on the SBG941, 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 SBG941.
	• To temporarily eliminate the Security Mode as a potential issue, disable security.
	After resolving your problem, be sure to re-enable wireless security.
	• On the Wireless Access Control Page, be sure the MAC address for each affected wireless client is correctly listed.
Slow wireless transmission speed with WPA enabled	On the Wireless Primary Network Page, check whether the WPA Encryption type is TKIP. If all of your wireless clients support AES, change the WPA Encryption to AES.

Front Panel LEDs and Error Conditions

The SBG941 front panel LEDs provide status information for the following error conditions:

Table 3 – Front Panel LEDs and Error Conditions

LED	Status	If, During Startup:	If, During Normal Operation:
POWER	OFF	SBG941 is not properly plugged into the power outlet	The SBG941 is unplugged
RECEIVE	FLASHING	Downstream receive channel cannot be acquired	The downstream channel is lost
SEND	FLASHING	Upstream send channel cannot be acquired	The upstream channel is lost
ONLINE	FLASHING	IP registration is unsuccessful	The IP registration is lost

B Software License & Warranty

SURFboard SBG941 Wireless Cable Modem Gateway

Motorola, Inc.
Home & Networks Mobility Solutions Business ("Motorola")
101 Tournament Drive
Horsham, PA 19044

Software License

IMPORTANT: PLEASE READ THIS SOFTWARE LICENSE ("LICENSE") CAREFULLY BEFORE YOU INSTALL, DOWNLOAD OR USE ANY APPLICATION SOFTWARE, USB DRIVER SOFTWARE, FIRMWARE AND RELATED DOCUMENTATION ("SOFTWARE") PROVIDED WITH MOTOROLA'S CABLE DATA PRODUCT (THE "CABLE DATA PRODUCT"). BY USING THE CABLE DATA PRODUCT AND/OR INSTALLING, DOWNLOADING OR USING ANY OF THE SOFTWARE, YOU INDICATE YOUR ACCEPTANCE OF EACH OF THE TERMS OF THIS LICENSE. UPON ACCEPTANCE, THIS LICENSE WILL BE A LEGALLY BINDING AGREEMENT BETWEEN YOU AND MOTOROLA. THE TERMS OF THIS LICENSE APPLY TO YOU AND TO ANY SUBSEQUENT USER OF THIS SOFTWARE.

IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS LICENSE (I) DO NOT INSTALL OR USE THE SOFTWARE AND (II) RETURN THE CABLE DATA PRODUCT AND THE SOFTWARE (COLLECTIVELY, "PRODUCT"), INCLUDING ALL COMPONENTS, DOCUMENTATION AND ANY OTHER MATERIALS PROVIDED WITH THE PRODUCT, TO YOUR POINT OF PURCHASE OR SERVICE PROVIDER, AS THE CASE MAY BE, FOR A FULL REFUND. BY INSTALLING OR USING THE SOFTWARE, YOU AGREE TO BE BOUND BY THE PROVISIONS OF THIS LICENSE AGREEMENT.

The Software includes associated media, any printed materials, and any "on-line" or electronic documentation. Software provided by third parties may be subject to separate end-user license agreements from the manufacturers of such Software.

The Software is never sold. Motorola licenses the Software to the original customer and to any subsequent licensee for personal use only on the terms of this License. Motorola and its 3rd party licensors retain the ownership of the Software.

You may:

USE the Software only in connection with the operation of the Product.

TRANSFER the Software (including all component parts and printed materials) permanently to another person, but only if the person agrees to accept all of the terms of this License. If you transfer the Software, you must at the same time transfer the Product and all copies of the Software (if applicable) to the same person or destroy any copies not transferred.

TERMINATE this License by destroying the original and all copies of the Software (if applicable) in whatever form.

You may not:

(1) Loan, distribute, rent, lease, give, sublicense or otherwise transfer the Software, in whole or in part, to any other person, except as permitted under the TRANSFER paragraph above. (2) Copy or translate the User Guide included with the Software, other than for personal use. (3) Copy, alter, translate, decompile, disassemble or reverse engineer the Software, including but not limited to, modifying the Software to make it operate on non-compatible hardware. (4) Remove, alter or cause not to be displayed, any copyright notices or startup message contained in the Software programs or documentation. (5) Export the Software or the Product components in violation of any United States export laws.

The Product is not designed or intended for use in on-line control of aircraft, air traffic, aircraft navigation or aircraft communications; or in design, construction, operation or maintenance of any nuclear facility. MOTOROLA AND ITS 3RD PARTY LICENSORS DISCLAIM ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR SUCH USES. YOU REPRESENT AND WARRANT THAT YOU SHALL NOT USE THE PRODUCT FOR SUCH PURPOSES.

Title to this Software, including the ownership of all copyrights, mask work rights, patents, trademarks and all other intellectual property rights subsisting in the foregoing, and all adaptations to and modifications of the foregoing shall at all times remain with Motorola and its 3rd party licensors. Motorola retains all rights not expressly licensed under this License. The Software, including any images, graphics, photographs, animation, video, audio, music and text incorporated therein is owned by Motorola or its 3rd party licensors and is protected by United States copyright laws and international treaty provisions. Except as otherwise expressly provided in this License, the copying, reproduction, distribution or preparation of derivative works of the Software, any portion of the Product or the documentation is strictly prohibited by such laws and treaty provisions. Nothing in this License constitutes a waiver of Motorola's rights under United States copyright law.

This License and your rights regarding any matter it addresses are governed by the laws of the Commonwealth of Pennsylvania, without reference to conflict of laws principles. THIS LICENSE SHALL TERMINATE AUTOMATICALLY if you fail to comply with the terms of this License.

Motorola is not responsible for any third party software provided as a bundled application, or otherwise, with the Software.

U.S. GOVERNMENT RESTRICTED RIGHTS

The Product and documentation is provided with RESTRICTED RIGHTS. The use, duplication or disclosure by the Government is subject to restrictions as set forth in subdivision (c)(1)(ii) of The Rights in Technical Data and Computer Software clause at 52.227-7013. The contractor/manufacturer is Motorola, Inc., Home & Networks Mobility Solutions Business, 101 Tournament Drive, Horsham, PA 19044.

Warranty Information

SURFboard SBG941 Wireless Cable Modem Gateway

Home & Networks Mobility ("Motorola")

What is my limited warranty? A limited warranty for this Product (including Software) is provided by Motorola to your distributor, cable operator, or Internet service provider, as applicable. Please contact your cable operator or Internet service provider ("Service Provider") for details. Motorola does not warrant that any Software will perform error-free or without bugs. Motorola's warranty 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. Motorola's warranty applies only to a Product that is manufactured by Motorola and identified by Motorola-owned trademarks, trade names, or product identification logos affixed to the Product. MOTOROLA DOES NOT WARRANT THIS PRODUCT DIRECTLY TO YOU, THE END USER. EXCEPT AS DESCRIBED IN THIS SECTION "WARRANTY INFORMATION," THERE ARE NO WARRANTIES OR REPRESENTATIONS 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 WARRANTY AGAINST INFRINGEMENT. MOTOROLA IS NOT RESPONSIBLE FOR, AND PROVIDES "AS IS," ANY SOFTWARE SUPPLIED BY 3RD PARTIES.

What additional provisions should I be aware of? Because it is impossible for Motorola 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, Motorola 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. MOTOROLA IS NOT RESPONSIBLE FOR PROBLEMS OR DAMAGE CAUSED BY THE INTERACTION OF THE PRODUCT WITH ANY OTHER SOFTWARE OR HARDWARE.

How long does this Limited Warranty last? Contact your Service Provider for details.

What you must do to obtain warranty service. For Product customer service, technical support, warranty claims, questions about your Internet service or connection, contact your Service Provider. 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 MOTOROLA 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 MOTOROLA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO CASE SHALL MOTOROLA'S LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

Motorola's warranty is governed by the laws of the Commonwealth of Pennsylvania, excluding its conflict of laws principles and excluding the provisions of the United Nations.

MOTOROLA