Motorola SURFboard®

SBG901 Wireless Cable Modem Gateway

User Guide

Motorola reserves the right to revise this publication and to make changes in content from time to time without obligation on the part of Motorola to provide notification of such revision or change. Motorola provides this guide without warranty of any kind, implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Motorola may make improvements or changes in the product(s) described in this manual at any time.

Safety and Regulatory Information

SAFETY AND REGULATORY INFORMATION

IMPORTANT SAFETY INSTRUCTIONS

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.

- It is recommended that the customer install an AC surge protector in the AC outlet to which this device is connected. This is to avoid damaging the device by local lightning strikes and other electrical surges.
- Postpone installation until there is no risk of thunderstorm or lightning activity in the area.
- Do not 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 40º 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.

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.

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:

1. This Device May Not Cause Interference, and
2. 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 between the radiator and your body.

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.

INTERNATIONAL DECLARATION OF CONFORMITY

We, Motorola, Inc., 101 Tournament Drive, Horsham, PA 19044, U.S.A., declare under our sole responsibility that the SBG901 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	

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
- Waste Electrical and Electronic Equipment (WEEE) Directive 2002/96/EC
- Restriction of the Use of Certain Hazardous Substances in Electrical Equipment (RoHS) Directive 2002/95/EC

Table of Contents

Basic Pages

Advanced Pages

Firewall Pages

Parental Control Pages

Wireless Pages

1 Overview

The Motorola SBG901 SURFboard® Wireless Cable Modem Gateway is designed for your home, home office, or small business/enterprise. It can be used in households with one or more computers capable of wireless connectivity for remote access to the cable modem.

This user guide provides product overview and setup information for the SBG901. It also provides instructions for installing the cable modem and configuring the wireless, Ethernet, router, DHCP, and security settings.

Contact Information

For any questions or assistance with the SBG901 wireless gateway, contact your Internet Service provider.

For information on customer service, technical support, or warranty claims; see the Motorola SBG901 Software License, Warranty, Safety, and Regulatory Information card provided with the SBG901 wireless cable modem gateway.

SBG901 Features

The SBG901 wireless gateway combines high-speed Internet access, networking, and computer security for a home or small-office LAN. It offers the following features:

- Combination of four separate products in one compact unit — a DOCSIS® 2.0 cable modem, IEEE 802.11g wireless access point (Wi-Fi© certified), Ethernet 10/100Base-T connection, and firewall.
- Advanced firewall for enhanced network security from undesired attacks over the Internet. It supports stateful-inspection, intrusion detection, DMZ, denial-of-service attack prevention, and Network Address Translation (NAT).
- Data encryption and network access control for wireless transmissions.
- An easy installation and security setup wizard. The Installation Assistant application on the SBG901 Installation CD-ROM enables easy connection to the cable network and setup for security.
- An integrated high-speed cable modem for continuous broadband access to the Internet and other online services with much faster data transfer than traditional dial-up or ISDN modems.
- One broadband connection for up to 245 computers to surf the web; all computers on the LAN communicate as if they were connected to the same physical network.

- An IEEE 802.11g wireless access point to enable laptop users to remain connected while moving around the home or small office or to connect desktop computers without installing network wiring. Depending on distance, wireless connection speeds can vary.
- A secure Wi-Fi (Wireless Fidelity) broadband connection for Wi-Fi enabled devices on your network, such as your cellular telephone, laptops, printers, PDAs, and desktops.
- One 10/100Base-T Ethernet uplink port supporting a half- or full-duplex connection with auto-MDIX capability.
- A built-in DHCP server to easily configure a combined wired and/or wireless Class C private LAN.
- SBG901 Configuration Manager (CMGR) which provides a graphical user interface (GUI) for easy configuration of necessary wireless, Ethernet, router, DHCP, and security settings.
- Port Forwarding to configure ports to run applications having special network requirements.

For the most recent product documentation, visit the Modems & Gateways page on the Motorola website: http://broadband.motorola.com/consumers/support/default.asp.

SBG901 LAN Choices

You can connect up to 245 client computers to the SBG901 using one or any combination of the following network connections:

- Ethernet local area network (LAN)
- Wireless LAN (WLAN)
- Wi-Fi connections to Wi-Fi enabled devices

Each computer needs appropriate network adapter hardware and driver software. The clients on the Ethernet or wireless interfaces can share:

- Internet access with a single Internet Service provider account, subject to Internet Service provider terms and conditions.
- Files, printers, storage devices, multi-user software applications, games, and video conferencing.
- Wireless and wired network connections use Windows networking to share files and peripheral devices such as printers, CD-ROM drives, and external USB drives.

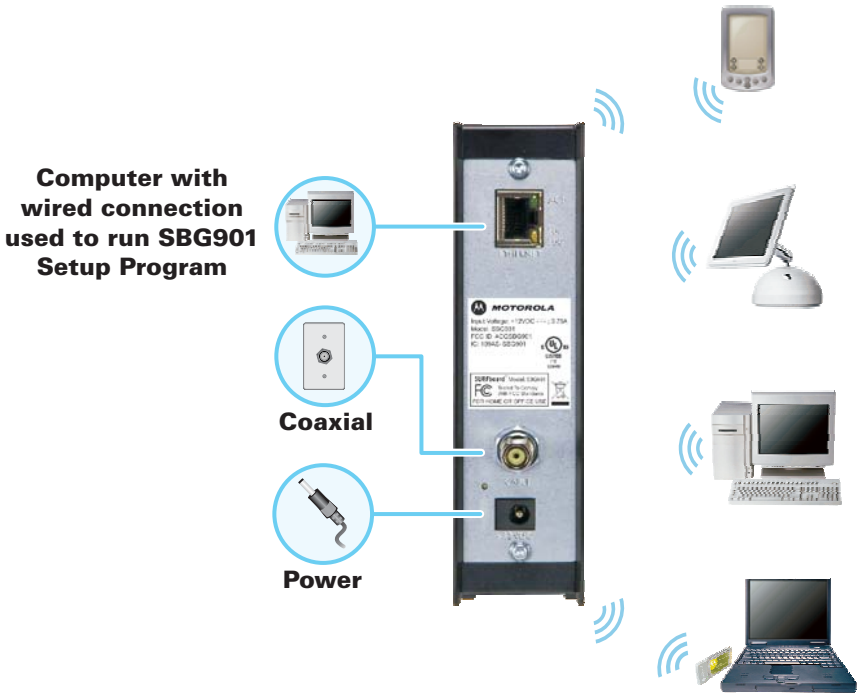
Wireless LAN

Wireless communication occurs over radio waves rather than a wire. Like a cordless telephone, a WLAN uses radio signals instead of wires to exchange data. A wireless network eliminates the need for expensive and intrusive wiring to connect computers throughout the home or office. Mobile users can remain connected to the network even when carrying their laptop to different locations in the home or office.

Each computer or other device on a WLAN must be Wi-Fi enabled with either a built-in or external wireless adapter.

Laptops — Use a wireless notebook adapter in the PCMCIA slot or a wireless USB adapter.

Desktops — Use a wireless PCI adapter, wireless USB adapter, or compatible product in the PCI slot or USB port, respectively.



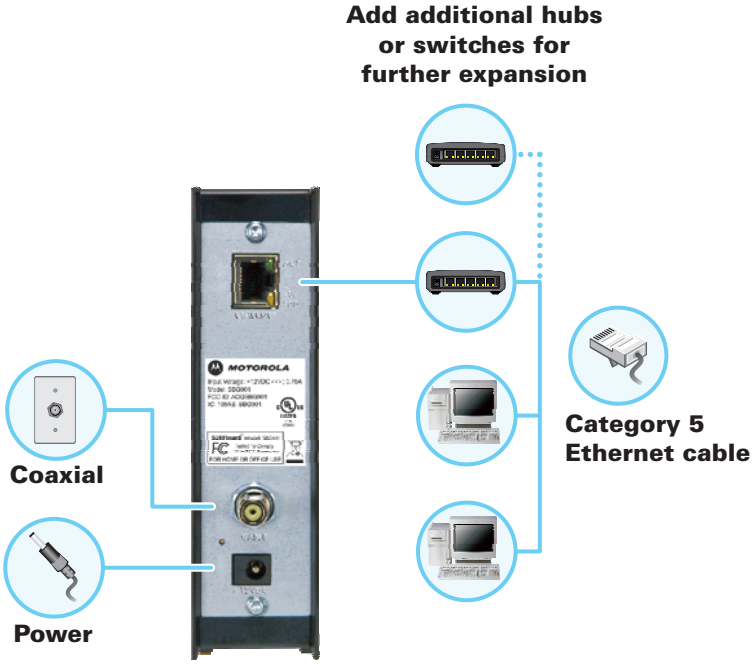
Sample Wireless Network Connections

To set up the SBG901 on a computer wired to the SBG901 with an Ethernet connection, perform the procedures in the section, Wireless Pages. *Do not attempt to configure the SBG901 over a wireless connection.*

Your maximum wireless operation distance depends on the type of materials through which the signal must pass and the location of your SBG901 and clients (stations). *Motorola cannot guarantee wireless operation for all supported distances in all environments.*

Wired Ethernet LAN

You can easily connect any PC with an Ethernet LAN port to the SBG901 Ethernet connection. Because the SBG901 Ethernet port supports auto-MDIX, you can use straight-through or cross-over cable to connect a hub, switch, or computer. Use category 5, or better, cabling for all Ethernet connections.



Sample Ethernet to Computer Connection

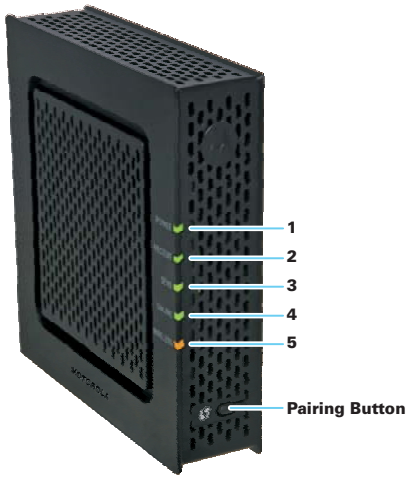
A wired Ethernet LAN with more than one computer requires one or more hubs, switches, or routers. You can:

- Connect a hub or switch to the Ethernet port on the SBG901.
- Use Ethernet hubs, switches, or routers to connect up to a combination of 245 computers and wireless clients to the SBG901.

More detailed information on Ethernet cabling is beyond the scope of this document.

Front Panel LEDs Overview

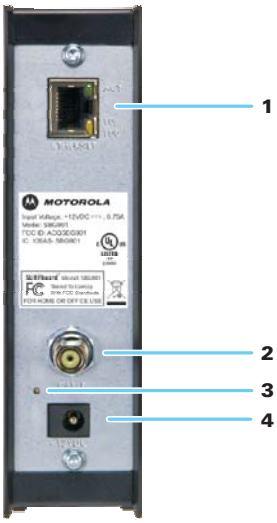
The SBG901 front panel contains indicator lights and a **Pairing button** which is used for configuring a secure wireless connection with a client card that also has a Pairing button/feature to automatically connect to the SBG901 wireless network. The display remains dark until there is a connection or activity on an interface.



The SBG901 front panel LED indicators provide the following status information for power, communications, and errors:

Key	LED	Flashing	On
1	POWER	Not applicable — LED does not flash	**Green**: Power is properly connected
2	RECEIVE	Scanning for a receive (downstream) channel connection	**Green**: Downstream channel is connected
3	SEND	Scanning for a send (upstream) channel connection	**Green**: Upstream channel is connected
4	ONLINE	Scanning for Internet connection; transmitting or receiving data over the Internet	**Green**: Startup process completed
5	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 SBG901 and another Wi-Fi enabled device on your network — printer, PDA, laptop, etc. **Amber**: WPS pairing was successful. LED turns green after five minutes.

Rear Panel Overview



The SBG901 rear panel contains the following cabling port and connectors:

Key	Item	Description
1	ETHERNET	Connects to an Ethernet-equipped computer, hub, or switch using an RJ-45 cable connection. **Activity LED** — Green LED defines the activity of the Ethernet connector. When LED is ON, this indicates that there is no data traffic and a connection is stabilized. When LED is FLASHING, this indicates that there is data being transmitted upstream or downstream. When LED is OFF, this indicates that the unit is not powered or there is no Ethernet connection. **10/100 LED** — Indicates the connection data rate. When Green LED is ON, this indicates a 100Base-T data connection. When Green LED is OFF **and** Activity LED is ON, this indicates a 10Base-T data connection.
2	CABLE	Connects the SBG901 to a cable wall outlet.
3	RESET	Resets the cable modem which may take from five to 30 minutes.
4	+12VDC	Provides power to the cable modem.

MAC Label

The SBG901 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 will need to provide the MAC address marked **HFC MAC ID** to your Internet Service provider.

2 Getting Started

This section provides information on setting up and installing the SBG901 wireless gateway. For information on WLAN setup, see Setting Up Your Wireless LAN.

Before You Begin

Before you begin the installation, check that the following items were included with your Motorola SBG901 Wireless Cable Modem Gateway:

Item		Description
Power cord		Connects the SBG901 to an AC electrical outlet
10/100Base-T Ethernet cable		Connects the SBG901 to the network via the Ethernet port. Cable must be Cat 5 or greater with an RJ-45 connector.
Software License & Regulatory Card		Contains software license, warranty, and safety information for the SBG901.
SBG901 Installation CD-ROM		Contains the SBG901 Installation Assistant, and this user guide
SBG901 Install Sheet		Provides basic information for setting up the SBG901

You must have the latest service packs and patches installed on your computer for your operating system. You will need a 75-ohm coaxial cable with F-type connectors to connect the SBG901 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 both the TV and the SBG901.

Determine which connection types you will make to the SBG901. Check that you have the required cables, adapters, and adapter software. You may need:

Item	Description
Wireless LAN	Wireless adapter and driver software for each computer having a wireless connection
Wired Ethernet	Ethernet cables and network interface cards (NICs) with accompanying installation software
LAN	To connect more than one computer via an Ethernet connection to the SBG901

Precautions

Postpone SBG901 installation until there is no risk of thunderstorm or lightning activity in the area.

To avoid potential shock, always unplug the power cord from the wall outlet or other power source before disconnecting it from the SBG901 rear panel.

To prevent overheating the SBG901, do not block the ventilation holes on the sides of the unit. Do not open the unit. Refer all service to your Internet Service provider.

Signing Up for Service

You must sign up with an Internet Service provider to access the Internet and other online services. To activate your service, call your local Internet Service provider.

You will need to provide the MAC address marked **HFC MAC ID** printed on the MAC Label. You can record it on the *SBG901 Install Sheet*.

You should ask your Internet Service provider the following questions:

- Do I have any special system requirements?
- When can I begin to use my SBG901?
- Are there any files I need to download after connecting the SBG901?
- Do I need a user name or password to access the Internet or use e-mail?

System Requirements

You can connect Microsoft® Windows®, Macintosh®, UNIX®, or Linux® computers to the SBG901 LAN using one of the following connections:

- **Ethernet** — 10Base-T or 10/100Base-T Ethernet adapter with proper driver software installed.
- **Wireless** — Any IEEE 802.11g or IEEE 802.11b device. This includes any Wi-Fi certified wireless device, such as a cellular telephone equipped with this feature.

In addition, your computer must meet the following requirements:

- Computer with Pentium© class or better processor
- Windows XP, Windows Vista, Macintosh, Linux, or UNIX operating system with available operating system CD-ROM

You can use any web browser such as Microsoft® Internet Explorer, Netscape Navigator®, or Mozilla® Firefox® with the SBG901 wireless gateway.

Connecting the SBG901 to the Cable System

> ***Note**: Before starting, be sure the computer is turned on and the SBG901 is unplugged.*

1. Connect one end of the coaxial cable to the cable outlet or splitter.
2. Connect the other end of the coaxial cable to the cable connector on the SBG901. Hand-tighten the connectors to avoid damaging them.
3. Plug the power cord into the power connector on the SBG901.
4. Plug the power cord into the electrical outlet. This turns on the SBG901. You do not need to unplug it when not in use. The first time you plug in the SBG901, allow it five to 30 minutes to find and lock on the appropriate communications channels.

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

SBG901 LED Activity During Startup

LED	Description
POWER	Turns on when AC power is connected to the SBG901. 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 SBG901 registration and configuration. Changes to solid green when the SBG901 is registered.

Cabling the LAN

After connecting to the cable system, you can connect your wired Ethernet LAN. Some sample connections are shown in Wired Ethernet LAN. On each networked computer, you must install proper drivers for the Ethernet adapter. Detailed information about network cabling is beyond the scope of this document.

Obtaining an IP Address for an Ethernet Connection

To obtain the IP address for your computer's network interface, use 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 Motorola SBG901 gateway provides a DHCP server on its LAN. It is recommended that you configure your LAN to obtain the IPs for the LAN and DNS server automatically.

Configuring TCP/IP

Make sure all client computers are configured for TCP/IP, which is a protocol for communication between computers. Perform one of the following for the operating system you are running:

- Configuring TCP/IP in Windows XP
- Configuring TCP/IP in Windows Vista
- For UNIX systems, follow the instructions in the applicable UNIX user documentation.

After configuring TCP/IP on your computer, perform one of the following to verify the IP address:

- Verifying the IP Address in Windows XP
- Verifying the IP Address in Windows Vista

For UNIX systems, follow the instructions in the applicable UNIX user documentation.

Your cable provider may provide additional instructions to set up your computer.

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.
7. 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**.
8. Select **Internet Protocol Version4 (TCP/IPv4)** and click **Properties** to display the Internet Protocol Version 4 (TCP/IPv4) Properties window.
9. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
10. Click **OK** to save the TCP/IP settings and close the Internet Protocol Version 4 (TCP/IPv4) Properties window.
11. Click **OK** to close the Local Area Connection Properties window.
12. Close the remaining windows and exit the Control Panel.
13. 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, it indicates possible broadband network problems or an improper connection between your computer and the SBG901. 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 SBG901 is configured to automatically obtain an IP address from a Dynamic Host Configuration Protocol (DHCP) server. When Autoconfiguration is enabled, Windows automatically assigns 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, see Renewing 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 Autoconfiguration IP address is displayed, it indicates possible broadband network problems or an improper connection between your computer and the SBG901. The Autoconfiguration 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

To renew 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. Click **Run** to open the Run dialog.
   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.

Wall Mounting the SBG901

Do the following to mount the SBG901 on the wall:

- 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).

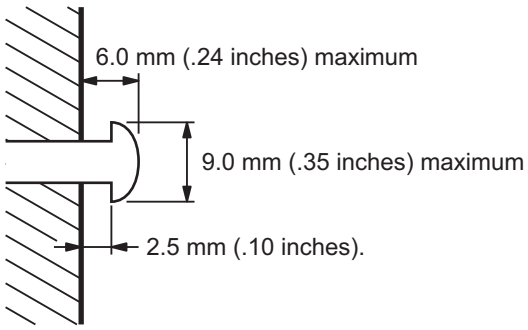
If possible, mount the unit to concrete, masonry, a wooden stud, or some other very solid wall material. Use anchors if necessary (for example, if you must mount the unit on drywall).

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

Make sure the AC power plug is disconnected from the wall outlet and all cables are removed from the back of the SBG901 before starting the installation.

You can mount the SBG901 horizontally or vertically. Do the following to mount your SBG901 on the wall:

1. Print a copy of the Wall Mounting Template.
2. Measure the printed template with a ruler to ensure that it is the correct size.
3. Use a center punch to mark the center of the holes.
4. On the wall, locate the marks for the mounting holes.
5. Drill the holes to a depth of at least 1 1/2 inches (3.8 cm). Use M3.5 x 38 mm (#6 x 11/2 inch) screws with a flat underside and maximum screw head diameter of 9.0 mm to mount the SBG901.
6. Using a screwdriver, turn each screw until part of it protrudes from the wall, as shown in the following wall mounting screw dimensions illustration.



   There must be .10 inches (2.5 mm) between the wall and the underside of the screw head.
7. Place the SBG901 so the keyholes on the back of the unit are aligned above the mounting screws.
8. Slide the SBG901 down until it stops against the top of the keyhole opening.

After mounting, reconnect the coaxial cable input and Ethernet connection. Plug the power cord into the +12VDC connector on the cable modem and the electrical outlet. Route the cables so that they are not a safety problem.

Wall Mounting Template

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

Be sure you print it at 100% scale. In the Print dialogue window, be sure that Scale to paper size is set to **No scaling** in the Print dialog box.

Measure the printed template with a ruler to ensure that it is the correct size.

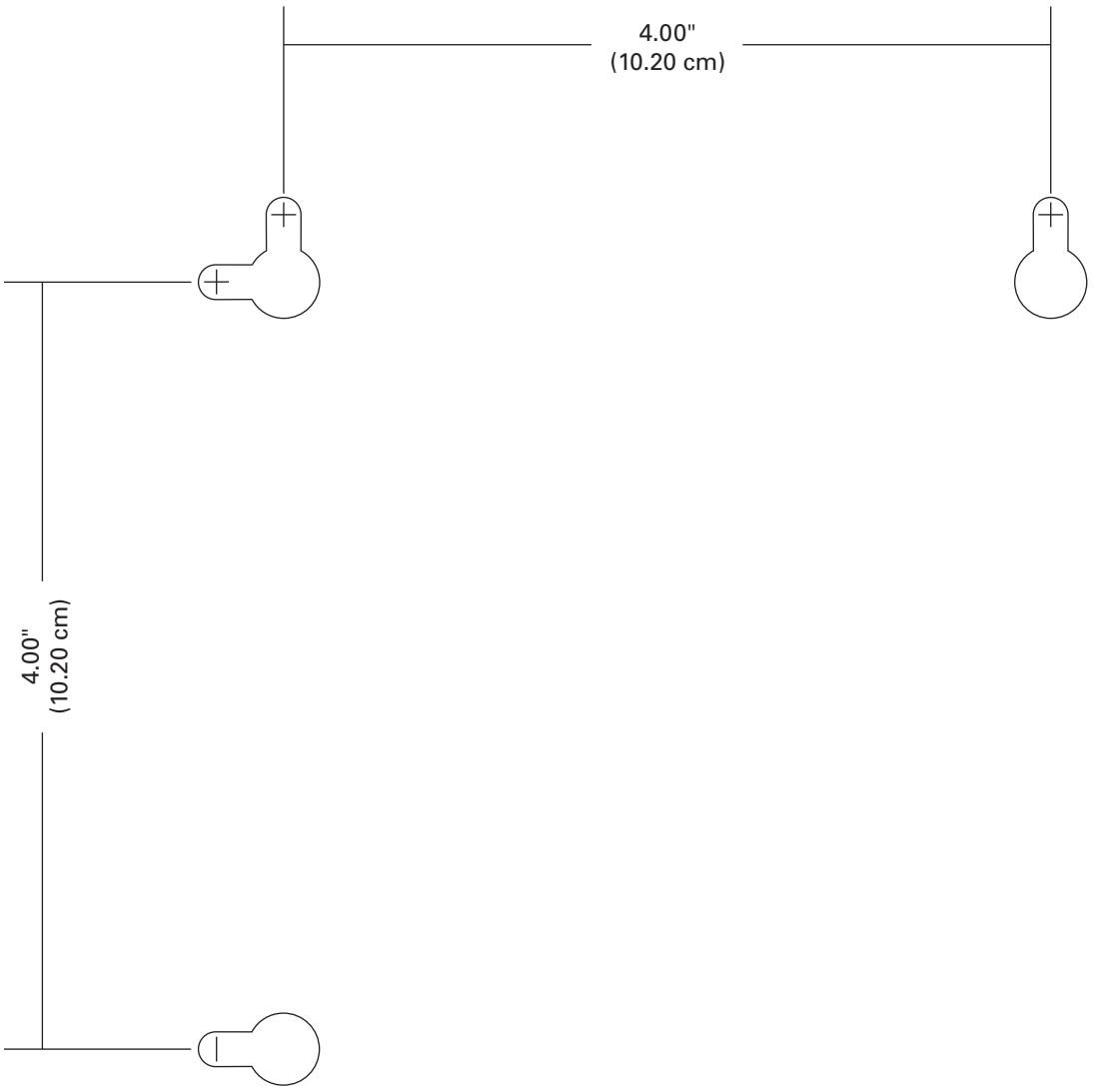


Figure 1 Wall Mounting Template

3 Basic Configuration

For more advanced configuration information, see Configuring TCP/IP 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 SBG901. See Changing the SBG901 Default Password.*
>
> *Firewalls are not foolproof. Choose the most secure firewall policy you can. See the Firewall Pages.*

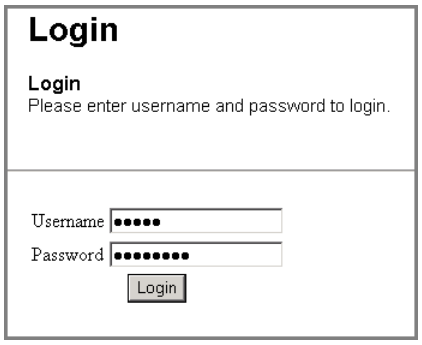
Starting the SBG901 Configuration Manager (CMGR)

The SBG901 Configuration Manager (CMGR) allows you to change and view the settings on your SBG901.

1. Open the web browser on a computer connected to the SBG901 over an Ethernet connection.

   > ***Note:*** *Do not attempt to configure the SBG901 over a wireless 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).



5. Click **Login** to display the SBG901 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 SBG901:

- RF Downstream Channel, which uses lower cable frequencies to transmit data
- RF Upstream Channel, which uses higher cable frequencies to receive data

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 SBG901 Configuration Manager (CMGR), see Troubleshooting for more information.

SBG901 Menu Options Bar

The SBG901 Menu Options bar is displayed along the top of the SBG901 Configuration Manager window. When a menu option is selected, a top-level page for that option is displayed.

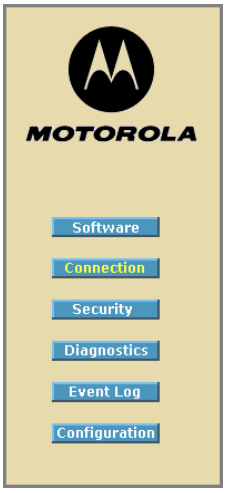
Configuration Manager Menu Options Bar

Menu Option Pages	Function
Status	Provides information about the SBG901 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 SBG901 user name and password.
Basic	Views and configures SBG901 IP-related configuration data, including Network Configuration, WAN Connection Type, DHCP, and DDNS. The Backup option allows you to save your SBG901 configuration on your computer.
Advanced	Configures and monitors how the SBG901 routes IP traffic
Firewall	Configures and monitors the SBG901 firewall
Parental Control	Configures and monitors the SBG901 parental control feature
Wireless	Configures and monitors SBG901 wireless networking features
Logout	Exits the SBG901 Configuration Manager

CAUTION: *To prevent unauthorized configuration, immediately change the default password when you first configure your Motorola SBG901.*

SBG901 Submenu Options

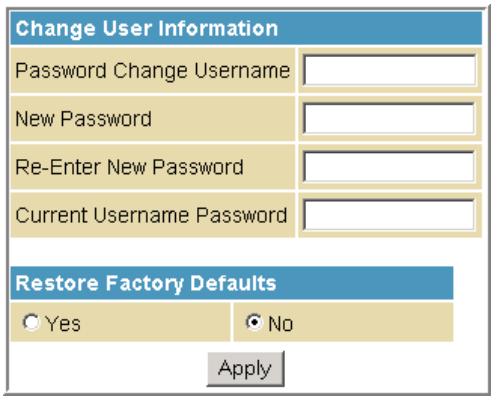
Additional features for each menu option are displayed by clicking a Submenu Option in the left panel of each page. When selected, the submenu option will be highlighted in yellow.



Changing the SBG901 Default Password

Do the following to change the default password:

1. On the SBG901 Status page, click the **Security** submenu option.



2. In the Password Change Username field, type your new User Name.
3. In the New Password field, type your new password (this field is case sensitive).
4. In the Re-Enter New Password field, type your new password again (this field is case sensitive).
5. In the Current Username Password field, type your old password.
6. Click **Apply** to save your changes.

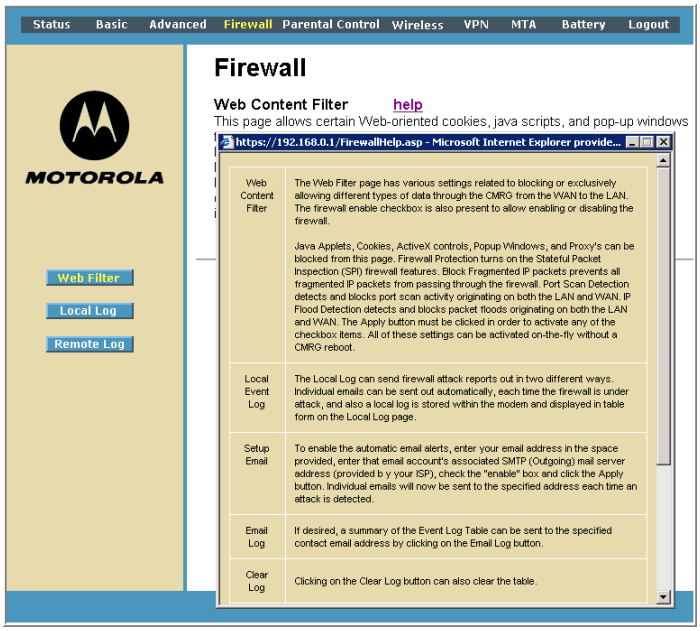
Restore Factory Defaults

To reset the user name and password back to the original factory settings:

1. Select **Yes**, and then click **Apply**.
2. You must login with the default user name, **admin**, and password, **motorola,** after applying this change. All entries are case-sensitive.

Getting Help

To retrieve help information for any menu option, click **help** on that page. See the sample Firewall help page shown below:



You can use the Windows scroll bar to view additional items on the help screens.

Gaming Configuration Guidelines

The following provides information about configuring the SBG901 firewall and DMZ for gaming.

Configuring the Firewall for Gaming

By default, the SBG901 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 SBG901 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 SBG901 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 can be designated as the gaming DMZ at once.

Exiting the SBG901 Configuration Manager

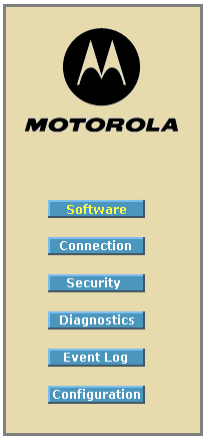
To logoff and close the SBG901 Configuration Manager:

- Click **Logout** on the SBG901 Menu Options bar.

4 Status Pages

The SBG901 Status pages provide information about the SBG901 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 SBG901 user name and password.

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



Status Software Page

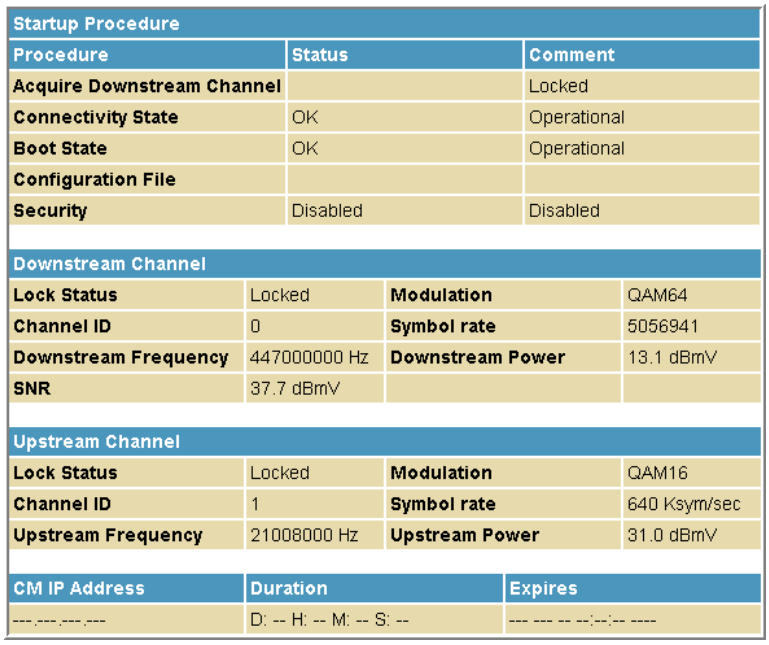
This page displays information about the hardware version, software version, MAC address, cable modem IP address, serial number, system "up" time, and network registration status.

Information	
Standard Specification Compliant	DOCSIS 2.0
Hardware Version	1
Software Version	SBG901N-2.0.2.1-LAB-01-SH
Cable Modem MAC Address	00:21:80:d2:80:12
Cable Modem Serial Number	16925871423344880101 2001
CM certificate	Installed
Status	
System Up Time	3 days 14h:01m:17s
Network Access	Allowed
Cable Modem IP Address	---.---.---.---

Status Connection Page

This page provides the HFC and IP network connectivity status of the SBG901 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

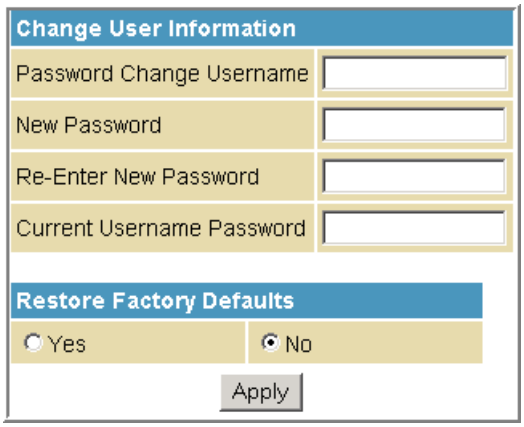
CM IP Address	Duration	Expires
---.---.---.---	D: -- H: -- M: -- S: --	--- --- -- --:--:-- ----

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 SBG901 user name and password. It also allows you to reset your user name and password to the default setting.



Changing the SBG901 Default Password

1. In the Password Change Username field, type your new User Name.
2. In the New Password field, type your new password (this field is case-sensitive).
3. In the Re-Enter New Password field, type your new password again (this field is case-sensitive).
4. In the Current Username Password field, type your old password.
5. Select **Yes** if you want to reset the user name and password to the original factory settings.
6. Click **Apply** to update the user name password.

> ***Note:*** *You must login with the default user name,* ***admin****, and password,* ***motorola****, after applying the restore factory settings change.*

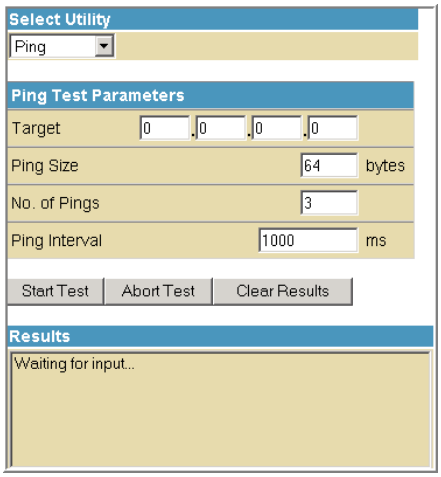
Status Diagnostics Page

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 SBG901 and other devices on the SBG901 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 SBG901.



Testing Network Connectivity with the SBG901

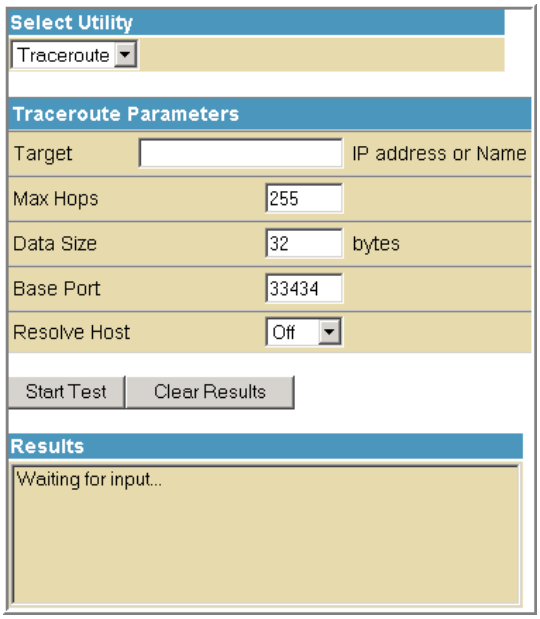
To check connectivity between the SBG901 and other devices on the SBG901 LAN, perform the following test:

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 between Ping send operations in milliseconds in the Ping Interval field.
6. Click **Start Test** to begin the Ping operation. The Ping results will 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 SBG901 Configuration Manager to a public host. Selecting Traceroute from the Select Utility drop-down list will present alternate controls for the Traceroute utility.



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

Field Descriptions for the Status Event Log Page

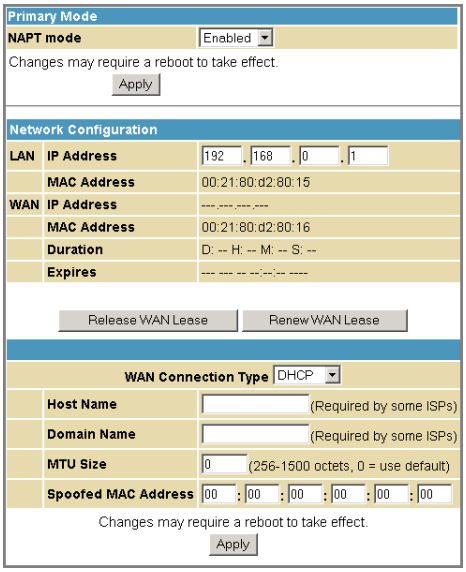
Field	Description
Time	Indicates the date and time the error occurred
Priority	Indicates the level of importance of the error
Description	A brief definition of the error

5 Basic Pages

The SBG901 Basic Pages allow you to view and configure SBG901 IP-related configuration data, including Network Configuration, WAN Connection Type, DHCP, and DDNS. The Backup option allows you to save a copy of your SBG901 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 SBG901 gateway related to your ISP connection.



Field Descriptions for the Basic Setup Page

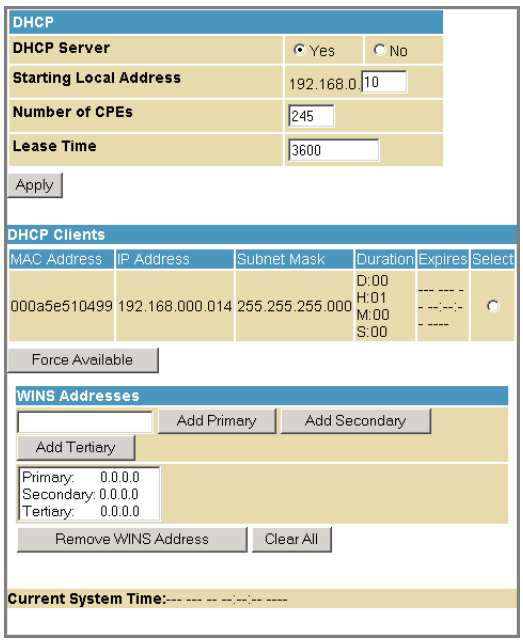
Field	Description
NAPT mode	NAPT is a special case of NAT, where many IP numbers are hidden behind a number of addresses. In contrast to the original NAT, however, this does not mean there can be only that number of connections at a time. In NAPT mode, an almost arbitrary number of connections are multiplexed using TCP port information. The number of simultaneous connections is limited by the number of addresses multiplied by the number of available TCP ports.

Field	Description
LAN	
IP Address	Enter the IP address of the SBG901 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 SBG901 Access Point.
WAN	
IP Address	The public WAN IP address of your SBG901 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 SBG901 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 SBG901 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 SBG901 DHCP Server. Select **No** to disable the SBG901 DHCP Server.
Starting Local Address	Enter the starting IP address to be assigned by the SBG901 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 SBG901 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 SBG901 DHCP server leases an IP address to a client. The default is 3600 seconds (60 minutes).
DHCP Clients	Lists DHCP client device information.

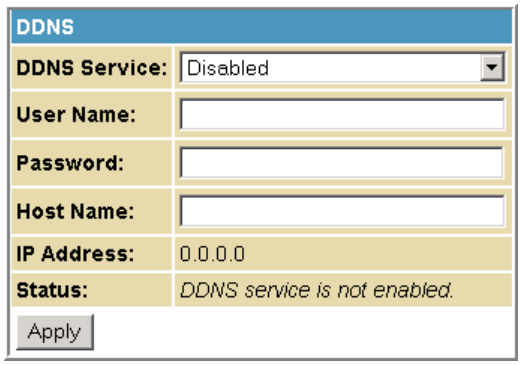
Field	Description
WINS Addresses	Specifies up to three Windows Internet Name Service (WINS) Server Addresses.

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 SBG901 to be more easily accessed from various locations on the Internet.



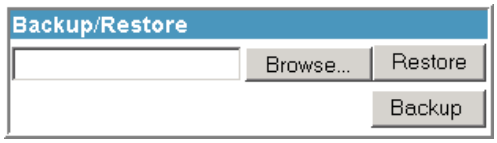
Field Descriptions for Basic DDNS Page

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 SBG901 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 SBG901 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 SBG901 settings.

Backing Up Your SBG901 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 SBG901 settings.

6 Advanced Pages

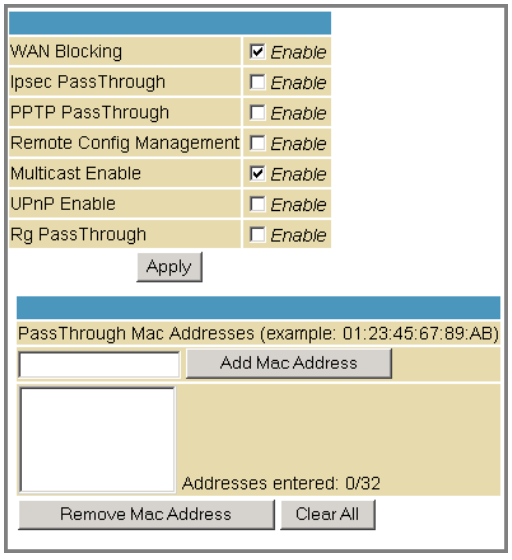
The SBG901 Advanced Pages allow you to configure the advanced features of the SBG901:

- 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 SBG901 device routes IP traffic.



Field Descriptions for the Advanced Options Page

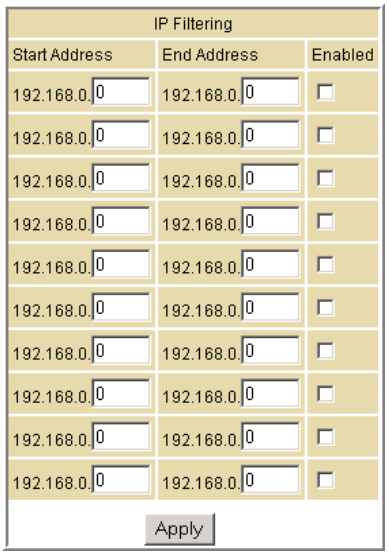
Field	Description
WAN Blocking	Prevents the SBG901 Configuration Manager or the PCs behind it from being visible to other computers on the SBG901 WAN. Checkmark **Enable** to turn on this option.
IPsec PassThrough	Enables the IPsec Pass-Through protocol to be used through the SBG901 Configuration Manager so that a VPN device (or software) may communicate properly with the WAN. Checkmark **Enable** to turn on this option.
PPTP PassThrough	Enables the Point-to-Point Tunneling Protocol (PPTP) Pass-Through protocol to be used through the SBG901 Configuration Manager so that a VPN device (or software) may communicate properly with the WAN. Checkmark **Enable** to turn on this option.
Remote Config Management	Allows remote access to the SBG901 Configuration Manager. This enables you to configure the SBG901 WAN by accessing the WAN IP address at Port 8080 of the configuration manager from anywhere on the Internet. For example, in the browser URL window, type **http://WanIPAddress:8080/** to access the SBG901 Configuration Manager remotely. Checkmark **Enable** to turn on this option.
Multicast Enable	Allows multicast-specific traffic (denoted by a multicast specific address) to be passed to and from the PCs on the private network behind the configuration manager. Checkmark **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. Checkmark **Enable** to turn on this option.
Rg PassThrough	Disables NAT operation allowing all client computers to act as passthrough clients. Checkmark **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 SBG901 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 that you only need to enter the LSB (Least-significant byte) of the IP address; the upper bytes of the IP address are set automatically from the SBG901 Configuration Manager's IP address.

The Enabled option allows you to store filter settings commonly used but not have them active.



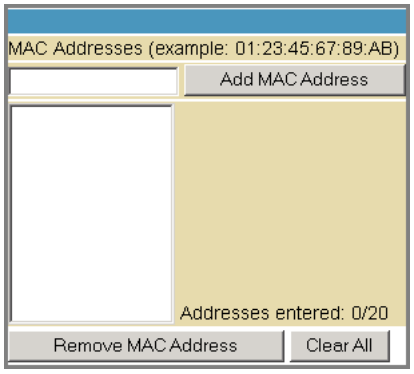
Field Descriptions for the Advanced IP Filtering Page

Field	Description
Start Address	Enter the starting IP address range of the computers for which you want to deny access to the SBG901 WAN. Be sure to 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 SBG901 WAN. Be sure to only enter the least significant byte of the IP address.
Enabled	Activates the IP address filter, when selected. Checkmark **Enabled** for each range of IP addresses you want to deny access to the SBG901 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.

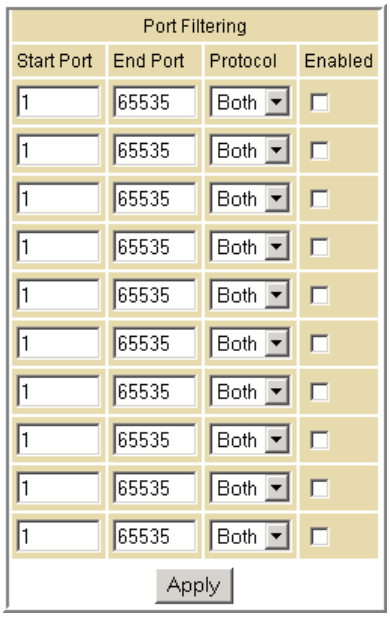
Setting a MAC Address Filter

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, if you wanted to block all PCs on the private LAN from accessing HTTP sites (or "web surfing"), you would set the "Start Port" to 80, "End Port" to 80, "Protocol" to TCP, checkmark Enabled, and then click* ***Apply.***

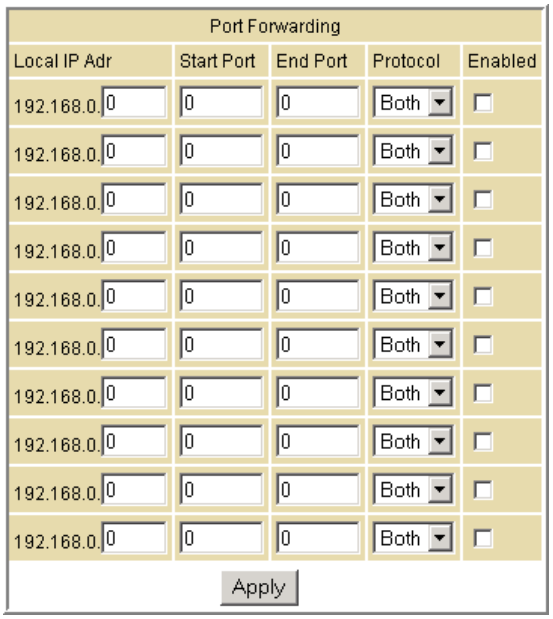


Field Descriptions for the Advanced Port Filtering Page

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	Checkmark 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.



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

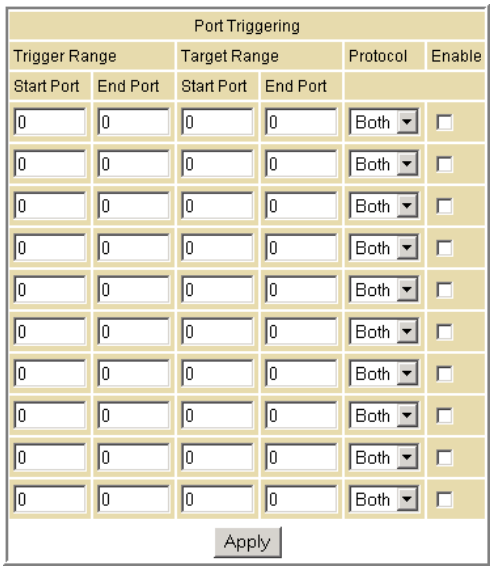
- HTTP: 80
- FTP: 20, 21
- Secure Shell: 22
- Telnet: 23
- SMTP e-mail: 25
- SNMP: 161

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, voice, 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.

Field	Description
Protocol	Select **TCP**, **UDP**, or **Both** from the drop-down list.
Enable	Select checkbox 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.

You may configure one PC to be the DMZ host. This setting is generally used for PCs using problem applications that use random port numbers and do not function correctly with specific port triggers or the port forwarding setups mentioned earlier. If a specific PC is set as a DMZ Host, remember to set this back to 0 when you are finished with the needed application, since this PC will be effectively exposed to the public Internet, though still protected from Denial of Service (DoS) attacks via the Firewall.

Setting Up the DMZ Host

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

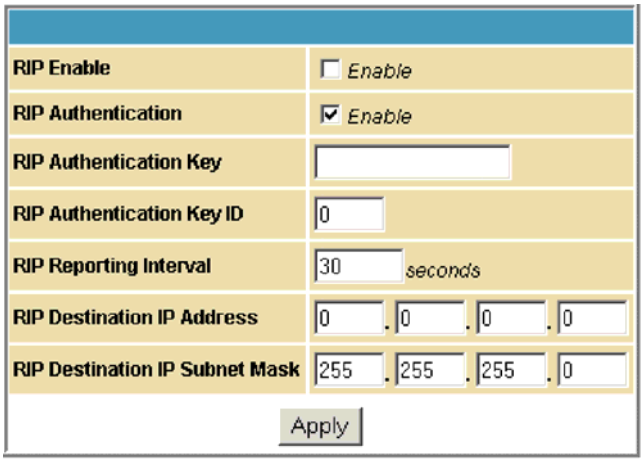
Advanced Routing Information Protocol Setup Page

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 is normally a function that is tightly controlled via the ISP. RIP Authentication Keys and IDs are normally held as secret information from the end user to prevent unauthorized RIP settings.*



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 now considered obsolete since newer routing protocols, such as OSPF and ISIS, have been introduced.
RIP Authentication	If this field is 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

Field	Description
	packet, and it also indicates the authentication algorithm.
RIP Reporting Interval	Determines how long before a RIP packet is sent out 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.

7 Firewall Pages

The SBG901 Firewall Pages allow you to configure the SBG901 firewall filters and firewall alert notifications. The SBG901 firewall protects the SBG901 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.

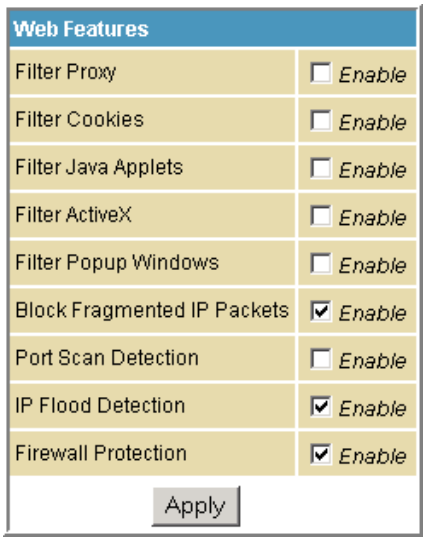
The predefined policies provide outbound Internet access for computers on the SBG901 LAN. The SBG901 firewall uses stateful-inspection to allow inbound responses when there already is an outbound session running that corresponds to the data flow. For example, if you use a web browser, outbound HTTP connections are permitted on port 80. Inbound responses from the Internet are allowed because an outbound session is established.

When required, you can configure the SBG901 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.



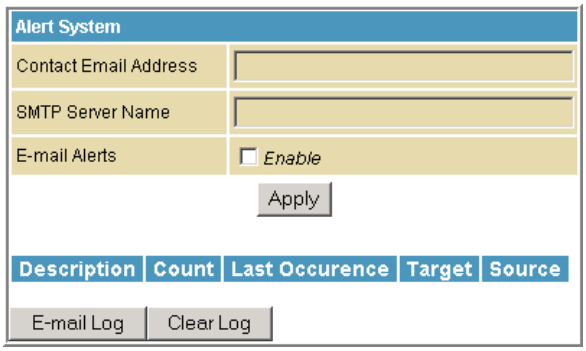
Checkmark **Enable** for each Web filter you want to set for the firewall, and then click **Apply**. The Web filters will activate without having to reboot the SBG901 Configuration Manager.

> ***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

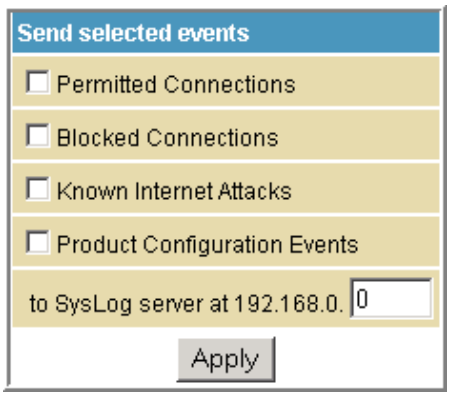


Field Descriptions for the Firewall Local Log Page

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 would be hard-coded so that the address does not change and always agrees with the entry on this page.



Field Description for the Firewall Remote Log Page

Field	Description
Permitted Connections	Check for the server to e-mail you logs of who is connecting to your network.
Blocked Connections	Check for the server to e-mail you logs of who is blocked from connecting to your network.
Known Internet Attacks	Check for the server to e-mail you logs of known Internet attacks against your network.
Product Configuration Events	Check 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**.

8 Parental Control Pages

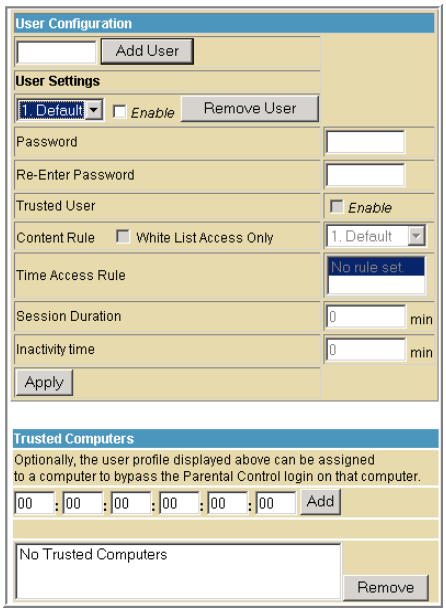
The SBG901 Parental Control Pages allow you to configure access restrictions to a specific device connected to the SBG901 LAN.

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

Parental Control User Setup Page

This page is the master 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. The user must enter their password only the first time to access the Internet. It is not necessary to enter the password each time a new web page is accessed. 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. These timed logins ensure that a specific user uses the Internet gateway appropriately.



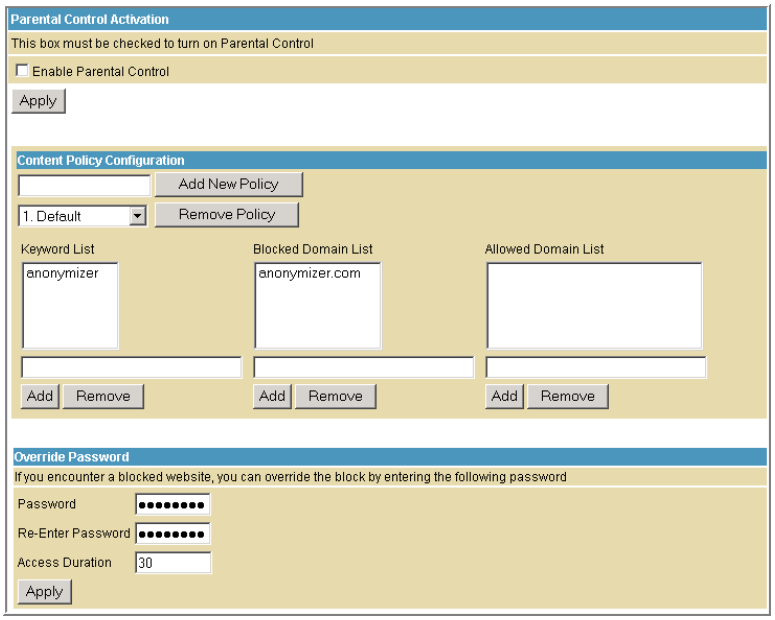
Field Descriptions for the Parental Control User Setup Page

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. Checkmark **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. Checkmark **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. Check **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.



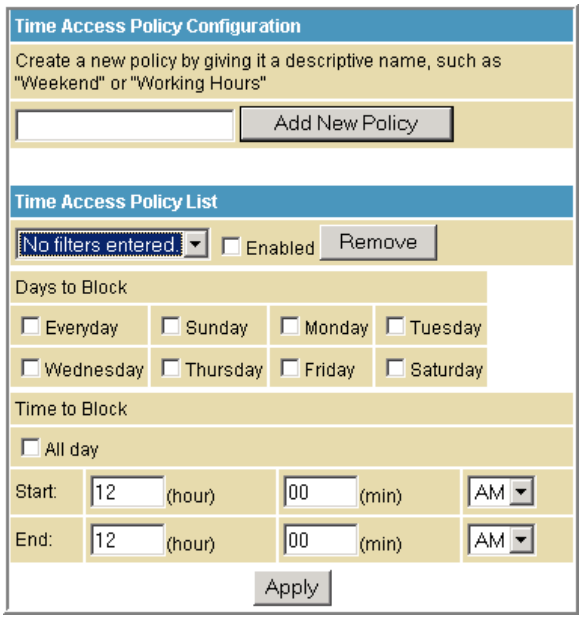
After you have changed your Parental Control settings, click the appropriate **Apply**, **Add**, or **Remove** button.

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 SBG901 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.



Once each category change has been made, the user must 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 can be 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

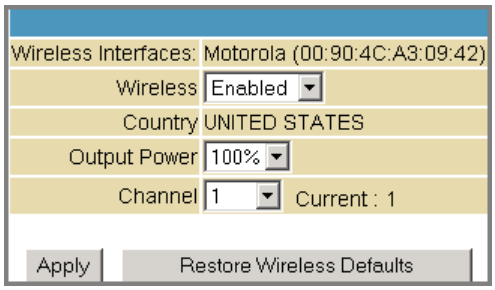
9 Wireless Pages

The SBG901 Wireless Pages allow you to configure your wireless LAN (WLAN).

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

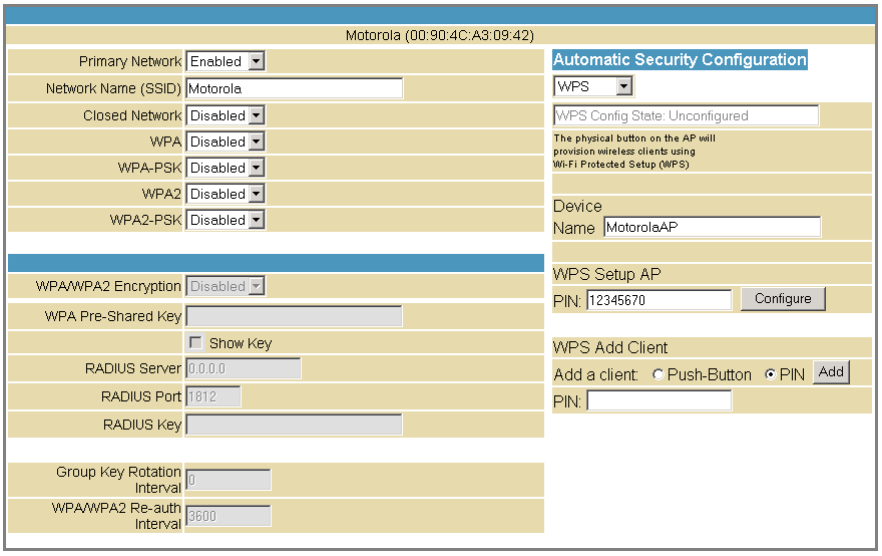


Field Descriptions for the Wireless 802.11 Radio Page

Field	Description
Wireless Interfaces	Shows the MAC address of the installed wireless card. It is 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 SBG901.

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

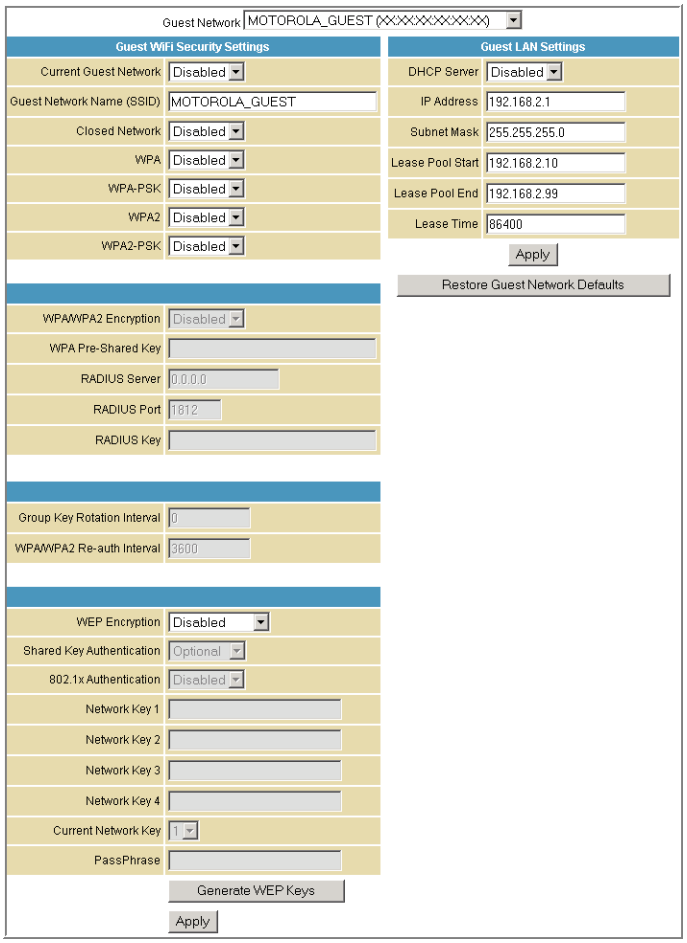
Field	Description
Primary Network	When set to **Enabled**, beacon frames are transmitted with the Primary Network SSID.
Network Name (SSID)	Sets the Network Name (also known as SSID) of the Primary wireless network. This is a 1-32 ASCII character string.
Closed Network	With a closed network, users type 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.

Field	Description
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 Shared Key Authentication, which is an 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 will decrypt the encrypted text and then compare the decrypted message with the original challenge text. If they are the same, the access point will let the CPE connect; if it doesn't match, then the access point does not let the CPE connect.

Field	Description
802.1x Authentication	This is another type of authentication and is used on top of WEP. 802.1x Authentication 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 will be isolated from the private LAN and can only communicate with WAN hosts.



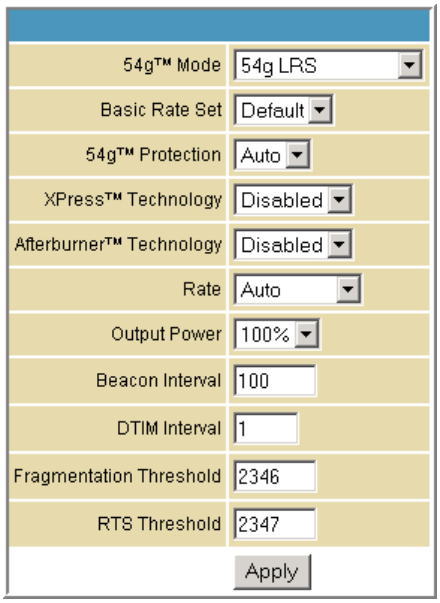
Field Descriptions for the Wireless 802.11 Guest Network Page

Field	Description
Guest Network	You may have several different wireless Guest Networks running with different options. This field lets you select which wireless Guest Network you want to modify.
Current Guest Network	When set to **Enabled**, beacon frames are transmitted with the Guest SSID

Field	Description
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 slightly 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.



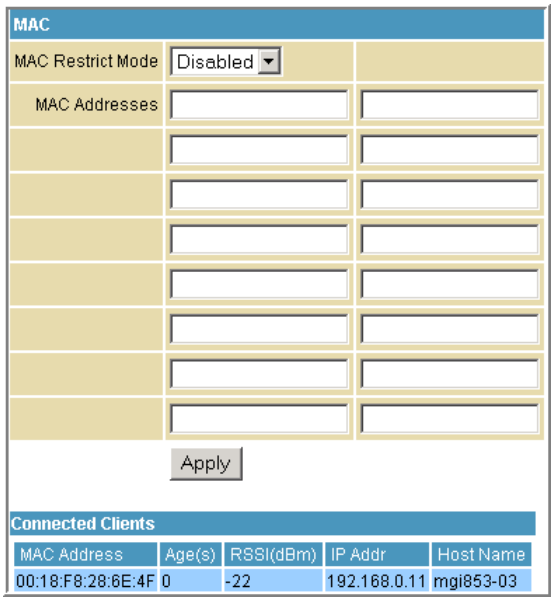
Field Descriptions for the Wireless 802.11 Advanced Page

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 will use 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	This is a performance-enhancing Wi-Fi technology designed for increasing throughput and efficiency. It is used when there

Field	Description
	are mixed wireless networks in the surrounding area from 802.11a/b/g networks.
Afterburner™ Technology	This is also 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 will be fragmented into packets no larger than the threshold before packet transmission.
RTS Threshold	Sets the RTS threshold. Packets exceeding this threshold will 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.

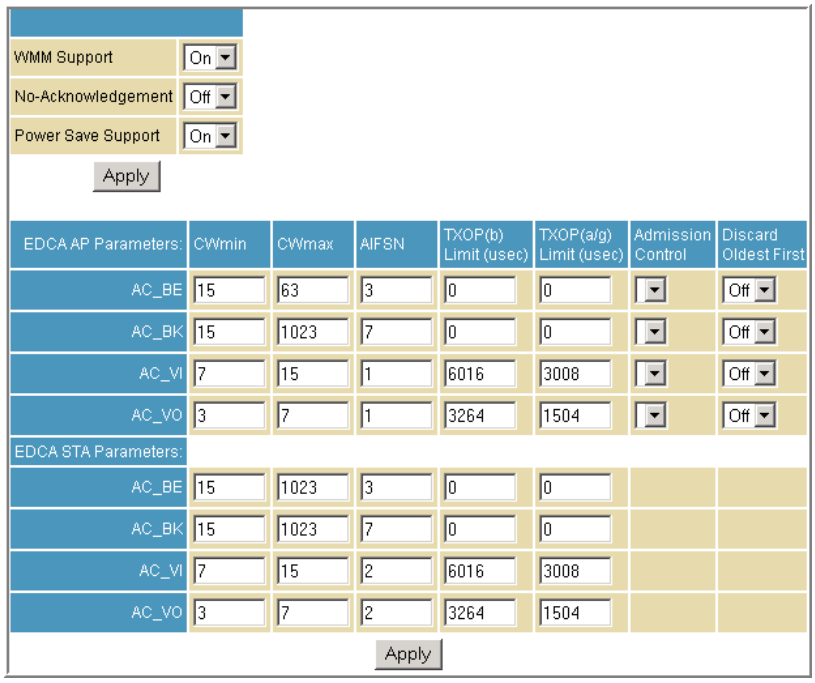


Field Descriptions for the Wireless 802.11 Access Control Page

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	A list of connected wireless clients. When a client connects (associates) to the network, it is added to the list; when a client leaves (disassociates) from the network, it 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).



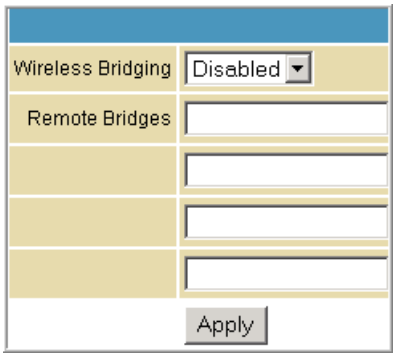
Field Descriptions for the Wireless 802.11 Wi-Fi Multimedia Page

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.

Field	Description
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) 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.



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 SBG901 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 SBG901:

- 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 SBG901 Ethernet port to perform configuration. Do not attempt to configure the SBG901 over a wireless connection.

You need to configure each wireless client (station) to access the SBG901 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 SBG901	Required on Each Wireless Client
If all of your wireless clients support Wi-Fi Protected Access (WPA), Motorola recommends configuring WPA on the SBG901	If you use a local pre-shared key (WPA-PSK) passphrase, you must configure the identical passphrase to the SBG901 on each wireless client. Home and small-office settings typically use a local passphrase.
Otherwise, configure WEP on the SBG901	You must configure the identical WEP key to the SBG901 on each wireless client.

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

- Provides much stronger encryption and is more secure
- Provides authentication to ensure that only authorized users can log in to your WLAN
- Is much easier to configure
- Uses a standard algorithm on all compliant products to generate a key from a textual passphrase
- Will be incorporated into the new IEEE 802.11i wireless networking standard

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

Installing Wireless Clients

> ***Note**: Use the SBG901 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.
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 SBG901	Configuring a Wireless Client for WPA or WPA2
Configuring WEP on the SBG901	Configuring a Wireless Client for WEP
Configuring the Wireless Network Name on the SBG901	Configuring a Wireless Client with the Network Name (SSID)
Configuring a MAC Access Control List on the SBG901	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 SBG901, you must configure the same passphrase (key) on each wireless client. The SBG901 cannot authenticate a client if:

- WPA is enabled on the SBG901, but not on the client
- The client passphrase does not match the SBG901 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 SBG901, you must configure the same WEP key on each wireless client. The SBG901 cannot authenticate a client if:

- Shared Key Authentication is enabled on the SBG901 but not on the client
- The client WEP key does not match the SBG901 WEP key

For all wireless adapters, you must enter the 64-bit or 128-bit WEP key generated by the SBG901.

> ***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 SBG901 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 SBG901.

10 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 SBG901. Resetting the SBG901 may take five 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 1 – Troubleshooting Solutions

Problem	Possible Solution
Power light is off	Check that the SBG901 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 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 SBG901 and wall outlet. Hand-tighten if necessary. Check the IP address. Follow the steps for verifying the IP address for your system described in Configuring TCP/IP. Call your service provider if you need an IP address. Check that the Ethernet cable is properly connected to the SBG901 and the computer. If a device is connected via the Ethernet port, verify connectivity by checking the LINK LEDs on the rear panel.

Problem	Possible Solution
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 SBG901, 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 SBG901, 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 SBG901. • 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 SBG901 front panel LEDs provide status information for the following error conditions:

Table 2 – Front-Panel LEDs and Error Conditions

LED	Status	If, During Startup:	If, During Normal Operation:
POWER	OFF	SBG901 is not properly plugged into the power outlet	The SBG901 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

A Product Specifications

All features, functionality, and other product specifications are subject to change without notice or obligation.

Certain features may not be activated by your service provider and/or their network settings may limit the feature's functionality. Additionally, certain features may require a subscription. Contact your service provider for details. All features, functionality, and other product specifications are subject to change without notice or obligation.

GENERAL	
Standards	Interoperates with DOCSIS
Cable Interface	F-connector, female, 75 Ω
Network Interface	One 10/100 Ethernet port
Wireless Interface	802.11b/g Wi-Fi
Dimensions	146 mm x 146 mm x 38 mm (5.7 in x 5.7 in x 1.5 in)
INPUT POWER	
North America	105 to 125 VAC, 60 Hz
Outside North America	90 to 264 VAC, 45 to 65 Hz
ENVIRONMENT	
Operating Temperature	0° C to 40° C (32° F to 104° F)
Storage Temperature	–30° C to 70° C (–22° F to 158° F)
Operating Humidity	0 to 95% R.H. (non-condensing)
DOWNSTREAM	
Modulation	64 or 256 QAM
Maximum Data Rate*	38 Mbps (256 QAM at 5.361 Msym/s)
Bandwidth	6 MHz
Symbol Rates	64 QAM at 5.069 Msym/s, 256 QAM at 5.361 Msym/s
Operating Level Range	–15 to 15 dBmV
Frequency Range	88 to 860 MHz
Input Impedance	75 Ω (nominal)

**When comparing download speeds with a traditional 28.8k analog modem. Actual speeds will vary and are often less than the maximum possible. Several factors affect upload and download speeds, including, but not limited to, network traffic and services offered by your cable operator or broadband service provider, computer equipment, type of service, number of connections to server, and availability of Internet route(s).*

UPSTREAM	
Modulation	8***, 16, 32***, 64***,128*** QAM or QPSK
Maximum Channel Rate	30 Mbps**
Bandwidth	200 kHz, 400 kHz, 800 kHz, 1.6 MHz, 3.2 MHz, 6.4 MHz***
Symbol Rates	160, 320, 640, 1280, 2560, 5120*** ksym/s
Operating Level Range	
A-TDMA	8 to 54 dBmV (32, 64 QAM), 8 to 55 dBmV (8, 16 QAM) , 8 to 58 dBmV (QPSK)
S-CDMA	8 to 53 dBmV (all modulations)
Output Impedance	75 Ω (nominal)
Frequency Range	5 to 42 MHz (edge to edge) 5-65 for Euro-DOCSIS

***Actual data throughput will be less due to physical layer overhead (error correction coding, burst preamble, and guard interval).*

****With A-TDMA or S-CDMA enabled Cable Modem Termination System (CMTS).*

NETWORK	
Gateway	DHCP, NAT; static routing and dynamic IP routing (RIPv1, RIPv2); SPI firewall with DoS protection and intrusion prevention; port, packet, and URL keyword filtering; full suite of ALGs; UPnP IGD 1.0
Wireless LAN	802.11b/g Wi-Fi, two internal antennas, WDS bridging, 802.11e WMM admission control, QoS
Power Management	802.11e WMM power save/U-APSD (Unscheduled-Automatic Power Save Delivery)
802.11i Security	WEP-64/128, WPA-PSK, WPA, WPA2, TKIP, AES, 802.1x, 802.11i (pre-authentication)
Mobile Pairing	User-friendly Wi-Fi–protected setup (WPS) for secure mobile pairing with compatible dual-mode handset
Regulatory Domains	To include US, Canada, ETSI, World
Transmit Power Output	19 dBm +1/–1.5 dB at all rates in all channels
IEEE 802.11b	16 dBm +1/–1 dB at 54 Mbps in all channels
IEEE 802.11g	> –90 dBm at 11 Mbps;
Receiver Sensitivity	> –74 dBm at 54 Mbps

B

Glossary

This glossary defines some of the terms and acronyms used in this document.

TERM	DEFINITION
Authentication	A process where the CMTS verifies that access is authorized, using a password, trusted IP address, or serial number.
cable modem	A device installed at a subscriber location to provide data communications over an HFC network. Unless otherwise specified, all references to "cable modem" in this documentation refer to DOCSIS cable modems only.
coaxial cable	A type of cable consisting of a center wire surrounded by insulation and a grounded shield of braided (coax) wire. The shield minimizes electrical and radio frequency interference. Coaxial cable has high bandwidth and can support transmission over long distances.
DHCP	Dynamic Host Configuration Protocol server — dynamically assigns IP addresses to client hosts on an IP network. DHCP eliminates manually assigning static IP addresses by "leasing" an IP address and subnet mask to each client. It enables the automatic reuse of unused IP addresses. The SBG901 is simultaneously a DHCP client and a DHCP server. A DHCP server at the cable system headend assigns a public IP address to the SBG901 and optionally to clients on the SBG901 LAN. The SBG901 contains a built-in DHCP server that assigns private IP addresses to clients.
DMZ	A "de-militarized zone" is one or more hosts logically located between a private LAN and the Internet. A DMZ prevents direct access by outside users to private data. (The term comes from the geographic buffers located between some conflicting countries, such as North and South Korea.) In a typical small DMZ configuration, the DMZ host receives requests from private LAN users to access external web sites and initiates sessions for these requests. The DMZ host cannot initiate a session back to the private LAN. Internet users outside the private LAN can access only the DMZ host. You can use a DMZ to set up a web server or for gaming without exposing confidential data.
downstream	In a cable data network, this is the direction of the data received by the computer from the Internet.
firewall	A security software system on the SBG901 that enforces an access control policy between the Internet and the SBG901 LAN.

TERM	DEFINITION
gateway	A device that enables communication between networks using different protocols. The SBG901 enables up to 245 computers supporting IEEE 802.11b/g or Ethernet to share a single broadband Internet connection.
ISP	Internet Service Provider
MAC address	The Media Access Control address is a unique, 48-bit value permanently saved in ROM at the factory to identify each Ethernet network device. It is expressed as a sequence of 12 hexadecimal digits printed on a label on the bottom of the SBG901. You need to provide the HFC MAC address to the Internet Service provider. Also called an Ethernet address, physical address, hardware address, or NIC address.
NAT	Network Address Translation is an Internet standard for a LAN to use one set of IP addresses for internal traffic and a second set of IP addresses for external traffic.
pass-through	A pass-through client on the SBG901 LAN obtains its public IP address from the Internet Service provider's DHCP server.
port mirroring	A feature that enables one port (source) on the SBG901 to be copied to another port (destination) to be studied. The destination mirrors the transmitted (from) or received (to) data on the source port to enable the person managing the network to monitor activity.
port triggering	A mechanism that allows incoming communication with specified applications. Primarily used for gaming applications.
private IP	An IP address assigned to a computer on the SBG901 LAN by the DHCP server on the SBG901 for an address-specified lease time. Private IP addresses are used by the SBG901 LAN only; they are invisible to devices on the Internet. See also public IP address.
public IP address	The IP address assigned to the SBG901 by the Internet Service provider. A public IP address is visible to devices on the Internet. See also private IP address.
QoS	Quality of service describes the priority, delay, throughput, and bandwidth of a connection.
RJ-11	The most common type of connector for household or office phones.
RJ-45	An 8-pin modular connector; this is the most common connector type for 10Base-T or 100Base-T Ethernet networks.

TERM	DEFINITION
stateful-inspection	A type of firewall that tracks each connection, traversing all firewall interfaces to ensure validity. In addition to examining the source and destination in the packet header based on static rules, a stateful inspection firewall: • Examines packet headers via the context established by previous packets that traversed the firewall • Monitors the connection state and saves it in a table • Closes ports until a connection to a specific port is requested • May examine the packet contents up through the application layer to determine more than just the source and destination A stateful inspection firewall is more advanced than a static filter firewall.
subscriber	A home or office user who accesses television, data, or other services from an Internet Service provider.
synchronous	The SBG901 uses synchronous timing for upstream data transmissions. The CMTS broadcasts timing messages that bandwidth is available. The SBG901 reserves data bytes requiring x number of mini-slots. The CMTS replies that it can receive data at a specified time (synchronized). At the specified time, the SBG901 transmits the x-number of data bytes.
upstream	In a cable data network, upstream describes the direction of data sent from the subscriber's computer through the cable modem to the CMTS and the Internet.
Wireless Cable Modem Gateway	The Motorola SURFboard Wireless Cable Modem Gateway is a single device that combines a cable modem, router, Ethernet switch, wireless access point, and DHCP server for SOHO or SME use.
WPA	Wi-Fi Protected Access (WPA) encryption, as described on the Wi-Fi Alliance web page: http://www.wifialliance.org. It is a far more robust form of encryption than WEP. Motorola recommends using WPA if all of your client hardware supports WPA.

C Software License

SURFboard SBG901 Wireless Cable Modem Gateway

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

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.

Motorola, Inc.
101 Tournament Drive
Horsham, PA 19044 U.S.A.

http://www.motorola.com

558660-001-c
05/2009