

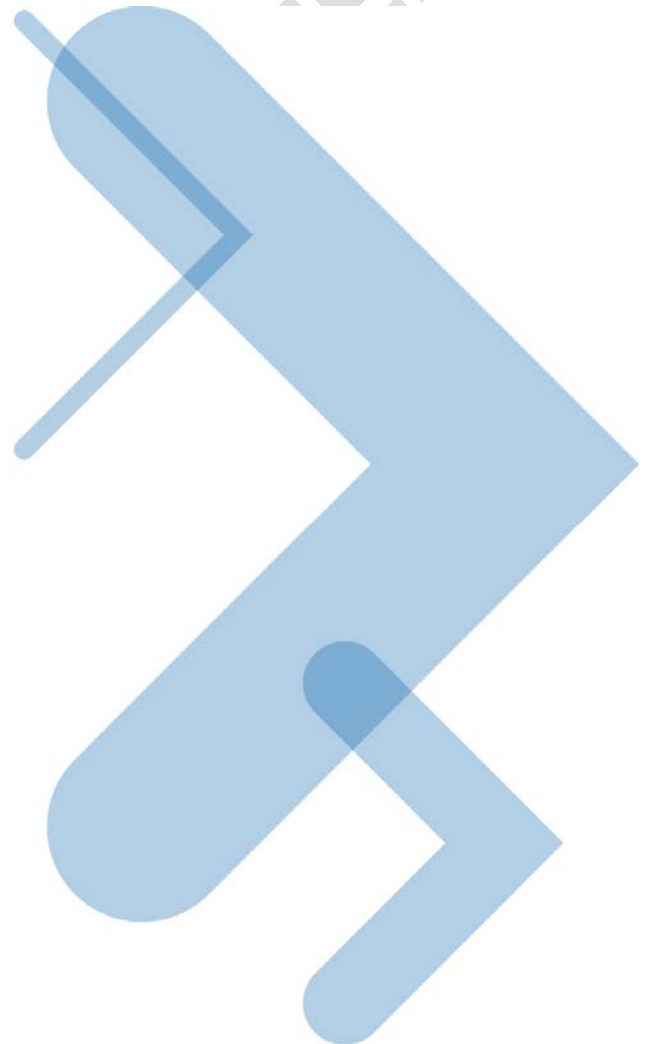


Motorola SURFboard[®]

SBG901 Wireless Cable Modem Gateway

User Guide

UNCOV





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 systems 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 40° C.

SAVE THESE INSTRUCTIONS

Note to CATV System Installer: This reminder is provided to call the CATV system installer's attention to Section 820-93 of the National Electric Code, which provides guidelines for proper grounding and, in particular, specifies that the coaxial cable shield shall be connected to the grounding system of the building, as close to the point of cable entry as practical.

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 operation 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 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. Please read the SBG901 User Guide or visit the Motorola website to learn how to protect your network.

INTERNATIONAL DECLARATION OF CONFORMITY

We, Motorola, Inc., 101 Tournament Drive, Horsham, PA 19044, U.S.A., declare under our sole responsibility that the SBG901 to which this declaration relates is in conformity with one or more of the following standards:

EN55022	EN55024	EN60950-1	EN61000-3-2	EN61000-3-3
CISPR-22	CISPR-24	IEC 60950-1	ETSI EN 300 328	ETSI EN 301 489-1/-17

and the following provisions of the Directive(s) of the Council of the European Union: WEEE Directive 2002/96/EC, R&TTE 1999/5/EC, RoHS Directive 2005/95/EC



Models

SBG901, SBG901 Diagnostic

Standards

FCC Part 15, ICES-003

UL60950-1, CAN/CSA-C22.2 No. 60950-1

EN55022, EN55024, CISPR22, CISPR24, EN61000-3-2,
EN61000-3-3, EN60950-1, IEC60950-1, ETSI EN 300 328,
ETSI EN 301 489-1/-17

© 2008 Motorola, Inc. All rights reserved. No part of this publication may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from Motorola, Inc.

MOTOROLA and the Stylized M logo are registered in the US Patent & Trademark Office. SURFboard is a registered trademark of General Instrument Corporation, a wholly-owned subsidiary of Motorola, Inc. Microsoft, Windows, Windows NT, Windows Vista, Internet Explorer, DirectX, and Xbox LIVE are registered trademarks of Microsoft Corporation; and Windows XP is a trademark of Microsoft Corporation. Linux® is a registered trademark of Linus Torvalds in the U.S. and other countries. UNIX is a registered trademark of the Open Group in the United States and other countries. Macintosh is a registered trademark of Apple Computer, Inc. Adobe, Adobe Acrobat, and Adobe Acrobat Reader are registered trademarks of Adobe Systems, Inc. All other product or service names are property of their respective owners. No part of the contents of this document may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

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.



Contents

Safety and Regulatory Information

Introduction

SBG901 Features	13
Easy Setup	14
Network Connection Types.....	14
Powerful Features in a Single Unit.....	14
Sample Hybrid LAN	15
Optional Accessories	15
Front Panel	16
Rear Panel	17
Bottom Label on the SBG901	18
SBG901 LAN Choices	18
Wireless LAN.....	19
Wired Ethernet LAN	20
Security	20
Firewall	21
DMZ.....	21
Port Triggering	21
Wireless Security.....	22
Port Forwarding	22

Getting Started

Before You Begin	23
Precautions.....	24
Signing Up for Service.....	24
Computer System Requirements	25
Connecting the SBG901 to the Cable System.....	25
Cabling the LAN	26
Obtaining an IP Address for an Ethernet Connection	27
Configuring TCP/IP	27
Configuring TCP/IP in Windows 2000	27
Configuring TCP/IP in Windows XP	30



Configuring TCP/IP in Windows Vista.....	32
Verifying the IP Address in Windows 2000 or Windows XP	34
Verifying the IP Address in Windows Vista	35
Renewing Your IP Address	35
Wall Mounting the SBG901	36
Wall Mounting Template	38
Basic Configuration	
Starting the SBG901 Configuration Manager (CMGR).....	40
SBG901 Menu Options Bar.....	42
SBG901 Submenu Options	42
Changing the SBG901 Default Password	43
Restore Factory Defaults.....	43
Getting Help	44
Gaming Configuration Guidelines	44
Configuring the Firewall for Gaming.....	44
Configuring Port Triggers.....	45
Configuring a Gaming DMZ Host	45
Exiting the SBG901 Configuration Manager	45
Status Pages	
Status Software Page	47
Status Connection Page.....	48
Status Security Page	49
Changing the SBG901 Default Password.....	49
Status Diagnostics Page	49
Ping Utility.....	50
Traceroute Utility	51
Status Event Log Page.....	52
Basic Pages	
Basic Setup Page	53
Basic DHCP Page.....	55
Basic DDNS Page.....	56
Basic Backup Page.....	57
Restoring Your SBG901 Configuration	57



Backing Up Your SBG901 Configuration	58
Advanced Pages	
Advanced Options Page	59
Advanced IP Filtering Page	61
Advanced MAC Filtering Page	62
Setting a MAC Address Filter	62
Advanced Port Filtering Page	63
Advanced Port Forwarding Page	64
Advanced Port Triggers Page	65
Advanced DMZ Host Page	66
Setting Up the DMZ Host	66
Advanced Routing Information Protocol Setup Page	67
Firewall Pages	
Firewall Web Content Filter Page	69
Firewall Local Log Page	71
Firewall Remote Log Page	72
Parental Control Pages	
Parental Control User Setup Page	73
Parental Control Basic Setup Page	75
Parental Control ToD Access Policy Page	76
Parental Control Event Log Page	77
Wireless Pages	
Setting Up Your Wireless LAN	79
Encrypting Wireless LAN Transmissions	80
Wireless 802.11b/g Basic Page	81
Wireless 802.11b/g Privacy Page	83
Wireless 802.11b/g Access Control Page	86
Wireless 802.11b/g Advanced Page	87
Wireless Bridging Page	89
Wireless 802.11b/g Wi-Fi Multimedia Page	90
Wireless 802.11b/g Guest Network Page	92
Configuring the Wireless Clients	94
Configuring a Wireless Client for WPA	94
Configuring a Wireless Client for WEP	95



Configuring a Wireless Client with the Network Name (SSID)	95
--	----

Troubleshooting

Solutions.....	97
Front-Panel LEDs and Error Conditions.....	98

Contact Us

Specifications

Glossary

Software License

Tables

SBG901 Front-Panel LED Indicators	16
SBG901 Rear Panel Connectors and Indicators.....	17
Items Included with Your SBG901.....	23
SBG901 Light Activity during Startup	26
Configuration Manager Menu Option Bar.....	42
Field Descriptions for the Status Connection Page.....	48
Descriptions for the Status Event Log Page.....	52
Field Descriptions for the Basic Setup Page.....	54
Field Descriptions for the Basic DHCP Page	56
Field Descriptions for Basic DDNS Page	57
Field Descriptions for the Basic Backup Page	57
Field Descriptions for the Advanced Options Page	60
Field Descriptions for the Advanced IP Filtering Page.....	61
Field Descriptions for the Advanced MAC Filtering Page.....	62
Field Descriptions for the Advanced Port Filtering Page	63
Field Descriptions for the Advanced Port Triggers Page	65
Field Descriptions for the Firewall Local Log Page.....	71
Field Description for the Firewall Remote Log Page	72
Field Descriptions for the Parental Control User Setup Page.....	74
Enabling Wireless Security on Your LAN	79
Encrypting Wireless LAN Transmissions	80
Field Descriptions for the Wireless 802.11b/g Basic Page.....	81
Field Descriptions for the Wireless 802.11b/g Privacy Page	84
Field Descriptions for the Wireless 802.11b/g Access Control Page	86
Field Descriptions for the Wireless 802.11b/g Access Control Page	87



Field Descriptions for the Wireless Bridging Page	89
Field Descriptions for the Wireless 802.11b/g Wi-Fi Multimedia Page	90
Field Descriptions for the Wireless 802.11b/g Guest Network Page	93
Configuring Wireless Clients.....	94
Troubleshooting Solutions.....	97
Front-Panel Lights and Error Conditions	98
Specifications	101
Glossary.....	105

Figures

Sample Hybrid LAN.....	15
SBG901 Front Panel LEDs	16
SBG901 Rear Panel.....	17
MAC Label.....	18
Sample Wireless Network Connections	19
Sample Ethernet to Computer Connection	20
Connecting the SBG901.....	26
Local Area Connection Status window	28
Local Area Connection Properties window.....	28
Select Network Component Type window.....	29
Local Area Connection Properties window.....	29
Network and Internet Connections window.....	30
Windows XP Classic View Control Panel.....	30
Network Connections window	31
Local Area Connection Properties window.....	31
Network and Sharing Center window.....	32
LAN or High-Speed Internet connections window	32
Local Area Connection Properties window.....	33
Internet Protocol Version 4 (TCP/IPv4) Properties window	33
IPCONFIG window 1 for Windows 2000 and XP.....	34
IPCONFIG window 2 for Windows 2000 and XP.....	34
IPCONFIG window for Windows Vista	35
Renew IPCONFIG window1	36
Printer Settings for Wall Mounting Template	37
Wall Mounting Screw Dimensions	37



Wall Mounting Template.....	39
Status Software Page	47
Status Connection Page.....	48
Change User Information window	49
Ping Utility window	50
Traceroute Utility window	51
Status Event Log Page.....	52
Basic Setup Page	53
Basic DHCP Page.....	55
Basic DDNS Page.....	56
Basic Backup Page.....	57
Advance Options Page.....	59
Advanced IP Filtering Page	61
Advanced MAC Filtering Page	62
Advanced Port Filtering Page.....	63
Advanced Port Forwarding Page.....	64
Advanced Port Triggers Page.....	65
Advanced DMZ Host Page.....	66
Advanced RIP Setup Page	67
Firewall Web Content Filter Page	70
Firewall Local Log Page	71
Firewall Remote Log Page.....	72
Parental Control User Setup Page	74
Parental Control Basic Setup Page	75
Parental Control ToD Access Policy Page.....	76
Parental Control Event Log Page	77
Wireless 802.11b/g Basic Page	81
Wireless 802.11b/g Privacy Page.....	83
Wireless 802.11b/g Access Control Page.....	86
Wireless 802.11b/g Advanced Page	87
Wireless Bridging Page	89
Wireless 802.11b/g Wi-Fi Multimedia Page.....	90
Wireless 802.11b/g Guest Network Page.....	92



1

Introduction

Congratulations, you have a Motorola SBG901 SURFboard® Wireless Cable Modem Gateway for your home, home office, or small business/enterprise. Applications where the Motorola SBG901 is especially useful include:

- Households with multiple computers requiring a network connection and Internet access
- Households with one or more computers capable of wireless connectivity for remote access to the cable modem
- Small businesses or home offices that require fast, affordable, and secure Internet access to provide an internet connection for wireless gaming systems
- Video conferencing

A home network enables you to share information between two or more computers. You can connect your home network to the Internet through your cable TV system. The SBG901 is the *central connection point* between your computers and the Internet. It directs (routes) information between the computers connected to your home network. A built-in cable modem transmits information between your home network and the Internet.

SBG901 Features

The SBG901 offers the following standard features:

- Combines four separate products — a DOCSIS® 2.0 cable modem, [IEEE 802.11g](#) wireless access point (Wi-Fi® certified), Ethernet 10/100Base-T connection, and firewall — into one compact unit
- Enables you to create a custom network sharing a single broadband connection, files, and peripherals, with or without wires
- Advanced firewall for enhanced network security for wired and wireless users
- Provides an easy installation and security setup wizard

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



Easy Setup

It is much easier to configure a local area network (LAN) using an SBG901 than using traditional networking equipment:

- The Installation Assistant application on the SBG901 Installation CD-ROM enables easy connection to the cable network and setup for security.
- For basic wired or wireless operation, most default settings require no modification.
- The SBG901 Configuration Manager (CMGR) provides a graphical user interface (GUI) for easy configuration of necessary wireless, Ethernet, router, DHCP, and security settings. For information about using the SBG901 Configuration Manager, see [Basic Configuration](#).

Network Connection Types

The SBG901 provides different network connection types for your computers to exchange data. The connection between your computers and the SBG901 may be with a wireless or a wired connection or a combination of the two. Your network can use one or any combination of the following network connections:

- Ethernet local area network (LAN)
- Wireless LAN ([IEEE 802.11g](#) that also supports [IEEE 802.11b](#) wireless clients)
- Wi-Fi (Wireless Fidelity) connections to Wi-Fi enabled devices

Powerful Features in a Single Unit

An SBG901 combines high-speed Internet access, networking, and computer security for a home or small-office LAN. An SBG901 provides:

- 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 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
- Routing for a wireless LAN (WLAN) or a wired Ethernet LAN; you can connect a single computer using a hub and/or switch
- A built-in DHCP server to easily configure a combined wired and/or wireless Class C private LAN



- An advanced [firewall](#) supporting [stateful-inspection](#), intrusion detection, [DMZ](#), denial-of-service attack prevention, and Network Address Translation (NAT)
- [Port Forwarding](#) to configure ports to run applications having special network requirements

Sample Hybrid LAN

The sample LAN illustrated below contains the following devices, all protected by the SBG901 firewall. Clockwise from top-right, the devices are:

- PDA, an Apple Macintosh® computer, a desktop PC, and a laptop PC with a 802.11g wireless LAN connection



Figure 1 Sample Hybrid LAN

Optional Accessories

All networks are composed of multiple devices. The SBG901 works with any Wi-Fi certified IEEE 802.11g or IEEE 802.11b compliant client product.

The Wi-Fi capability of the SBG901 can also be used to allow other Wi-Fi enabled devices to connect to the Internet.

The maximum range of Wi-Fi devices is 300 feet and the maximum data transfer speed is 54 Mbps

Note: Wi-Fi (Wireless Fidelity) is used to identify wireless products that have been certified to conform to the IEEE 802.11b/g wireless networking specification.



Front Panel

The front panel contains indicator lights and a button for client card pairing. The display remains dark until there is a connection or activity on an interface.



Figure 2 SBG901 Front Panel LEDs

The lights provide status and information about power, communications, and errors:

Table 1 SBG901 Front-Panel LED Indicators

Key	Light	Flashing	On
1	POWER	This light does not flash	Power is provided to the SBG901
2	RECEIVE	Scanning for a receive (downstream) channel connection	Downstream channel is connected
3	SEND	Scanning for a send (upstream) channel connection	Upstream channel is connected
4	ONLINE	Scanning for configuration parameters.	Startup process is complete and the SBG901 is online
5	WIRELESS	Green: Wi-Fi enabled with encrypted wireless data activity. A 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.



Rear Panel

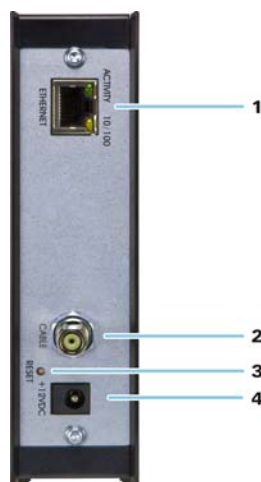



Figure 3 SBG901 Rear Panel

The rear panel contains cabling connectors and the power receptacle.

Table 2 SBG901 Rear Panel Connectors and Indicators

Key	Item	Description
1	ETHERNET	Connects to an Ethernet-equipped computer, hub, or switch using an RJ-45 cable connection
2	 CABLE	Connects the SBG901 to a cable wall outlet coaxial cable connection
3	RESET	Resets the digital voice modem. Resetting the modem may take from five to 30 minutes.
4	+12VDC	Provides power to the cable modem



Bottom Label on the SBG901

The label on the bottom of the SBG901 contains the Media Access Control (MAC) address, a unique, 48-bit value permanently saved in ROM at the factory to identify 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.



Figure 4 MAC Label

SBG901 LAN Choices

You can connect up to 245 [client](#) computers to the SBG901 using a combination of:

- Wireless LAN (WLAN) vs. LAN for wired

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, floppy disk 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 on a WLAN requires a wireless adapter.

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

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



Figure 5 Sample Wireless Network Connections

To set up the SBG901 on a computer wired to the SBG901 with an Ethernet connection, perform the procedures found on the [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.

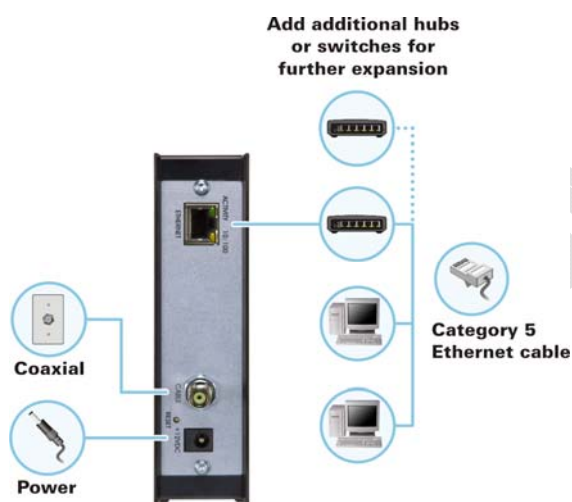


Figure 6 Sample Ethernet to Computer Connection

The physical wiring arrangement has no connection to the logical network allocation of IP addresses.

A wired Ethernet LAN with more than one computer requires one or more [hubs](#), [switches](#), or [routers](#). You can do the following:

- Connect a hub or switch to the Ethernet port on the SBG901
- Use Ethernet hubs, switches, or routers to connect up to 245 computers to the SBG901

A complete discussion of Ethernet cabling is beyond the scope of this document.

Security

The SBG901 provides the following:

- A [firewall](#) to protect the SBG901 LAN from undesired attacks over the Internet
- For wireless transmissions, data encryption and network access control

Network Address Translation ([NAT](#)) provides some security because the IP addresses of SBG901 LAN computers are not visible on the Internet.



Firewall

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](#).

DMZ

A de-militarized zone ([DMZ](#)) is one or more computers logically located outside the firewall between an SBG901 LAN and the Internet. A DMZ 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](#).

Port Triggering

When you run an application that accesses the Internet, it typically initiates communications with a computer on the Internet. For some applications, especially gaming, the computer on the Internet also initiates communications with your computer. Because NAT does not normally allow these incoming connections:

- If needed, you can configure additional port triggers on the Advanced Port Triggers Page.



Wireless Security

Because WLAN data is transmitted using radio signals, it may be possible for an unauthorized person to access your WLAN unless you prevent them from doing so. To prevent unauthorized eavesdropping of data transmitted over your LAN, you must enable wireless security. The default SBG901 settings neither provide security for transmitted data nor protect network data from unauthorized intrusions.

The SBG901 provides the following wireless security measures, which are described on the [Wireless Pages](#).

To prevent unauthorized eavesdropping, you must encrypt data transmitted over the wireless interface using *one* of the following:

- If all of your wireless clients support Wi-Fi Protected Access (WPA or WPA2) encryption, Motorola recommends using WPA2. Otherwise, configure a Wired Equivalency Privacy (WEP) key on the SBG901 and each WLAN client.
- To protect the wireless LAN from unauthorized intrusions (see [Setting Up Your Wireless LAN](#)), you can do one or both of the following:
 - Restrict WLAN access to computers having known MAC addresses
 - Enable closed network operation by disabling SSID broadcasting

Port Forwarding

The SBG901 opens logical data ports when a computer on its LAN sends data, such as e-mail messages or web data, to the Internet. A logical data port is different from a physical port, such as an Ethernet port. Data from a protocol must go through certain data ports.

Some applications, such as games and video conferencing, require multiple data ports. If you enable NAT, this can cause problems because NAT assumes that data sent through one port will return to the same port. You may need to configure port forwarding to run applications with special requirements.

To configure port forwarding, you must specify an inbound (source) port or range of ports. The inbound port opens only when data is sent to the inbound port and closes again after a specified time elapses with no data sent to it. You can configure up to 32 port forwarding entries using the Advanced Port Forwarding Page.



2

Getting Started

The following topics provide information about installing the SBG901 hardware:



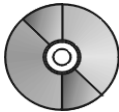

- [Before You Begin](#)
- [Precautions](#)
- [Signing Up for Service](#)
- [Computer System Requirements](#)
- [Connecting the SBG901 to the Cable System](#)
- [Cabling the LAN](#)
- [Configuring TCP/IP](#)
- [Wall Mounting Your SBG901](#)

For information about 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 Gateway:

Table 3 Items Included with Your SBG901

Item		Description
Power cord		Connects the SBG901 to a power adapter that connects to an AC electrical outlet
Ethernet cable		Connects to the Ethernet port
SBG901 Installation CD-ROM		Contains SBG901 Installation Assistant, and this user guide
SBG901 Install Sheet		Contains basic information for getting started with the SBG901



You must have the latest service packs and patches installed on your computer for your operating system. You will need 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 the 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 need to provide the MAC address marked **HFC MAC ID** printed on the [Bottom Label on the SBG901](#). You can record it in the *SBG901 Install Sheet*.

You should ask your Internet Service provider the following questions:

- Do you 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?



Computer System Requirements

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

- **Ethernet** — 10Base-T or 10/100Base-T Ethernet adapter with proper driver software installed.

For user with Microsoft Vista™, please note the following information on driver support:

- Vista OS support
- Vista Home Basic (32 bit and 64 bit)
- Vista Home Premium (32 bit and 64 bit)
- Vista Business (32 bit and 64 bit)
- Vista Ultimate (32 bit and 64 bit)

Please note the following Euro market versions without Windows Media Player:

- Vista Home Basic (32 bit and 64 bit)
 - Vista Home Premium (32 bit and 64 bit)
 - Vista Business (32 bit and 64 bit)
 - Vista Ultimate (32 bit and 64 bit)
- **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:

- PC with Pentium® class or better processor
- Windows 2000, Windows XP, Windows Vista, Macintosh, Linux, or UNIX operating system with operating system CD-ROM available
 - Minimum 256 MB RAM recommended
 - 10 MB available hard disk space

You can use any web browser with the SBG901.

Connecting the SBG901 to the Cable System

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 the SBG901 on. You do not need to unplug it when not in use. The first time you plug in the SBG901, allow it 5 to 30 minutes to find and lock on the appropriate communications channels.



Figure 7 Connecting the SBG901

Check that the lights on the front panel cycle through this sequence:

Table 4 SBG901 Light Activity During Startup

Light	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

You can use either of the following two options to obtain the IP address for the network interface on your computer:

- 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 2000](#)
- [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, you must verify the IP address. Perform one of the following:

- [Verifying the IP Address in Windows 2000 or 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 2000

1. Select **Control Panel** from either the Windows Start menu or Windows Desktop to display the Control Panel window.
2. Double-click **Network and Dial-up Connections** to display the Network and Dial-up Connections window.

In the steps that follow, a connection number such as 1, 2, or 3 represents PCs with multiple network interfaces. PCs having only one network interface may be represented as "Local Area Connection."

3. Double-click **Local Area Connection *number*** to display the Local Area Connection *number* Status window. The value of *number* varies from system to system.

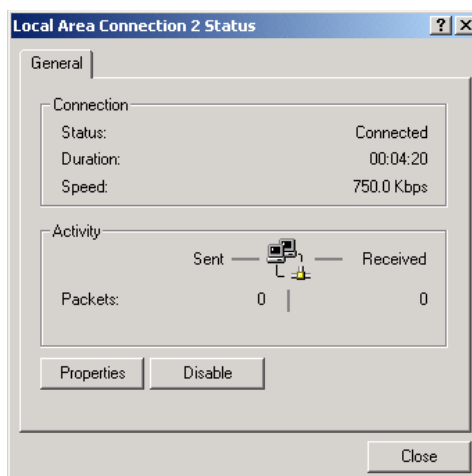


Figure 8 Local Area Connection Status window

4. Click **Properties** to display the Local Area Connection *number* Properties window. Information similar to the following is displayed.

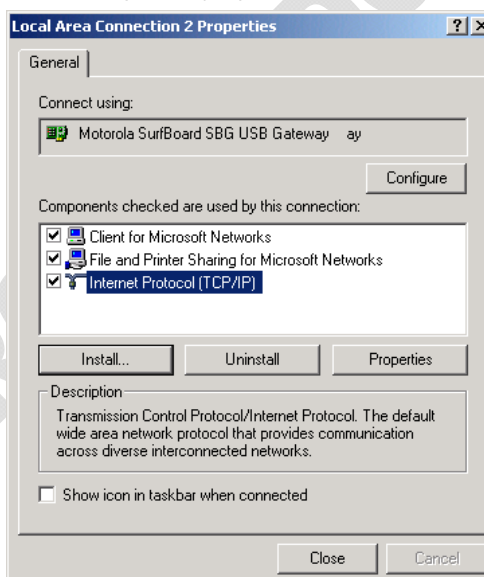


Figure 9 Local Area Connection Properties window

5. If Internet Protocol (TCP/IP) is in the list of components, TCP/IP is installed. You can skip to step 8.
6. If Internet Protocol (TCP/IP) is not in the list of components, click **Install**. The Select Network Component Type window is displayed.

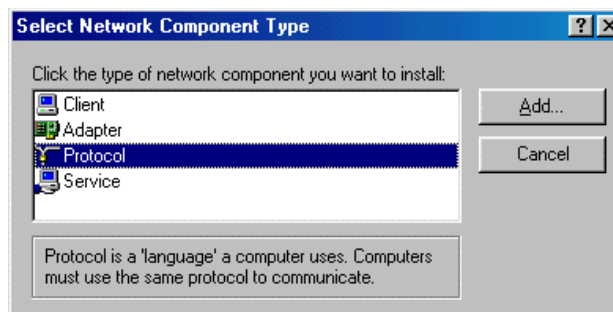


Figure 10 Select Network Component Type window

7. Click **Protocol** and then click **Add**. The Select Network Protocol window is displayed.
8. Click **Internet Protocol (TCP/IP)**, and then click **OK**. The Local Area Connection *number* Properties window is redisplayed.

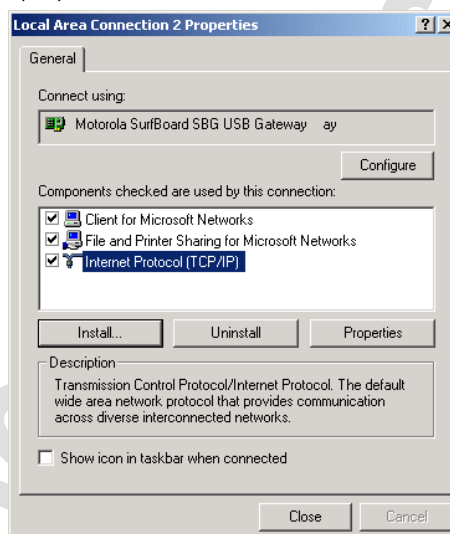


Figure 11 Local Area Connection Properties window

9. Click **Internet Protocol (TCP/IP)**, and then click **Properties** to display the Internet Protocol (TCP/IP) Properties window.
10. Be sure **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.
11. Click **OK** to save the TCP/IP settings and exit the TCP/IP Properties window.
12. Click **OK** to exit the Local Area Connection Properties window.
13. Click **OK** when prompted to restart the computer and click **OK** again.
14. When you complete the TCP/IP configuration, go to [Verifying the IP Address in Windows 2000 or Windows XP](#).



Configuring TCP/IP in Windows XP

1. On the Windows desktop, click **Start** to display the Start window.
2. Click **Control Panel** to display the Control Panel window. The display varies, depending on the Windows XP view options. If the display is a Category view, as shown below, continue with step 3. Otherwise, skip to step 5.
3. Click **Network and Internet Connections** to display the Network and Internet Connections window.

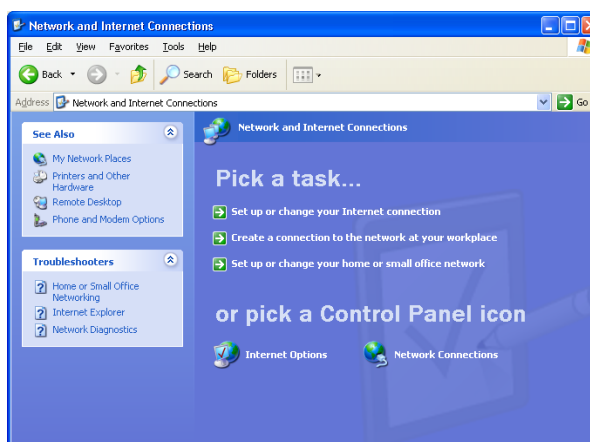


Figure 12 Network and Internet Connections window

4. Click **Network Connections** to display the LAN or High-Speed connections. You can skip to step 7.
5. If a Classic view similar to the screenshot below is displayed, double-click **Network Connections** to display LAN or High-Speed Internet connections.

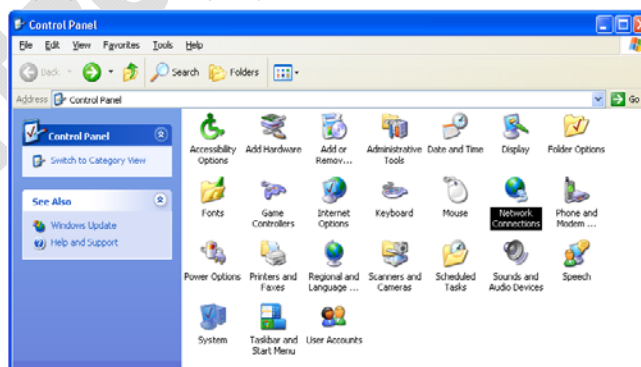


Figure 13 Windows XP Classic View Control Panel

6. Right-click the network connection. If more than one connection is displayed, be sure to select the one for your network interface.

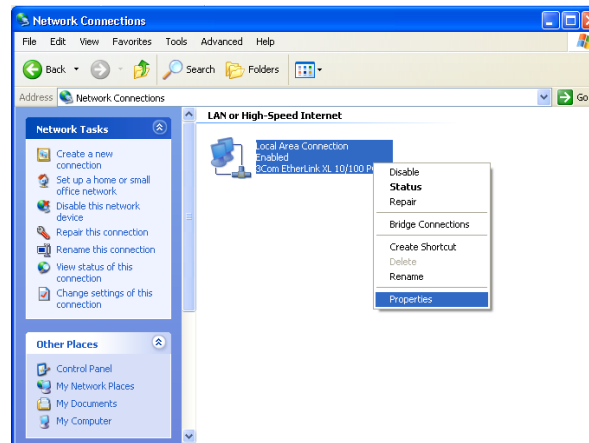


Figure 14 Network Connections window

7. Select **Properties** from the drop-down menu to display the Local Area Connection Properties window. Be sure Internet Protocol (TCP/IP) is checked.

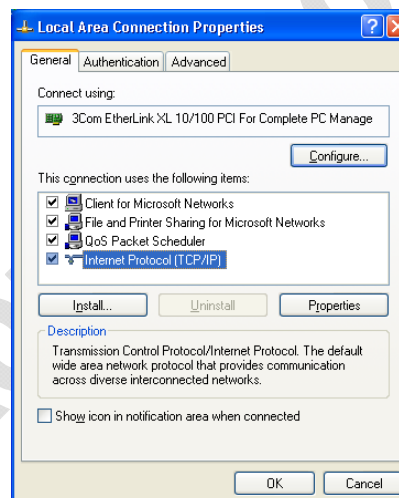


Figure 15 Local Area Connection Properties window

8. Select **Internet Protocol (TCP/IP)** and click **Properties** to display the Internet Protocol (TCP/IP) Properties window.
9. Make sure **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.
10. Click **OK** to save the TCP/IP settings and exit the TCP/IP Properties window.
11. Click **OK** to exit the Local Area Connection Properties window.
12. When you complete the TCP/IP configuration, go to [Verifying the IP Address in Windows 2000 or Windows XP](#).



Configuring TCP/IP in Windows Vista

1. On the Windows desktop, click **Start** to display the Start window.
2. Click **Control Panel** to display the Control Panel window.
3. Double-click **Network and Internet** and the Network and Internet window is displayed:
4. Double-click **Network and Sharing Center** and the Network and Sharing Center window is displayed:

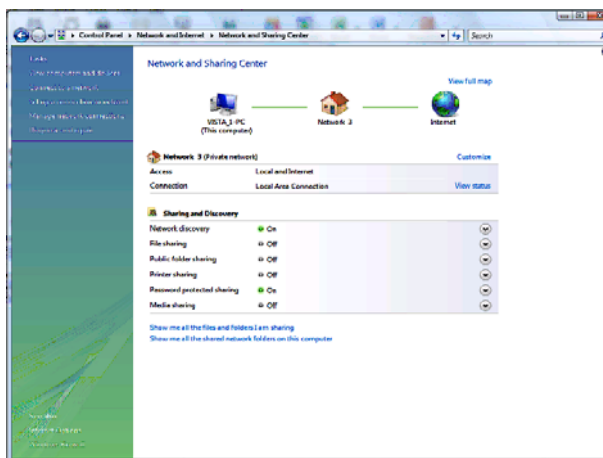


Figure 16 Network and Sharing Center window

5. Click **Manage network connections** and the LAN or High-Speed Internet connections window is displayed:

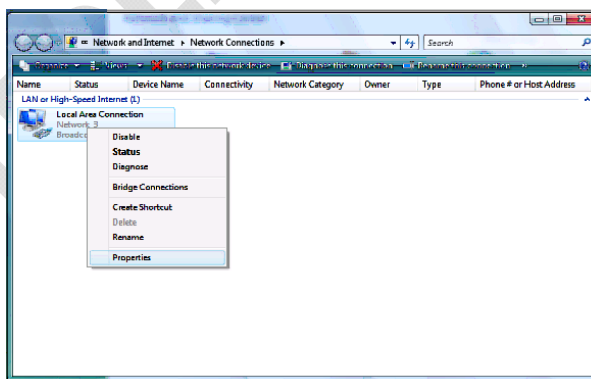


Figure 17 LAN or High-Speed Internet connections window



6. Right-click the network connection and select **Properties** to display the Local Area Connection Properties window:

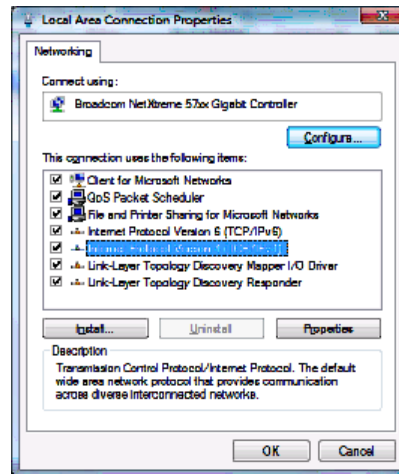


Figure 18 Local Area Connection Properties window

7. If more than one connection is displayed, make sure to select the one for your network interface.

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 Version 4 (TCP/IPv4)** and click **Properties** to display the Internet Protocol Version 4 (TCP/IPv4) Properties window.

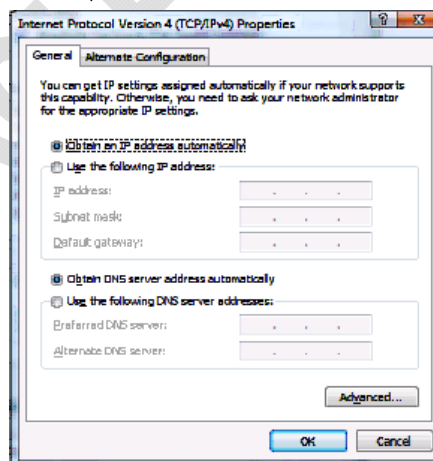


Figure 19 Internet Protocol Version 4 (TCP/IPv4) Properties window

9. Make sure **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.
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. Exit the Network Connections window.
13. Exit the Network and Sharing Center window and the Control Panel.

When you complete the TCP/IP configuration, go to [Verifying the IP Address in Windows Vista](#).

Verifying the IP Address in Windows 2000 or 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. A display, like below, indicates a normal configuration:

```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : surfboard.com
    IP Address . . . . . : 206.19.86.174
    Subnet Mask . . . . . : 255.255.255.224
    Default Gateway . . . . . : 206.19.86.161

Ethernet adapter Local Area Connection:

    Media State . . . . . : Cable Disconnected

C:\>
```

Figure 20 IPCONFIG window 1 for Windows 2000 and XP

If an Autoconfiguration IP Address is displayed as in the window below, there is an incorrect connection between your PC and the digital voice modem or there are cable network problems.

```
cmd
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    Autoconfiguration IP Address. . . : 169.254.45.20
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . :

C:\>
```

Figure 21 IPCONFIG window 2 for Windows 2000 and XP

Check the following:

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

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



Verifying the IP Address in Windows Vista

Do the following to verify the IP address:

1. On the Windows Vista 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.

A display similar to the following indicates a normal configuration.

```
C:\Windows\system32\cmd.exe
C:\Users\Vista_1>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::5db3:468b:1f5b:7c98%9
    IPv4 Address. . . . . : 192.168.1.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Tunnel adapter Local Area Connection* 6:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : 2001:0:4136:e37a:108a:b5a:3f57:fe8b
    Link-local IPv6 Address . . . . . : fe80::108a:b5a:3f57:fe8b%8
    Default Gateway . . . . . : ::

Tunnel adapter Local Area Connection* 7:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::5efe:192.168.1.4%10
    Default Gateway . . . . . : 

C:\Users\Vista_1>
```

Figure 22 IPCONFIG window for Windows Vista

If an Autoconfiguration IP Address is displayed, there is an incorrect connection between the PC and the SBG901, or there are broadband network problems.

Renewing Your IP Address

To renew your IP address in Windows 2000, Windows XP, or Windows Vista:

1. On the Windows Desktop, click **Start**.
2. Select **Run**. The Run window is displayed.
3. Type **cmd** and click **OK**.
4. Type **ipconfig /renew** and press **ENTER**. If a valid IP address is displayed as shown, Internet access should be available.



```
cmd
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig /renew

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : surfboard.com
    IP Address. . . . . : 206.19.86.174
    Subnet Mask . . . . . : 255.255.255.224
    Default Gateway . . . . . : 206.19.86.161

C:\>_
```

Figure 23 Renew IPCONFIG window1

5. Type **exit** and press **ENTER** to return to Windows.

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

Wall Mounting the SBG901

If you mount your SBG901 on the wall, you must:

- 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 electric 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. See [Wall Mounting Template](#) to print a copy of the template.
2. Click the Print icon or choose Print from the File menu to display the Print dialog box.

The sample Print dialogue window shown below may vary slightly on your computer, depending upon your operating system.

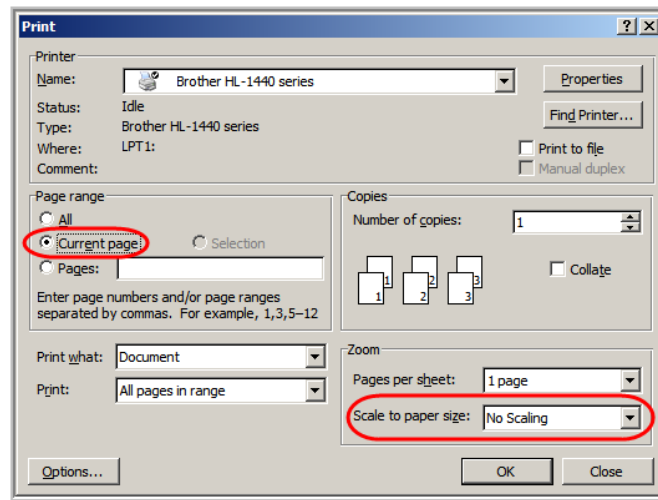


Figure 24 Printer Settings for Wall Mounting Template

To print the template only, select **Current page** as the Print Range. Be sure you print the template at 100% scale. Be sure **No Scaling** is selected for Scale to paper size.

3. Click **OK** to print the template.
4. Measure the printed template with a ruler to ensure that it is the correct size.
5. Use a center punch to mark the center of the holes.
6. On the wall, locate the marks for the mounting holes.
7. 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.
8. Using a screwdriver, turn each screw until part of it protrudes from the wall, as shown in the following illustration.

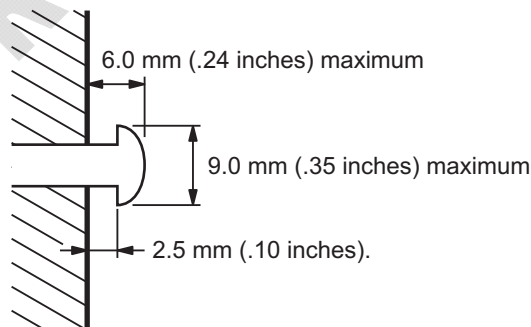


Figure 25 Wall Mounting Screw Dimensions

There must be .10 inches (2.5 mm) between the wall and the underside of the screw head.

9. Place the SBG901 so the keyholes on the back of the unit are aligned above the mounting screws.



10. 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.

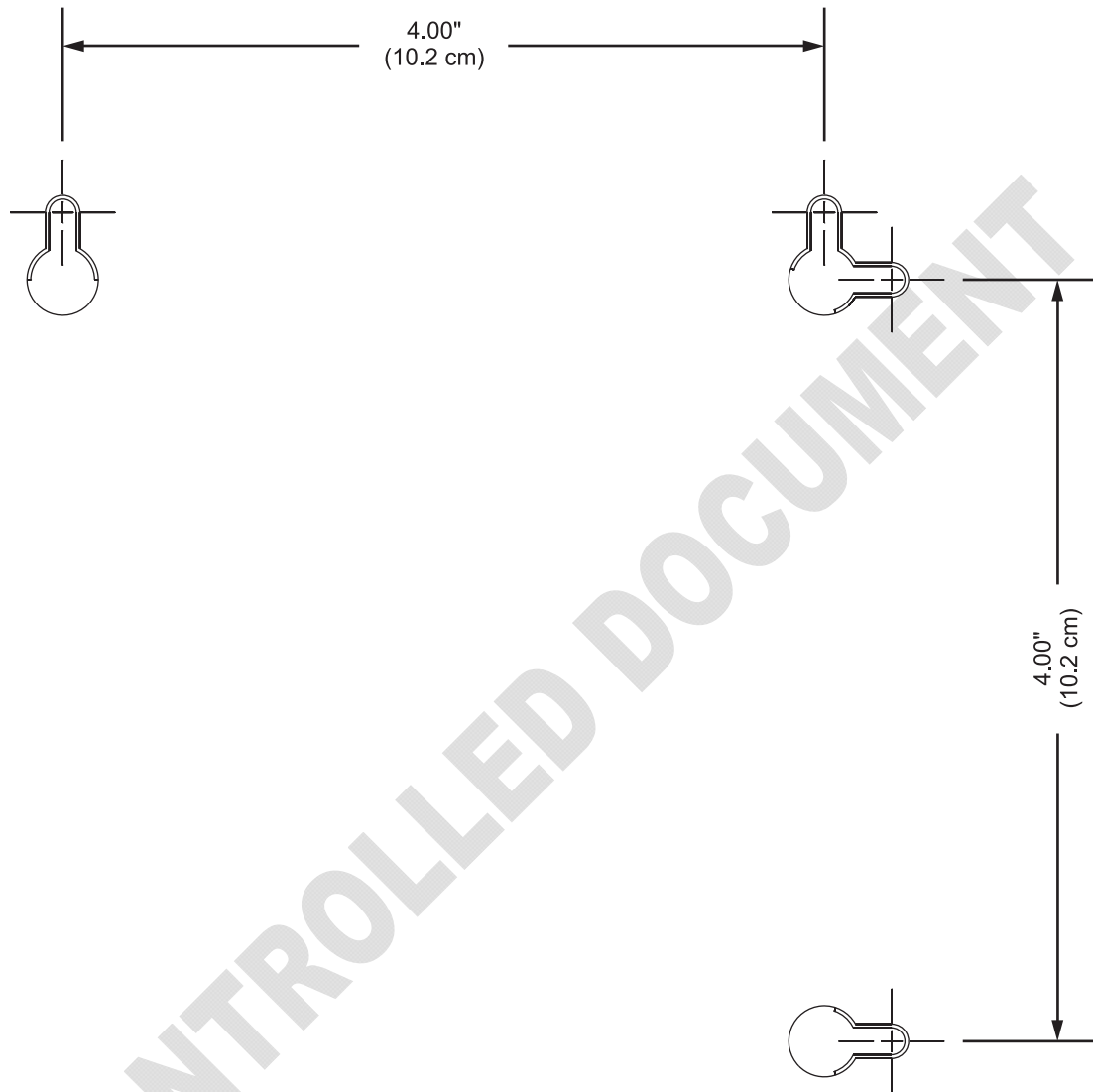


Figure 26 Wall Mounting Template



3

Basic Configuration

The following topics provide information about basic SBG901 configuration:

- [Starting the SBG901 Configuration Manager \(CMGR\)](#)
- [SBG901 Menu Options Bar](#)
- [Changing the SBG901 Default Password](#)
- [Getting Help](#)
- [Gaming Configuration Guidelines](#)
- [Exiting the SBG901 Configuration Manager](#)

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](#).

If you are using a wired LAN only and have no wireless clients, be sure you disable the wireless interface. See [Wireless 802.11b/g Basic Page](#) to disable.

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).

Username: [masked]
Password: [masked]
Login

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 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.

Table 5 Configuration Manager Menu Option 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 PC.
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.

Change User Information	
Password Change Username	<input type="text"/>
New Password	<input type="text"/>
Re-Enter New Password	<input type="text"/>
Current Username Password	<input type="text"/>

Restore Factory Defaults	
<input type="radio"/> Yes	<input checked="" type="radio"/> No
<input type="button" value="Apply"/>	

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

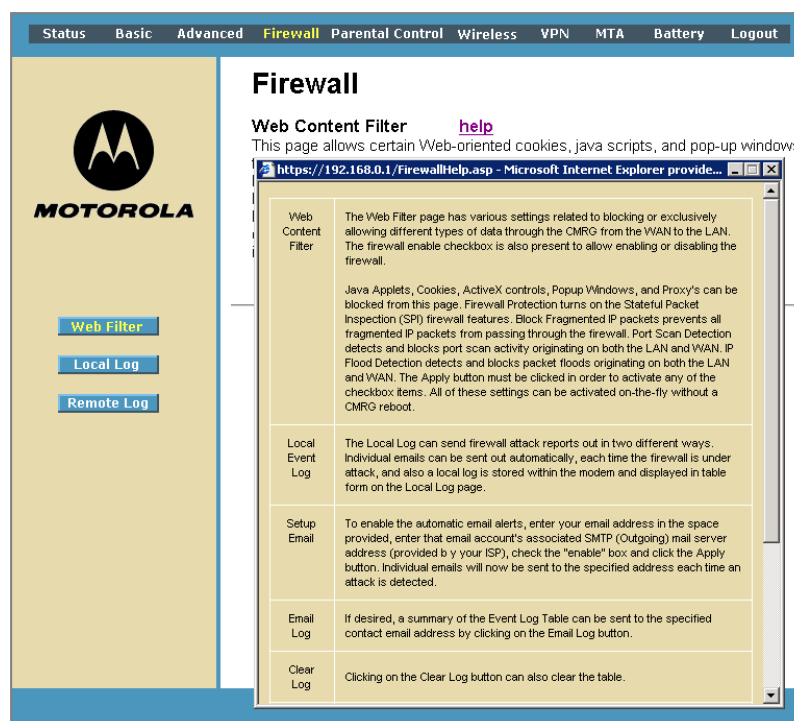
To reset the user name and password back to the original factory settings:

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. As an example, the Firewall help page is 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. If, as recommended, 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 one of:

- 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



UNCONTROLLED DOCUMENT



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	169258714233448801012001
CM certificate	Installed
Status	
System Up Time	3 days 14h:01m:17s
Network Access	Allowed
Cable Modem IP Address	---.---.---.---

Figure 27 Status Software Page



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: --	-----	

Figure 28 Status Connection Page

Table 6 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.

Change User Information	
Password Change Username	<input type="text"/>
New Password	<input type="text"/>
Re-Enter New Password	<input type="text"/>
Current Username Password	<input type="text"/>
Restore Factory Defaults	
<input type="radio"/> Yes	<input type="radio"/> No
<input type="button" value="Apply"/>	

Figure 29 Change User Information window

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 your 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.

Select Utility	
Ping	
Ping Test Parameters	
Target	0 . 0 . 0 . 0
Ping Size	64 bytes
No. of Pings	3
Ping Interval	1000 ms
Start Test Abort Test Clear Results	
Results	
Waiting for input...	

Figure 30 Ping Utility window

Testing Network Connectivity with the SBG901

Perform the following steps to check connectivity between the SBG901 and other devices on the SBG901 LAN:

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.

The screenshot shows a web-based utility window titled "Select Utility". A dropdown menu is set to "Traceroute". Below this is a section titled "Traceroute Parameters" containing several input fields: "Target" (with a placeholder "IP address or Name"), "Max Hops" (set to 255), "Data Size" (set to 32 bytes), "Base Port" (set to 33434), and "Resolve Host" (set to Off). There are two buttons: "Start Test" and "Clear Results". At the bottom, a "Results" section displays the text "Waiting for input...".

Figure 31 Traceroute Utility window

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
Wed Aug 08 20:58:34 2007	Warning (5)	DHCP RENEW WARNING - Field invalid in response
Wed Aug 08 20:23:02 2007	Critical (3)	Started Unicast Maintenance Ranging - No Response received - ...
Wed Aug 08 19:58:34 2007	Warning (5)	DHCP RENEW WARNING - Field invalid in response
Wed Aug 08 19:44:51 2007	Critical (3)	Started Unicast Maintenance Ranging - No Response received - ...
Wed Aug 08 19:17:19 2007	Warning (5)	DHCP RENEW WARNING - Field invalid in response
Wed Aug 08 18:10:38 2007	Critical (3)	Started Unicast Maintenance Ranging - No Response received - ...
Wed Aug 08 17:47:19 2007	Warning (5)	DHCP RENEW WARNING - Field invalid in response
Wed Aug 08 16:53:16 2007	Critical (3)	Started Unicast Maintenance Ranging - No Response received - ...
Wed Aug 08 16:47:19 2007	Warning (5)	DHCP RENEW WARNING - Field invalid in response
Tue Aug 07 10:31:40 2007	Critical (3)	Started Unicast Maintenance Ranging - No Response received - ...
Tue Aug 07 10:24:49 2007	Warning (5)	DHCP RENEW WARNING - Field invalid in response
Tue Aug 07 10:12:01 2007	Critical (3)	Started Unicast Maintenance Ranging - No Response received - ...
Tue Aug 07 09:54:49 2007	Warning (5)	DHCP RENEW WARNING - Field invalid in response
Mon Aug 06 15:04:39 2007	Critical (3)	Started Unicast Maintenance Ranging - No Response received - ...
Mon Aug 06 14:54:48 2007	Warning (5)	DHCP RENEW WARNING - Field invalid in response
Mon Aug 06 14:51:38 2007	Critical (3)	Started Unicast Maintenance Ranging - No Response received - ...
Mon Aug 06 14:24:48 2007	Warning (5)	DHCP RENEW WARNING - Field invalid in response
Mon Aug 06 13:32:23 2007	Critical (3)	Started Unicast Maintenance Ranging - No Response received - ...
Mon Aug 06 13:24:48 2007	Warning (5)	DHCP RENEW WARNING - Field invalid in response
Fri Aug 03 08:38:19 2007	Notice (6)	Ethernet link up - ready to pass packets
Fri Aug 03 08:38:17 2007	Notice (6)	Ethernet link dormant - not currently active
Fri Aug 03 08:37:50 2007	Notice (6)	Ethernet link up - ready to pass packets
Fri Aug 03 08:37:48 2007	Notice (6)	Ethernet link dormant - not currently active
Time Not Established	Critical (3)	DHCP WARNING - Non-critical field invalid in response.
Time Not Established	Notice (6)	Ethernet link up - ready to pass packets

Figure 32 Status Event Log Page

Table 7 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 PC.

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.

Primary Mode	
NAPT mode	Enabled <input type="button" value="Apply"/>
Network Configuration	
LAN IP Address:	192 . 168 . 0 . 1
MAC Address	00:1a:66:07:ab:01
WAN IP Address:	---:---:---:---
MAC Address:	00:1a:66:07:ab:02
Duration	D: -- H: -- M: -- S: --
Expires	---:---:---:---
<input type="button" value="Release WAN Lease"/> <input type="button" value="Renew WAN Lease"/>	
WAN Connection Type	
WAN Connection Type	DHCP <input type="button" value="Apply"/>
Host Name	<input type="text"/> (Required by some ISPs)
Domain Name	<input type="text"/> (Required by some ISPs)
MTU Size	0 (256-1500 octets, 0 = use default)
Spoofed MAC Address	00 : 00 : 00 : 00 : 00 : 00 <input type="button" value="Apply"/>

Figure 33 Basic Setup Page



Table 8 Field Descriptions for the Basic Setup Page

Field	Description
NAPT mode	<p>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.</p> <p>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.</p>
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	<p>DHCP or Static IP</p> <p>If your ISP uses DHCP, select DHCP and enter a Host Name and Domain name, if required.</p> <p>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.</p>



Field	Description
Host Name	If the WAN Connection Type is DHCP, enter a Host Name if required by your ISP.
Domain Name	If the WAN Connection Type is DHCP, enter a Domain Name if required by your ISP.
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 the 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.

DHCP					
DHCP Server	<input checked="" type="radio"/> Yes <input type="radio"/> No				
Starting Local Address	192.168.0.10				
Number of CPEs	245				
Lease Time	3600				
<input type="button" value="Apply"/>					
DHCP Clients					
MAC Address	IP Address	Subnet Mask	Duration	Expires	Select
0018f8286e4f	192.168.000.011	255.255.255.000	D:00 H:01 M:00 S:00	Fri Aug 03 08:57:13 2007	<input type="radio"/>
Current System Time: Fri Aug 03 08:56:31 2007					
<input type="button" value="Force Available"/>					

Figure 34 Basic DHCP Page

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



Table 9 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.

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.

DDNS	
DDNS Service:	Disabled
User Name:	
Password:	
Host Name:	
IP Address:	0.0.0.0
Status:	DDNS service is not enabled.
<input type="button" value="Apply"/>	

Figure 35 Basic DDNS Page



Table 10 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.

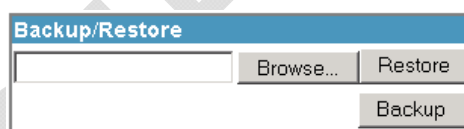


Figure 36 Basic Backup Page

Table 11 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.

UNCONTROLLED DOCUMENT



6

Advanced Pages

The SBG901 Advanced Pages allow you to configure the advanced features of the SBG901, including IP Filtering, MAC Filtering, Port Filtering, Port Forwarding, Port Triggers, DMZ Host, and Routing Information Protocol 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.

WAN Blocking	<input checked="" type="checkbox"/> Enable
Ipssec PassThrough	<input type="checkbox"/> Enable
PPTP PassThrough	<input type="checkbox"/> Enable
Remote Config Management	<input type="checkbox"/> Enable
Multicast Enable	<input checked="" type="checkbox"/> Enable
UPnP Enable	<input type="checkbox"/> Enable
<input type="button" value="Apply"/>	

Figure 37 Advance Options Page



Table 12 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 or uncheck to disable it.
IPsec Pass-Through	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 or uncheck to disable it.
PPTP Pass-Through	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 or uncheck to disable it.
Remote Configuration 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 or uncheck to disable it.
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 or uncheck to disable it.
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 or uncheck to disable it.

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.

IP Filtering		
Start Address	End Address	Enabled
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
<input type="button" value="Apply"/>		

Figure 38 Advanced IP Filtering Page

Table 13 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 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.

MAC Address Filters	
MAC 01	00 : 00 : 00 : 00 : 00 : 00
MAC 02	00 : 00 : 00 : 00 : 00 : 00
MAC 03	00 : 00 : 00 : 00 : 00 : 00
MAC 04	00 : 00 : 00 : 00 : 00 : 00
MAC 05	00 : 00 : 00 : 00 : 00 : 00
MAC 06	00 : 00 : 00 : 00 : 00 : 00
MAC 07	00 : 00 : 00 : 00 : 00 : 00
MAC 08	00 : 00 : 00 : 00 : 00 : 00
MAC 09	00 : 00 : 00 : 00 : 00 : 00
MAC 10	00 : 00 : 00 : 00 : 00 : 00
MAC 11	00 : 00 : 00 : 00 : 00 : 00
MAC 12	00 : 00 : 00 : 00 : 00 : 00
MAC 13	00 : 00 : 00 : 00 : 00 : 00
MAC 14	00 : 00 : 00 : 00 : 00 : 00
MAC 15	00 : 00 : 00 : 00 : 00 : 00
MAC 16	00 : 00 : 00 : 00 : 00 : 00
MAC 17	00 : 00 : 00 : 00 : 00 : 00
MAC 18	00 : 00 : 00 : 00 : 00 : 00
MAC 19	00 : 00 : 00 : 00 : 00 : 00
MAC 20	00 : 00 : 00 : 00 : 00 : 00

Apply

Figure 39 Advanced MAC Filtering Page

Table 14 Field Descriptions for the Advanced MAC Filtering Page

Field	Description
MAC xx	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 xx field for each PC you want to block.
2. When done, click **Apply**.



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**.

Port Filtering			
Start Port	End Port	Protocol	Enabled
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>

Apply

Figure 40 Advanced Port Filtering Page

Table 15 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
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.

Port Forwarding				
Local IP Adr	Start Port	End Port	Protocol	Enabled
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>

Figure 41 Advanced Port Forwarding Page

A table of commonly used Port numbers is also displayed on the page for your convenience.

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.

The ports used by some common applications are:

- FTP: 20, 21
- HTTP: 80
- NTP: 123
- Secure Shell: 22
- SMTP e-mail: 25
- Telnet: 23



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 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.

Port Triggering					
Trigger Range		Target Range		Protocol	Enable
Start Port	End Port	Start Port	End Port		
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Both	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Both	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Both	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Both	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Both	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Both	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Both	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Both	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Both	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Both	<input type="checkbox"/>

Figure 42 Advanced Port Triggers Page

Table 16 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.



Field	Description
Target Range	
Start Port	The starting port number of the Port Trigger range.
End Port	The ending port number of the Port Trigger range.
Protocol	Choice, TCP, UDP, or Both
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 sits between the trusted internal private LAN and the untrusted public Internet.

DMZ Address 192.168.0.0

Apply

Figure 43 Advanced DMZ Host Page

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.

RIP Enable	<input type="checkbox"/> Enable
RIP Authentication	<input checked="" type="checkbox"/> Enable
RIP Authentication Key	<input type="text"/>
RIP Authentication Key ID	<input type="text" value="0"/>
RIP Reporting Interval	<input type="text" value="30"/> seconds
RIP Destination IP Address	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
RIP Destination IP Subnet Mask	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>
<input type="button" value="Apply"/>	

Figure 44 Advanced RIP Setup Page



Table 17 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 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.

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.



Web Features	
Filter Proxy	<input type="checkbox"/> Enable
Filter Cookies	<input type="checkbox"/> Enable
Filter Java Applets	<input type="checkbox"/> Enable
Filter ActiveX	<input type="checkbox"/> Enable
Filter Popup Windows	<input type="checkbox"/> Enable
Block Fragmented IP Packets	<input checked="" type="checkbox"/> Enable
Port Scan Detection	<input type="checkbox"/> Enable
IP Flood Detection	<input checked="" type="checkbox"/> Enable
Firewall Protection	<input checked="" type="checkbox"/> Enable

Figure 45 Firewall Web Content Filter Page

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

Alert System				
Contact Email Address	<input type="text"/>			
SMTP Server Name	<input type="text"/>			
E-mail Alerts	<input type="checkbox"/> Enable			
<input type="button" value="Apply"/>				
Description	Count	Last Occurrence	Target	Source
<input type="button" value="E-mail Log"/>		<input type="button" value="Clear Log"/>		

Figure 46 Firewall Local Log Page

Table 18 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.

Send selected events

Permitted Connections

Blocked Connections

Known Internet Attacks

Product Configuration Events

to SysLog server at 192.168.0.

Apply

Figure 47 Firewall Remote Log Page

Table 19 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.



Figure 48 Parental Control User Setup Page

Table 20 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.



Field	Description
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.

Parental Control Activation
This box must be checked to turn on Parental Control
 Enable Parental Control
Apply

Content Policy Configuration
Add New Policy
1. Default Remove Policy
Keyword List: anonymizer
Blocked Domain List: anonymizer.com
Allowed Domain List
Add Remove Add Remove Add Remove

Override Password
If you encounter a blocked website, you can override the block by entering the following password
Password:
Re-Enter Password:
Access Duration: 30
Apply

Figure 49 Parental Control Basic Setup Page

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 ToD 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](#).

Time Access Policy Configuration

Create a new policy by giving it a descriptive name, such as "Weekend" or "Working Hours"

Time Access Policy List

Enabled

Days to Block

Everyday Sunday Monday Tuesday
 Wednesday Thursday Friday Saturday

Time to Block

All day

Start: (hour) (min)

End: (hour) (min)

Figure 50 Parental Control ToD Access Policy 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

Last Occurrence	Action	Target	User	Source
<input type="button" value="Clear Log"/>				

Figure 51 Parental Control Event Log Page



UNCONTROLLED DOCUMENT



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.

Setting Up Your Wireless LAN

You can use the SBG901 as an access point for a wireless LAN (WLAN) without changing its default settings.

CAUTION: To prevent unauthorized eavesdropping or access to WLAN data, you must enable wireless security. The default SBG901 settings provide no wireless security. After your WLAN is operational, be sure to enable wireless security

To enable security for your WLAN, you can do the following on the SBG901:

Table 21 Enabling Wireless Security on Your LAN

To	Perform	Use in SBG901 Configuration Mgr
Encrypt wireless transmissions and restrict WLAN access	Encrypting Wireless LAN Transmissions	Wireless 802.11b/g Privacy Page
Further prevent unauthorized WLAN intrusions	Restricting Wireless LAN Access	Wireless 802.11b/g 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 [Configuring the 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.

Use the [Wireless 802.11b/g Privacy Page](#) to encrypt your transmitted data. Choose one of:

Table 22 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.



Wireless 802.11b/g Basic Page

This page allows you to configure the Access Point parameters, including the SSID and channel number.

Creating a SecureEasySetup™ (SES) network ensures strong security for preventing unauthorized wireless network access. However, traditional wireless network installation can be a complicated and time-consuming task, requiring the user to possess the technical know-how to manually enter several settings (such as network name and encryption key or WPA pass phrase) on each Wi-Fi device. Motorola SecureEasySetup technology dramatically simplifies installation by automating the configuring new wireless networks processes and adding devices to existing networks. SecureEasySetup establishes a private connection between the devices and automatically configures the network's Service Set Identifier (SSID) and WPA-Personal security settings. It configures a new network only on each new device that is authorized to join the network.

Wireless MAC Address: 00:1A:73:54:B1:9D

Network Name (SSID): Motorola

Network Type: Open

Country: USA

Channel: 11 Current: 11

Interface: Enabled

Apply Restore Wireless Defaults

SecureEasySetup
Use these buttons to manage your SecureEasySetup network.

Create SES Network Open SES Window

Figure 52 Wireless 802.11b/g Basic Page

Table 23 Field Descriptions for the Wireless 802.11b/g Basic Page

Field	Description
Wireless MAC Address	Shows the MAC address of the installed wireless card. It is not configurable.
Network Name (SSID)	Sets the Network Name (also known as SSID) of the wireless network. This is a 1-32 ASCII character string.



Field	Description
Network Type	Selecting Closed prevents the network name from appearing in a wireless client's "Available Wireless Networks" list. Only clients who already know the network name will be able to connect. Closed disables the SSID broadcast in beacon packets. Selecting Open allows broadcasting to the SSID in beacon packets.
Country	Restricts the channel set based on the country's regulatory requirements. This is a display-only field.
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.
Interface	Allows the access point to be Enabled or Disabled.
Create SES Network	This action button generates a new SecureEasySetup network, applies the configuration to the wireless interface, and stores the settings to non-volatile memory. It enables WPA-PSK authentication and generates a unique Network Name (SSID) and random, 16-character Pre-Shared Key (PSK). The pop-up window shown informs the user a SecureEasySetup network has been successfully created.
Open SES Window	This action button opens a 2-minute security window that allows a SecureEasySetup client to connect. Only 1 SecureEasySetup client may connect during an Open Window period. If you have more than 1 client to connect to your SecureEasySetup, you must open the window multiple times. When the SecureEasySetup window is open, the pop-up window below indicates the CMRG is waiting for a SecureEasySetup client.



Wireless 802.11b/g Privacy Page

This page allows you to configure the WEP keys and/or passphrase.

WPA	Disabled
WPA-PSK	Disabled
WPA2	Disabled
WPA2-PSK	Disabled
WPAWPA2 Encryption	Disabled
WPA Pre-Shared Key	<input type="text"/>
RADIUS Server	0.0.0.0
RADIUS Port	1812
RADIUS Key	<input type="text"/>
Group Key Rotation Interval	0
WPAWPA2 Re-auth Interval	3600
WEP Encryption	Disabled
Shared Key Authentication	Optional
802.1x Authentication	Disabled
Network Key 1	<input type="text"/>
Network Key 2	<input type="text"/>
Network Key 3	<input type="text"/>
Network Key 4	<input type="text"/>
Current Network Key	1
PassPhrase	<input type="text"/> <input type="button" value="Generate WEP Keys"/>
<input type="button" value="Apply"/>	
WiFi Protected Setup (WPS)	
WPS Config	Disable
Button Mode	SES
Device Name	BroadcomAP
STA PIN	94380507
<input type="button" value="Apply"/>	
WPS Method	Push Button <input type="button" value="Start WPS"/>
WPS Status:	

Figure 53 Wireless 802.11b/g Privacy Page



Table 24 Field Descriptions for the Wireless 802.11b/g Privacy Page

Field	Description
WPA WPA2	Enables or disables Wi-Fi Protected Access (WPA) encryption.
WPA-PSK WPA2-PSK	Enables or disables a local pre-shared key (WPA-PSK) passphrase.
WPA/WPA2 Encryption	When using WPA or WPA-PSK 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	Sets the WPA Pre-Shared Key (PSK). This is either an 8-63 ASCII character string or a 64-digit hex number. Enabled when the Network Authentication method is WPA-PSK.
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	WPA and WPA2 are two security features in Wi-Fi technology. This field, re-authentication interval, is the amount of time the wireless router can wait before re-establishing authentication with the CPE.
WEP Encryption	Enables or disables Wired Equivalent Privacy encryption.



Field	Description
Shared Key Authentication	<p>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.</p> <p>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.</p>
802.1x Authentication	<p>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.</p>
Network Key 1-4	<p>Sets the static WEP keys when WEP encryption is enabled.</p> <p>Enter 5 ASCII characters or 10 hexadecimal digits for a 64-bit key.</p> <p>Enter 13 ASCII characters or 26 hexadecimal digits for a 128-bit key.</p> <p>When both WPA encryption and WEP encryption are enabled, only keys 2 and 3 are available for WEP encryption.</p>
Current Network Key	<p>Selects the encryption (transmit) key when WEP encryption is enabled.</p>
PassPhrase	<p>Sets the text to use for WEP key generation.</p>
WPS Config	<p>Allows the Wi-Fi Protected Setup to be enabled or disabled.</p>
Button Mode	<p>Allows the type of setup for the Wireless Security:</p> <p>SES — Secure Easy Setup</p> <p>WPS — Wi-Fi Protected Setup</p>
Device Name	<p>Name of the WPS device</p>
STA PIN	<p>The station PIN method, entered as the "representative" of the Network that follows the WPS protocol architecture.</p>
WPS Method	<p>There are two types of methods used for the Wi-Fi Protected Setup: PIN and Push Button</p>
WPS Status	<p>Shows the status of the Wi-Fi Protected Setup.</p>



Wireless 802.11b/g Access Control Page

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

MAC				
MAC Restrict Mode	Disabled ▼			
MAC Addresses	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Apply				
Connected Clients				
MAC Address	Age(s)	RSSI(dBm)	IP Addr	Host Name
00:18:F8:28:6E:4F	0	-22	192.168.0.11	mg1853-03

Figure 54 Wireless 802.11b/g Access Control Page

Table 25 Field Descriptions for the Wireless 802.11b/g 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 802.11b/g Advanced Page

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

54g™ Mode	54g LRS
Basic Rate Set	Default
54g™ Protection	Auto
XPress™ Technology	Disabled
Afterburner™ Technology	Disabled
Rate	Auto
Output Power	100%
Beacon Interval	100
DTIM Interval	1
Fragmentation Threshold	2346
RTS Threshold	2347
<input type="button" value="Apply"/>	

Figure 55 Wireless 802.11b/g Advanced Page

Table 26 Field Descriptions for the Wireless 802.11b/g Access Control 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.



Field	Description
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 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 SGB901N-2.1.1.0-LAB-00-SH.bin values provide higher performance but result in decreased client battery life, while higher values provide lower performance but result in increased client battery life.
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 Bridging Page

This page allows you to configure the WDS features.

Wireless Bridging	Disabled ▾
Remote Bridges	<input type="text"/>
	<input type="text"/>
	<input type="text"/>
	<input type="text"/>
	Apply

Figure 56 Wireless Bridging Page

Table 27 Field Descriptions for the Wireless 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.



Wireless 802.11b/g Wi-Fi Multimedia Page

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

WMM Support								On
No-Acknowledgement								Off
Power Save Support								On
Apply								
EDCA AP Parameters:	CWmin	CWmax	AIFSN	TxOP(b) Limit (usec)	TxOP(a/g) Limit (usec)	Admission Control	Discard Oldest First	
AC_BE	15	63	3	0	0		Off	
AC_BK	15	1023	7	0	0		Off	
AC_VI	7	15	1	6016	3008		Off	
AC_VO	3	7	1	3264	1504		Off	
EDCA STA Parameters:								
AC_BE	15	1023	3	0	0			
AC_BK	15	1023	7	0	0			
AC_VI	7	15	2	6016	3008			
AC_VO	3	7	2	3264	1504			
Apply								

Figure 57 Wireless 802.11b/g Wi-Fi Multimedia Page

Table 28 Field Descriptions for the Wireless 802.11b/g 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 that are in power-save mode. Queued packets are transmitted when the STA notifies AP that it has left power-save mode.



Field	Description
EDCA AP Parameters	<p>Specifies the transmit parameters for traffic transmitted from the AP to the STA in four Access Categories:</p> <ul style="list-style-type: none">Best Effort (AC_BE)Background (AC_BK)Video (AC_VI)Voice (AC_VO) <p>Transmit parameters include Contention Window (CW_{min} and CW_{max}), Arbitration Inter Frame Spacing Number (AIFSN), and Transmit Opportunity Limit (TXOP Limit).</p> <p>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.</p>
EDCA STA Parameters	<p>Specifies the transmit parameters for traffic transmitted from the STA to the AP in four Access Categories:</p> <ul style="list-style-type: none">Best Effort (AC_BE)Background (AC_BK)Video (AC_VI)Voice (AC_VO) <p>Transmit parameters include Contention Window (CW_{min} and CW_{max}), Arbitration Inter Frame Spacing Number (AIFSN), and Transmit Opportunity Limit (TXOP Limit).</p>



Wireless 802.11b/g 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.

Guest Network	
MOTOROLA_GUEST (XXXXXXXXXXXX)	
Guest WiFi Security Settings	
Current Guest Network	Disabled
Guest Network Name (SSID)	MOTOROLA_GUEST
Closed Network	Disabled
WPA	Disabled
WPA-PSK	Disabled
WPA2	Disabled
WPA2-PSK	Disabled
Guest LAN Settings	
DHCP Server	Disabled
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Lease Pool Start	192.168.2.10
Lease Pool End	192.168.2.99
Lease Time	86400
Apply	
Restore Guest Network Defaults	
WPA/WPA2 Encryption	
WPA/WPA2 Encryption	Disabled
WPA Pre-Shared Key	
RADIUS Server	0.0.0.0
RADIUS Port	1812
RADIUS Key	
WPA/WPA2 Re-auth Interval	
Group Key Rotation Interval	0
WPA/WPA2 Re-auth Interval	3600
WEP Encryption	
WEP Encryption	Disabled
Shared Key Authentication	Optional
802.1x Authentication	Disabled
Network Key 1	
Network Key 2	
Network Key 3	
Network Key 4	
Current Network Key	1
PassPhrase	
Generate WEP Keys	
Apply	

Figure 58 Wireless 802.11b/g Guest Network Page



Table 29 Field Descriptions for the Wireless 802.11b/g 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
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 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.



Configuring the Wireless Clients

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.


On a PC with Wireless Client Manager installed, the  icon is displayed on the Windows task bar. Double-click the icon to launch the utility. You may need to do the following to use a wireless client computer to access the Internet:

Table 30 Configuring 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 Basic 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.



UNCONTROLLED DOCUMENT



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 Lights and Error Conditions](#).

Solutions

Table 31 Troubleshooting Solutions

Problem	Possible Solution
Power light is off	<p>Check that the SBG901 is properly plugged into the electrical outlet.</p> <p>Check that the electrical outlet is working.</p> <p>Press the Reset button.</p>
Cannot send or receive data	<p>On the front panel, note the status of the LEDs and refer to Front-Panel Lights 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.</p> <p>Check the coaxial cable at the SBG901 and wall outlet. Hand-tighten if necessary.</p> <p>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.</p> <p>Check that the Ethernet cable is properly connected to the SBG901 and the computer.</p>
A wireless client(s) cannot send or receive data	<p>Perform the first four checks in "Cannot send or receive data."</p> <p>Check the Security Mode setting on the Wireless Security Page:</p> <ul style="list-style-type: none">• 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.



Problem	Possible Solution
	<p>After resolving your problem, be sure to re-enable wireless security.</p> <p>On the Wireless Basic Page:</p> <ul style="list-style-type: none">• Check whether you turned on Disable SSID Broadcast. If it is on, be sure the network name (SSID) on each affected wireless client is identical to the SSID on the SBG901.• 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	<p>On the Wireless Security Page, check whether the WPA Encryption type is TKIP. If all of your wireless clients support AES, change the WPA Encryption to AES.</p>

Front-Panel LEDs and Error Conditions

The SBG901 front panel LEDs provide status information for the following error conditions:

Table 32 Front-Panel LEDs and Error Conditions

LED	Status	If, During Startup:	If, During Normal Operation:
POWER	OFF	The SBG901 is not properly plugged into the power outlet	The SBG901 is unplugged
RECEIVE	FLASHING	The downstream receive channel cannot be acquired	The downstream channel is lost
SEND	FLASHING	The upstream send channel cannot be acquired	The upstream channel is lost
ONLINE	FLASHING	IP registration is unsuccessful	The IP registration is lost



11

Contact Us

If you need assistance while working with the SBG901, contact your Internet Service provider.

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

For answers to typical questions, see [Frequently Asked Questions](#).

UNCONTROLLED DOCUMENT



UNCONTROLLED DOCUMENT



Specifications

Table 33 Product Specifications

GENERAL	
Standards	Interoperates with DOCSIS and Euro-DOCSIS 2.0/1.1
Cable Interface	F-connector, female, 75 Ω
Network Interface	One 10/100 Ethernet port
Wireless Interface	802.11b/g Wi-Fi
Dimensions	26.7 cm L x 18.41 cm W x 5.72 cm H (10.50 in x 7.25 in x 2.25 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)
802.11 i 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

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. Battery back-up times may vary based on many factors, including the battery age, charging state, storing conditions, and operating temperature, as well as by factors such as data activity.

UNCONTROLLED DOCUMENT



UNCONTROLLED DOCUMENT



B

Glossary

This glossary defines terms and lists acronyms used with the SBG901.

Table 34 Glossary

TERM	DEFINITION
A	
access point	A device that provides WLAN connectivity to wireless clients (stations). The SBG901 acts as a wireless access point.
adapter	A device or card that connects a computer, printer, or other peripheral device to the network or to some other device. A wireless adapter connects a computer to the WLAN.
address	See NAT translation.
ALG	Some file transfer (for example, FTP), game, and video conferencing applications require application-level gateway triggers to open one or more ports to enable the application to operate properly.
American Wire Gauge (AWG)	A standard system used to designate the size of electrical conductors; gauge numbers are inverse to Gauge (AWG) size.
ANX	Automotive Network Exchange
ARP	Address Resolution Protocol broadcasts a datagram to obtain a response containing a MAC address corresponding to the host IP address. When it is first connected to the network, a client sends an ARP message. The SBG901 responds with a message containing its MAC address. Subsequently, data sent by the computer uses the SBG901 MAC address as its destination.
ASCII	The American Standard Code for Information Interchange refers to alphanumeric data for processing and communication compatibility among various devices; normally used for asynchronous transmission.
attenuation	The difference between transmitted and received power resulting from loss through equipment, transmission lines, or other devices; usually expressed in decibels.



TERM	DEFINITION
Authentication	A process where the CMTS verifies that access is authorized, using a password, trusted IP address, or serial number.
Authorization	Part of the process between a CMTS and the cable modem or gateway to enable Baseline Privacy.
auto-MDIX	Automatic medium-dependent interface crossover detects and corrects cabling errors by automatically reversing the send and receive pins on any port. It enables the use of straight-through wiring between the SBG901 Ethernet port and any computer, printer, or hub
B	
bandwidth	The transmission capacity of a medium in terms of a range of frequencies. Greater bandwidth indicates the ability to transmit more data over a given period of time.
Baseline Privacy	An optional feature that encrypts data between the CMTS and the cable modem or gateway. Protection of service is provided by ensuring that a cable modem or gateway, uniquely identified by its MAC address, can only obtain keys for services it is authorized to access.
Baud	The analog signaling rate. For complex modulation modes, the digital bit rate is encoded in multiple bits per baud. For example, 64 QAM encodes 6 bits per baud, and 16 QAM encodes 4 bits per baud.
BER	The bit error rate is the ratio of the number of erroneous bits or characters received from some fixed number of bits transmitted.
binary	A numbering system that uses two digits, 0 and 1.
bit rate	The number of bits (digital 0s and 1s) transmitted per second in a communications channel. It is usually measured in bits per second bps.
BPKM	Baseline Protocol Key Management encrypts data flows between a cable modem or gateway and the CMTS. The encryption occurs after the cable modem or gateway registers to ensure data privacy across the RF network.
bps	Bits per second



TERM	DEFINITION
bridge	An OSI layer 2 networking device that connects two LANs using similar protocols. It filters frames based on the MAC address to reduce the amount of traffic. A bridge can be placed between two groups of hosts that communicate a lot together, but not so much with the hosts in the other group. The bridge examines the destination of each packet to determine whether to transmit it to the other side. See also switch.
broadband	High bandwidth network technology that multiplexes multiple, independent carriers to carry voice, video, data, and other interactive services over a single cable. A communications medium that can transmit a relatively large amount of data in a given time period. A frequently used synonym for cable TV that can describe any technology capable of delivering multiple channels and services.
broadcast	Simultaneous transmission to multiple network devices; a protocol mechanism supporting group and universal addressing. See also multicast and unicast.
C	
CableHome	A project of CableLabs and technology suppliers to develop interface specifications for extending high-quality, cable-based services to home network devices. It addresses issues such as device interoperability, QoS, and network management. CableHome will enable cable service providers to offer more services over HFC. It will improve consumer convenience by providing cable-delivered services throughout the home.
CableLabs	A research consortium that defines the interface requirements for cable modems and acknowledges that tested equipment complies with DOCSIS.
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 or Euro-DOCSIS cable modems only.
cable modem configuration file	File containing operational parameters that a cable modem or gateway downloads from the Internet Service provider TFTP server during registration.
Class C network	An IP network containing up to 253 hosts. Class C IP addresses are in the form "network.network. network. host."
client	In a client/server architecture, a client is a computer that requests files or services, such as file transfer, remote login, or printing from the



TERM	DEFINITION
	server. Also called a CPE. On a WLAN, a client is any host that can communicate with the access point. A wireless client is also called a "station."
CMTS	A cable modem termination system is a device in the cable system headend that interfaces the HFC network to local or remote IP networks to connecting IP hosts, cable modems or gateways, and subscribers. It manages all cable modem bandwidth. It is sometimes called an edge router.
CNR	carrier to noise ratio
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.
CoS	Class of service traffic management or scheduling functions are performed when transferring data upstream or downstream on HFC.
CPE	Customer premise equipment, typically computers, printers, etc., are connected to the cable modem or gateway at the subscriber's location. CPE can be provided by the subscriber or the Internet Service provider. Also called a client.
crosstalk	An undesired signal interfering with the desired signal.
D	
default route	The route by which packets are forwarded when other routes in the routing table do not apply.
dB	Decibel
dBc	Signal level expressed in dB relative to the unmodulated carrier level desired.
DBm	A unit of measurement referenced to one milliwatt across specified impedance. 0dBm = 1 milliwatt across 75 ohms.
dBmV	Signal level expressed in dB as the ratio of the signal power in a 75-ohm system to a reference power when 1 mV is across 75 ohms.



TERM	DEFINITION
demodulation	An operation to restore a previously modulated wave and separate the multiple signals that were combined and modulated on a sub carrier.
DHCP	<p>A Dynamic Host Configuration Protocol server dynamically assigns IP addresses to client hosts on an IP network. DHCP eliminates the need to manually assign static IP addresses by “leasing” an IP address and subnet mask to each client. It enables the automatic reuse of unused IP addresses.</p> <p>The SBG901 is simultaneously a DHCP client and a DHCP server.</p> <p>A DHCP server at the cable system headend assigns a public IP address to the SBG901 and optionally to clients on the SBG901 LAN.</p> <p>The SBG901 contains a built-in DHCP server that assigns private IP addresses to clients.</p>
Distortion	An undesired change in signal waveform within a transmission medium. A nonlinear reproduction of the input waveform.
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.
DNS	The Domain Name System is the Internet system for converting domain names to IP addresses. A DNS server contains a table matching domain names, such as Internetname.com, to IP addresses, such as 192.169.9.1. When you access the world-wide web, a DNS server translates the URL displayed on the browser to the destination website IP address. The DNS lookup table is a distributed Internet database; no one DNS server lists all domain names to IP address matches.
DOCSIS	The CableLabs Data-Over-Cable Service Interface Specification defines interface standards for cable modems, gateways, and supporting equipment to deliver data between an HFC network and computer systems or television sets. To emphasize its use as a cable modem standard, DOCSIS is now called CableLabs Certified Cable Modems. Euro-DOCSIS is DOCSIS adapted for use in Europe.



TERM	DEFINITION
domain name	A unique name, such as motorola.com, that maps to an IP address. Domain names are typically much easier to remember than are IP addresses.
dotted-decimal format	A method of representing an IP address or subnet mask using four decimal numbers called octets. Each octet represents eight bits. In a class C IP address, the octets are "network.network.network.host." The first three octets together represent the network address and the final octet is the host address. In the SBG901 LAN default configuration, 192.168.100 represents the network address. In the final octet, the host address can range from 2 to 254.
download	To copy a file from one computer to another. You can use the Internet to download files from a server to a computer. A DOCSIS or Euro-DOCSIS cable modem or gateway downloads its configuration file from a TFTP server during start-up.
downstream	In a cable data network, the direction of data received by the computer from the Internet.
driver	Software that enables a computer to interact with a network or other device. For example, there are drivers for printers, monitors, graphics adapters, modems, Ethernet, USB, HPNA, and many others.
DSSS	Direct Sequence Spread Spectrum is an IEEE 802.11b RF modulation protocol.
dynamic IP address	An IP address that is temporarily leased to a host by a DHCP server. The opposite of static IP address.
E	
encapsulate	To introduce data into some other data unit to hide the format of the data.
encode	To alter an electronic signal so that only an authorized user can unscramble it to view the information.
encrypt	To encode data.
Ethernet	The most widely used LAN type, also known as IEEE 802.3. The most common Ethernet networks are 10Base-T, which provide transmission speeds up to 10 Mbps, usually over unshielded, twisted-pair wire terminated with RJ-45 connectors. Fast Ethernet (100Base-T) provides



TERM	DEFINITION
	speeds up to 100 Mbps. "Base" means "baseband technology" and "T" means "twisted pair cable." Each Ethernet port has a physical address called the MAC address.
Euro-DOCSIS	A ComLabs standard that is DOCSIS adapted for use in Europe.
event	A message generated by a device to inform an operator or the network management system that something has occurred.
expansion slot	A connection point in a computer where a circuit board can be inserted to add new capabilities.
F	
F-type connector	A type of connector used to connect coaxial cable to equipment such as the SBG901.
firewall	A security software system on the SBG901 that enforces an access control policy between the Internet and the SBG901 LAN.
flow	A data path moving in one direction.
FEC	Forward error correction is a technique to correct transmission errors without requiring the transmitter to resend any data.
FMDA	Frequency Division Multiple Access is a method to allow multiple users to share a specific radio spectrum. Each active user is assigned an individual RF channel (or carrier), with the carrier frequency of each channel offset from its adjacent channels by an amount equal to the channel spacing, which allows the required bandwidth per channel.
Frame	A unit of data transmitted between network nodes that contain addressing and protocol control data. Some control frames contain no data.
frequency	Number of times an electromagnetic signal repeats an identical cycle in a unit of time, usually one second, measured in Hz, kHz, MHz, or GHz.
FTP	File Transfer Protocol is a standard Internet protocol for exchanging files between computers. FTP is commonly used to download programs and other files to a computer from web pages on Internet servers.
full-duplex	The ability to simultaneously transmit and receive data. See also half-



TERM	DEFINITION
	duplex.
G	
gain	The extent to which a signal is boosted. A high-gain antenna increases the wireless signal level to increase the distance the signal can travel and remain usable.
gateway	A device that enables communication between networks using different protocols. See also router. The SBG901 enables up to 245 computers supporting IEEE 802.11b, or Ethernet to share a single broadband Internet connection.
gateway IP address	The address of the default gateway router on the Internet. Also known as the "giaddr."
GHz	Gigahertz — one billion cycles per second
GUI	graphical user interface
H	
half-duplex	Network where only one device at a time can transmit data. See also full-duplex.
headend	A location that receives TV programming, radio programming, and data that it modulates onto the HFC network. It also sends return data. Headend equipment includes transmitters, preamplifiers, frequency terminals, demodulators, modulators, and other devices that amplify, filter, and convert incoming broadcast TV signals to wireless and cable channels.
header	The data at the beginning of a packet that identifies what is in the packet.
hexadecimal	A base-sixteen numbering system that uses sixteen sequential numbers (0 to 9 and the letters A to F) as base units before adding a new position. On computers, hexadecimal is a convenient way to express binary numbers.
HFC	A hybrid fiber/coaxial cable network uses fiber-optic cable as the trunk and coaxial cable to the subscriber's premises.
hop	The interval between two routers on an IP network. The number of



TERM	DEFINITION
	hops a packet traverses toward its destination (called the hop count) is saved in the packet header. For example, a hop count of six means the packet has traversed six routers. The packet hop count increases as the time-to-live (TTL) value decreases.
host	In IP, a host is any computer supporting end-user applications or services with full two-way network access. Each host has a unique host number that, when combined with the network number, forms its IP address. Host also can mean: <ul style="list-style-type: none">• A computer running a web server that serves pages for one or more web sites belonging to organization(s) or individuals• A company that provides this service• In IBM environments, a mainframe computer
hub	On a LAN, a hub is a device that connects multiple hosts to the LAN. A hub performs no data filtering. See also bridge and router. An IP hub is typically a unit on a rack or desktop. On an HFC network, a hub is a scaled-down headend that performs some or all headend functions for part of the system.
Hz	Hertz — one cycle per second. The unit to measure the frequency that an alternating electromagnetic signal cycles through its highest and lowest states. Used to define the bands of the electromagnetic spectrum used in voice and data communications, or to define the bandwidth of a transmission medium.
I	
IANA	The Internet Numbering Address Authority (IANA) is an organization under the Internet Architecture Board (IAB) of the Internet Society that oversees IP address allocation. It is under a contract from the U.S. government.
ICMP	Internet Control Message Protocol is a protocol used for error, problem, and informational messages sent between IP hosts and gateways. ICMP messages are processed by the IP software and are not usually apparent to the end-user.
IEEE	The Institute of Electrical and Electronics Engineers, Inc. (http://www.ieee.org) is an organization that produces standards, technical papers, and symposiums for the electrical and electronic industries and is accredited by ANSI.



TERM	DEFINITION
IEEE 802.11b IEEE 802.11g	IEEE wireless network standards
IEEE 802.3	See Ethernet.
IGMP	Internet Group Membership Protocol is the Internet multicasting standard. IGMP establishes and maintains a database of group multicast addresses and interfaces to which a multicast router forwards multicast packets. IGMP runs between multicast hosts and their immediately-neighboring multicast routers.
IGMP spoofing	A process where a router acts as an IGMP querier for multicast hosts and an IGMP host to a multicast router.
impedance	The total opposition to AC electron current flow within a device. Impedance is typically 75 ohms for coax cable and other CATV components.
impulse noise	A noise of very short duration, typically along the order of 10 microseconds. It is caused by electrical transients such as voltage spikes, electric motors turning on, and lightning or switching equipment that bleed over to the cable.
ingress noise	Noise typically caused by discrete frequencies picked up by the cable plant from radio broadcasts or an improperly grounded or shielded home appliance such as a hair dryer. Ingress is the major source of cable system noise.
Internet	A worldwide collection of interconnected networks using TCP/IP.
Internetwork	A collection of interconnected networks allowing communication between all devices connected to any network in the collection.
IP	Internet Protocol is a set of standards that enable different types of computers to communicate with one another and exchange data through the Internet. IP provides the appearance of a single, seamless communication system and makes the Internet a virtual network.
IP address	<p>A unique 32-bit value that identifies each host on a TCP/IP network. TCP/IP networks route messages based on the destination IP address. An IP address has two parts:</p> <p>A network address assigned by IANA</p> <p>SBG901 network administrator assigns a host address to each host connected to the SBG901, automatically using its DHCP server as a</p>



TERM	DEFINITION
	static IP address. For a Class C network, the first 24 bits are the network address and the final 8 bits are the host address; in dotted-decimal format, the IP address appears as "network.network.network.host." If you enable the SBG901 DHCP client on the Basic DHCP Page, the Internet Service provider automatically assigns the network address, subnet mask, domain name, and DNS server to provide a continuous Internet connection.
IPSec	The Internet Protocol Security protocols are IETF authentication and encryption standards for secure packet exchange over the Internet. IPSec works at OSI layer 3 and secures everything on the network.
IKE	Internet Key Exchange
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
K	
kHz	kilohertz — one thousand cycles per second
L	
L2F	Layer 2 Forwarding is an OSI layer 2 protocol that establishes a secure tunnel across the Internet to create a virtual PPP connection between the user and the enterprise network. L2F is the most established and stable layer 2 tunneling protocol.
LAC	An L2TP access concentrator is a device to which the client directly connects. PPP frames are tunneled through the LAC to the LNS. The LAC need only implement the media over which L2TP operates to transmit traffic to one or more LNSs. The LAC may tunnel any protocol carried within PPP. The LAC initiates incoming calls and receives outgoing calls. A LAC is analogous to an L2F NAS.
LAN	A local area network provides a full-time, high-bandwidth connection over a limited area, such as a building or campus. Ethernet is the most widely used LAN standard.
layer	In networks, layers are software protocol levels. Each layer performs functions for the layers above it. OSI is a reference model having seven functional layers.



TERM	DEFINITION
LCP	Link Control Protocol establishes, configures, and tests data link connections used by PPP.
Latency	The time required for a signal to pass through a device. It is often expressed in a quantity of symbols.
LED	light-emitting diode
LNS	An L2TP network server is a termination point for L2TP tunnels where PPP frames are processed and passed to higher layer protocols. LNS can operate on any platform that terminates PPP. The LNS handles the server side of the L2TP protocol. L2TP relies only on the single media over which L2TP tunnels arrive. The LNS can have a single LAN or WAN interface, but can terminate calls arriving at any of the LAC's full range of PPP interfaces (asynchronous, synchronous, ISDN, V.120, etc.). The LNS initiates outgoing calls and receives incoming calls. LNS is analogous to a home gateway in L2F technology.
loopback	A test that loops the transmit signal to the receive signal. Usually, the loopback test is initiated on a network device. The test is used to verify a path or to measure the quality of a signal on that path.
M	
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.
MB	One megabyte; equals 1,024 x 1,024 bytes, 1,024 kilobytes, or about 8 million bits.
Mbps	Million bits per second (megabits per second). A rate of data transfer.
media	The various physical environments through which signals pass; for example, coaxial, unshielded twisted-pair (UTP), or fiber-optic cable.
MIB	A management information base is a unique hierarchical structure of software objects used by the SNMP manager and agent to configure, monitor, or test a device.
MHz	Megahertz — one million cycles per second. A measure of radio frequency.



TERM	DEFINITION
MPDU	MAC protocol data unit (PDU)
MSDU	MAC service data unit
MSO	Multiple System Operator. A company that owns and operates more than one cable system. Also called a group operator.
MTU	The Maximum Transmission Unit is the largest amount of data that can be transmitted in one discrete message on a given physical network. The MTU places an upper limit on the size of a message that can be transferred by the network in a single frame. Messages exceeding the MTU must be fragmented before transmission and reassembled at the destination.
Multicast	A data transmission sent from one sender to multiple receivers. See also broadcast and unicast.
mW	Milliwatts; a measure of electrical power
N	
NAS	Network access server
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.
NAPT	Network Address Port Translation is the most common form of address translation between public and private IP addresses. NAPT maps one public IP address to many private IP addresses. If NAPT is enabled on the Basic Setup Page, one public IP address is mapped to an individual private IP address for up to 245 LAN clients.
NEC	National Electrical Code (United States) — The regulations for construction and installation of electrical wiring and apparatus, suitable for mandatory application by a wide range of state and local authorities.
network	Two or more computers connected to communicate with each other. Networks have traditionally been connected using some kind of wiring.
network driver	Software packaged with a NIC that enables the computer to communicate with the NIC.
network layer	Layer 3 in the OSI architecture that provides services to establish a



TERM	DEFINITION
	path between open systems. The network layer knows the address of the neighboring nodes, packages output with the correct network address data, selects routes, and recognizes and forwards to the transport layer incoming messages for local host domains.
NIC	A network interface card converts computer data to serial data in a packet format that it sends over the LAN. A NIC is installed in an expansion slot or can be built-in. Every Ethernet NIC has a MAC address permanently saved in its ROM.
node	On a LAN, a generic term for any network device. On an HFC network, the interface between the fiber-optic trunk and coaxial cable feeders to subscriber locations. A node is typically located in the subscriber's neighborhood.
noise	Random spurts of electrical energy or interface. May produce a salt-and-pepper pattern on a television picture.
O	
ohm	A unit of electrical resistance.
OSI	The Open Systems Interconnection reference model is an illustrative model describing how data moves through a network from an application on the source host to an application on the destination host. It is a conceptual framework developed by ISO that is now the primary model for intercomputer communications. OSI is a model only; it does not define a specific networking interface.
P	
packet	The unit of data that is routed between the sender and destination on the Internet or other packet-switched network. When data, such as an e-mail message, is sent over the Internet, the sender's IP divides the data into uniquely-numbered packets. The packet header contains the source and destination IP addresses. The individual packets may travel different routes. When all packets arrive at the destination, IP at that end reassembles the packets.
packet-switched	A scheme to handle transmissions on a connectionless network such as the Internet. An alternative is circuit-switched.
PacketCable	A CableLabs-led project to define a common platform to deliver advanced, real-time multimedia services over two-way HFC cable plant. Built on DOCSIS 1.1, PacketCable networks use IP technology as the



TERM	DEFINITION
	basis for a highly-capable multimedia architecture.
pass-through	A pass-through client on the SBG901 LAN obtains its public IP address from the Internet Service provider's DHCP server.
PAT	Port Address Translation
PCI	Peripheral Component Interconnect
PCMCIA	The Personal Computer Memory Card International Association sets international standards for connecting peripherals to portable computers. Laptop computers typically have a PCMCIA slot that can hold one or two PC Cards to provide features such as Ethernet connectivity.
PDA	personal digital assistant
PDU	A protocol data unit is a message containing operational instructions used for SNMP. The basic SNMP V2 PDU types are get-request, get-next-request, get-bulk-request, response, set-request, inform-request, and trap.
periodic ranging	Ranging that is performed on an on-going basis after initial ranging has taken place.
physical layer	Layer 1 in the OSI architecture. It provides services to transmit bits or groups of bits over a transmission link between open systems. It entails the electrical, mechanical, and handshaking procedures.
piggybacking	A process that occurs when a cable modem simultaneously transmits data and requests additional bandwidth.
PING	A network utility that tests host reachability by sending a small packet to the host and waiting for a reply. If you PING a computer IP address and receive a reply, you know the computer is reachable over the network. It also stands for Packet InterNet Groper.
PMD	The physical media-dependent sublayer of the physical layer which transmits bits or groups of bits over particular types of transmission links between open systems. It entails the electrical, mechanical, and handshaking procedures.
point-to-point	Physical connection made from one point to another.



TERM	DEFINITION
port	On a computer or other electronic device, a port is a socket or plug used to physically connect it to the network or to other devices. In TCP/IP, a port is a number from 0 to 65536 used logically by a client program to specify a server program. Ports 0 to 1024 are reserved
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.
PPP	Point-to-Point Protocol is used to transport other protocols, typically for simple links over serial lines. It is most commonly used to access the Internet with a dial-up modem.
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.
protocol	A formal set of rules and conventions for exchanging data. Different computer types (for example PC, UNIX, or mainframe) can communicate if they support common protocols.
provisioning	The process of auto discovery or manually configuring a cable modem on the CMTS.
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.
Q	
QAM	Quadrature Amplitude Modulation uses amplitude and phase modulation to encode multiple bits of data in one signaling element. QAM achieves faster data transfer than amplitude or phase modulation alone, but the signal is more prone to errors caused by noise. QAM requires a transmission circuit with a higher CNR than alternate modulation formats such as QPSK. Two types of QAM are: 16 QAM, which encodes four bits per symbol as one of 16 possible amplitude and phase combinations. 64 QAM, which encodes six bits per symbol as one of 64 possible amplitude and phase combinations.



TERM	DEFINITION
QPSK	Quadrature Phase Shift Keying is a phase modulation algorithm. Phase modulation is a version of frequency modulation where the phase of the carrier wave is modulated to encode bits of digital information in each phase change.
QoS	Quality of service describes the priority, delay, throughput, and bandwidth of a connection.
R	
RAS	Remote Access Server
registration	How a cable modem makes itself known to the CMTS. The cable modem configuration file and authorization are verified and the CoS is negotiated.
return loss	A measurement of the quality of the match of the device to the cable system. Return loss is the ratio of the amount of power reflected by the device. A return loss of 20 dB or greater is preferred.
RF	Radio Frequency — signals used by the CMTS transmitter and receiver to send data over HFC. The carrier is modulated to encode the digital data stream for transmission across the cable network.
RJ-11	The most common type of connector for household or office phones.
RJ-45	An 8-pin modular connector; the most common connector type for 10Base-T or 100Base-T Ethernet networks.
ROM	read-only memory
router	<p>On IP networks, a device connecting at least two networks, which may or may not be similar. A router is typically located at a gateway between networks. A router operates on OSI network layer 3. It filters packets based on the IP address, examining the source and destination IP addresses to determine the best route on which to forward them.</p> <p>A router is often included as part of a network switch. A router can also be implemented as software on a computer.</p>
routing table	A table listing available routes that is used by a router to determine the best route for a packet.



TERM	DEFINITION
S	
scope	The set of IP addresses that a DHCP server can lease to clients.
server	In a client/server architecture, a dedicated computer that supplies files or services such as file transfer, remote login, or printing to clients.
service provider	A company providing data services to subscribers.
SDU	service data unit
SID	A service ID is a unique 14-bit identifier the CMTS assigns to a cable modem or gateway that identifies the traffic type it carries (for example, data). The SID provides the basis for the CMTS to allocate bandwidth to the cable modem and implement CoS.
SME	small and medium enterprise
SMTP	Simple Mail Transfer Protocol is a standard Internet protocol for transferring e-mail.
SNMP	Simple Network Management Protocol is a standard to monitor and manage networks and network devices. Data is exchanged using PDU messages.
SOHO	small office home office
spectrum	A specified range of frequencies used for transmission of electromagnetic signals.
spectrum allocation	An allocation of portions of the available electromagnetic spectrum for specific services, such as AM, FM, or personal communications.
splitter	A device that divides the signal from an input cable between two or more cables.
SSID	The Service Set Identifier or network name is a unique identifier that wireless clients use to associate with an access point to distinguish between multiple WLANs in the same area. All clients on a WLAN must have the same SSID as the access point.



TERM	DEFINITION
stateful-inspection	<p>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:</p> <ul style="list-style-type: none">• 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 <p>A stateful inspection firewall is more advanced than a static filter firewall.</p>
static filter	<p>A type of firewall that examines the source and destination in the packet header based on administrator-defined rules only.</p>
static IP address	<p>An IP address that is permanently assigned to a host. Normally, a static IP address must be assigned manually. The opposite of dynamic IP address.</p>
static route	<p>A manually-defined route.</p>
station	<p>IEEE 802.11b term for wireless client.</p>
subscriber	<p>A home or office user who accesses television, data, or other services from an Internet Service provider.</p>
subnet mask	<p>A bit mask that is logically ANDed with the destination IP address of a packet to determine the network address. A router routes packets using the network address.</p>
subnetwork	<p>A part of a network; commonly abbreviated "subnet." When subnetting is used, the host portion of the IP address is divided into a subnet and host number. Hosts and routers use the subnet mask to identify the bits used for the network and subnet number.</p>
switch	<p>On an Ethernet network, a switch filters frames based on the MAC address, in a manner similar to a bridge. A switch is more advanced because it can connect more than two segments.</p>



TERM	DEFINITION
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.
symbol rate	Also known as baud rate. This is a measure of the number of times per second a signal in a communications channel varies or makes a transition between states (states being frequencies, voltage levels or phase angles). Usually measured in symbols per second (sps).
SYSLOG	A de-facto UNIX standard for logging system events.
T	
TCP	Transmission Control Protocol on OSI transport layer four provides reliable transport over the network for data transmitted using IP (network layer three). It is an end-to-end protocol defining rules and procedures for data exchange between hosts on top of connectionless IP. TCP uses a timer to track outstanding packets, checks error in incoming packets, and retransmits packets if requested.
TCP/IP	Transmission Control Protocol/Internet Protocol suite. It provides standards and rules for data communication between networks on the Internet. It is the worldwide Internetworking standard and basic communications protocol of the Internet.
TFTP	Trivial File Transfer Protocol is a very simple protocol used to transfer files.
TKIP	Temporal Key Integrity Protocol
Transparent bridging	A method to enable all hosts on the wired Ethernet LAN, WLAN, and USB connection to communicate as if they were all connected to the same physical network.
transport layer	Layer of the OSI concerned with protocols for error recognition and recovery. This layer also regulates information flow.
trunk	Electronic path over which data is transmitted.
two-way	A cable system that can transmit signals in both directions to and from the headend and the subscriber.



TERM	DEFINITION
U-Z	
UDP	User Datagram Protocol
unicast	A point-to-point data transmission sent from one sender to one receiver. This is the normal way you access websites. See also broadcast and multicast.
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.
USB	Universal Serial Bus is a computer interface for add-on devices such as printers, scanners, mice, modems, or keyboards. USB supports data transfer rates of 480 bps and plug-and-play installation. You can connect up to 127 devices to a single USB port.
VLAN	A virtual local area network is group of devices on different LAN segments that are logically configured to communicate as if they are connected to the same wire.
WAN	A wide-area network provides a connection over a large geographic area, such as a country or the whole world. The bandwidth depends on need and cost, but is usually much lower than for a LAN.
WAP	Wireless access point or Wireless Access Protocol. See also access point
WECA	The Wireless Ethernet Compatibility Alliance is a trade organization that works to ensure that all wireless devices (computer cards, laptops, air routers, PDAs, etc) can communicate with each other.
WEP	Wired Equivalent Privacy encryption protects the privacy of data transmitted over a WLAN. WEP uses keys to encrypt and decrypt transmitted data. The access point must authenticate a client before it can transfer data to another client. WEP is part of IEEE 802.11b. Because WEP can be difficult to use and does not provide very strong encryption, Motorola recommends using WPA if possible.
Wi-Fi	Wireless fidelity (pronounced y-phi) brand name applied to products supporting IEEE 802.11b.
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.



TERM	DEFINITION
WLAN	wireless LAN
world wide web	An interface to the Internet that you use to navigate and hyperlink to information.
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.



Software License

SURFboard SBG901 Wireless Cable Modem Gateway

Motorola, Inc., ("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., 101 Tournament Drive, Horsham, PA 19044.



FOR PRODUCTION USE ONLY DO NOT TYPE OR DELETE PAST THIS SYMBOL: 

UNCONTROLLED DOCUMENT

UNCONTROLLED DOCUMENT



MOTOROLA

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

<http://www.motorola.com>

MOTOROLA and the Stylized M logo are registered in the US Patent and Trademark Office. All other product or service names are the property of their respective owners. ©2008 Motorola, Inc. All rights reserved.

558660-001-a
11/2008