



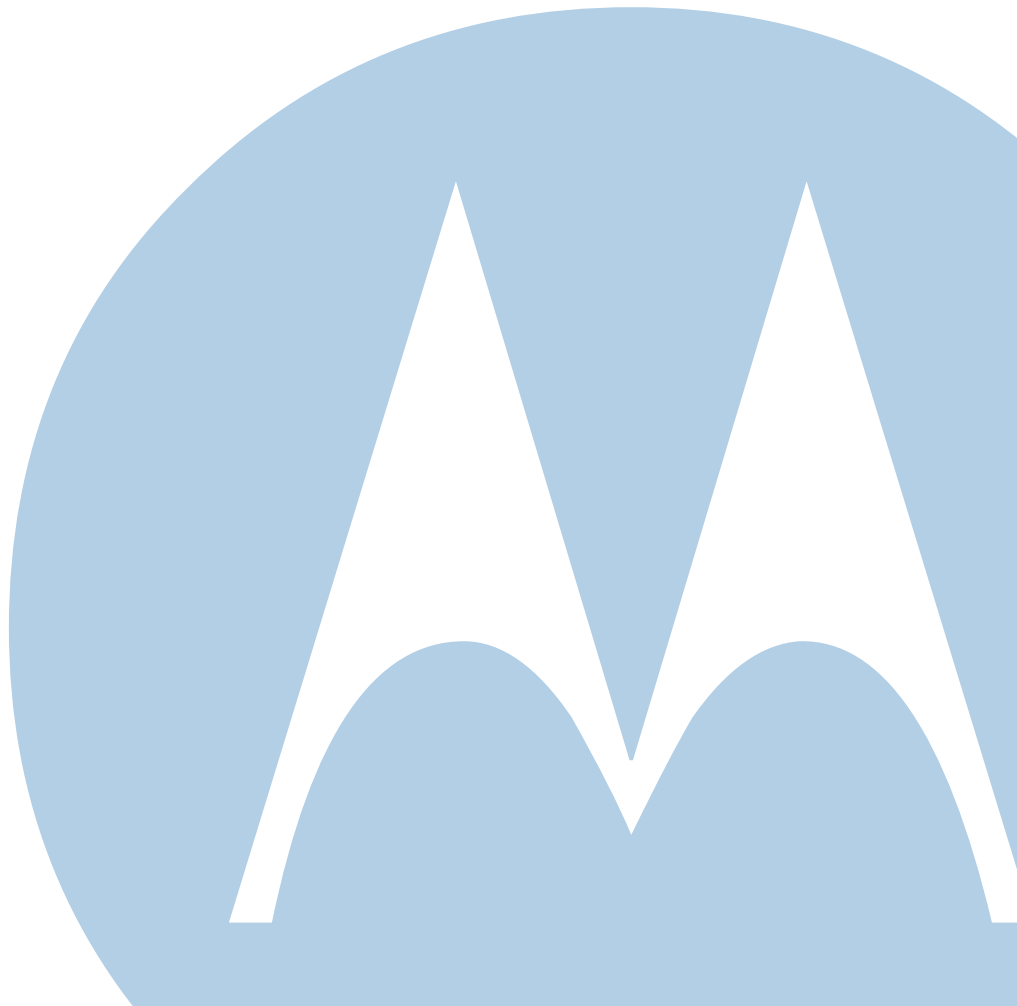
---

*User Guide*

---

**Motorola SURFboard<sup>®</sup>**

SVG1202 Wireless Voice Gateway





©2011 Motorola Mobility, Inc. All rights reserved.

MOTOROLA and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC. All other product or service names are the property of their respective owners. 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 Mobility, Inc.

Motorola Mobility reserves the right to revise this publication and to make changes in content from time to time without obligation on the part of Motorola Mobility to provide notification of such revision or change. Motorola Mobility 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 Mobility may make improvements or changes in the product(s) described in this manual at any time.



# Safety and Regulatory Information

## IMPORTANT SAFETY INSTRUCTIONS

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

- Read all of the instructions listed here and/or in the user manual before you operate this device. Give particular attention to all safety precautions. Retain the instructions for future reference.
- This device must be installed and used in strict accordance with manufacturer's instructions, as described in the user documentation that is included with the device.
- Comply with all warning and caution statements in the instructions. Observe all warning and caution symbols that are affixed to this device.
- To prevent fire or shock hazard, do not expose this device to rain or moisture. The device must not be exposed to dripping or splashing. Do not place objects filled with liquids, such as vases, on the device.
- This device was qualified under test conditions that included the use of the supplied cables between system components. To ensure regulatory and safety compliance, use only the provided power and interface cables and install them properly.
- Different types of cord sets may be used for connections to the main POWER supply circuit. Use only a main line cord that complies with all applicable device safety requirements of the country of use.
- Installation of this device must be in accordance with national wiring codes and conform to local regulations.
- Operate this device only from the type of power source indicated on the device's marking label. If you are not sure of the type of power supplied to your home, consult your dealer or local power company.
- Do not overload outlets or extension cords, as this can result in a risk of fire or electric shock. Overloaded AC outlets, extension cords, frayed power cords, damaged or cracked wire insulation, and broken plugs are dangerous. They may result in a shock or fire hazard.
- Route power supply cords so that they are not likely to be walked on or pinched by items placed upon or against them. Pay particular attention to cords where they are attached to plugs and convenience receptacles, and examine the point where they exit from the device.
- Place this device in a location that is close enough to an electrical outlet to accommodate the length of the power cord.
- Place the device to allow for easy access when disconnecting the power cord of the device from the AC wall outlet.
- Do not connect the plug into an extension cord, receptacle, or other outlet unless the plug can be fully inserted with no part of the blades exposed.
- Place this device on a stable surface.
- It is recommended that the customer install an AC surge protector in the AC outlet to which this device is connected. This is to avoid damaging the device by local lightning strikes and other electrical surges.
- Postpone installation until there is no risk of thunderstorm or lightning activity in the area.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning. For added protection, unplug the device from the wall outlet and disconnect the cables to avoid damage to this device due to lightning and power surges.
- Do not use this product near water: for example, near a bathtub, washbowl, kitchen sink or laundry tub, in a wet basement, or near a swimming pool.
- Do not use the telephone to report a gas leak in the vicinity of the leak.
- Disconnect TNV circuit connector before removing the cover.
- Disconnect TNV circuit connector(s) before disconnecting power.
- Do not cover the device or block the airflow to the device with any other objects. Keep the device away from excessive heat and humidity and keep the device free from vibration and dust.



- Wipe the device with a clean, dry cloth. Never use cleaning fluid or similar chemicals. Do not spray cleaners directly on the device or use forced air to remove dust.
- For added protection, unplug the device from the wall outlet and disconnect the cables to avoid damage to this device due to lightning and power surges.

**CAUTION:** To reduce the risk of fire, use only No. 26 AWG or larger (e.g., 24 AWG) UL Listed or CSA Certified Telecommunication Line Cord, or national equivalent.

- 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](http://www.motorola.com/recycle) for instructions on recycling.

## IMPORTANT VoIP SERVICE INFORMATION



Please contact your Internet Service Provider (ISP) and/or your local municipality for additional information on making emergency calls using VoIP service in your area.

**IMPORTANT:** When using this VoIP device, you CANNOT make any calls, including an emergency call, and emergency location services (where supported) WILL NOT be available, under the following circumstances:

- Your broadband ISP connection goes down, is lost, or otherwise fails.
- You lose electrical power.
- You have changed the physical address of your VoIP device, and you did not update or otherwise advise your VoIP service provider of this change.
- There are delays in making your location information available in or through the local automatic location information database.

**Note:** Your service provider, not Motorola, is responsible for the provision of VoIP telephony services through this equipment. Motorola shall not be liable for, and expressly disclaims, any direct or indirect liabilities, damages, losses, claims, demands, actions, causes of action, risks, or harms arising from or related to the services provided through this equipment.

## FCC STATEMENTS

### FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.



If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

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

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

### **FCC RADIATION EXPOSURE STATEMENT**

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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

### **WIRELESS LAN INFORMATION**

This device is a wireless network product that uses Direct Sequence Spread Spectrum (DSSS) radio technology. The device is designed to be inter-operable with any other wireless DSSS product that complies 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 assessible by unauthorized users. For more information on how to protect your, see the SVG1202 User Guide for instructions or visit the Motorola websits.



# Contents

<b>Safety and Regulatory Information</b> .....	<b>i</b>
<b>Getting Started</b> .....	<b>1</b>
Inside the Box .....	1
Minimum System Requirements .....	1
Contact Information.....	1
<b>Product Overview</b> .....	<b>2</b>
Front Panel .....	2
Rear Panel .....	3
MAC Label.....	3
<b>Connecting the Gateway</b> .....	<b>4</b>
Installing the SVG1202.....	4
Testing the Connections .....	5
Wall Mounting the Gateway.....	5
Wall Mounting Template.....	7
<b>Connecting to the Internet</b> .....	<b>8</b>
Before You Begin .....	8
Configuring TCP/IP for Windows 7 .....	8
Configuring TCP/IP for Windows Vista.....	8
Configuring TCP/IP for Windows XP .....	9
Renewing the IP Address in Windows 7 or Vista .....	9
Renewing the IP Address in Windows XP .....	10
Verifying the IP Address in Windows 7 or Vista.....	10
Verifying the IP Address in Windows XP .....	10
Setting Up a Wi-Fi Network Connection .....	10
<b>Monitoring Your Gateway</b> .....	<b>11</b>
Starting the Gateway Configuration Manager .....	11
SVG1202 Menu Options Bar .....	12
Changing the SVG1202 Default Password .....	13
Restoring Factory Defaults .....	13
Getting Help .....	13
Exiting the SVG1202 Configuration Manager.....	13
<b>Status Pages</b> .....	<b>14</b>
Status Software Page.....	14
Status Connection Page .....	14
Status Security Page .....	15
Status Diagnostics Page.....	15
Ping Utility.....	15
Traceroute Utility.....	16
Status Event Log Page .....	17
Status Configuration Page.....	17



<b>Basic Pages .....</b>	<b>18</b>
Basic Setup Page .....	18
Basic DHCP Page .....	19
Basic DDNS Page .....	20
Basic Backup Page .....	21
Restoring Your SVG1202 Configuration.....	21
Backing Up Your SVG1202 Configuration.....	21
<b>Advanced Pages .....</b>	<b>22</b>
Advanced Options Page .....	22
Advanced IP Filtering Page.....	24
Advanced MAC Filtering Page.....	25
Setting a MAC Address Filter .....	25
Advanced Port Filtering Page .....	26
Advanced Port Forwarding Page .....	27
Advanced Port Triggers Page .....	28
Advanced DMZ Host Page .....	29
Setting Up the DMZ Host .....	29
<b>Firewall Pages.....</b>	<b>30</b>
Firewall Web Content Filter Page.....	30
Firewall Local Log Page.....	31
Firewall Remote Log Page .....	31
<b>Parental Control Pages .....</b>	<b>32</b>
Parental Control User Setup Page.....	32
Parental Control Basic Setup Page.....	33
Parental Control Time of Day Filter Page .....	34
Parental Control Local Log Page .....	34
<b>Wireless Pages.....</b>	<b>35</b>
Wireless 802.11 Radio Page .....	35
Wireless 802.11 Primary Network Page .....	36
Wireless 802.11 Advanced Page.....	38
Wireless 802.11 Access Control Page .....	39
Wireless 802.11 Wi-Fi Multimedia Page.....	40
Wireless 802.11 Bridging Page .....	41
Setting Up Your Wireless LAN.....	41
Encrypting Wireless LAN Transmissions.....	42
Installing Wireless Clients .....	42
Installing a Wireless Client for WPA.....	43
Configuring a Wireless Client for WEP.....	43
Configuring a Wireless Client with the Network Name (SSID) .....	43
<b>MTA Pages .....</b>	<b>44</b>
MTA Status Page .....	44
MTA DHCP Page.....	44
MTA QoS Page.....	45
<b>Troubleshooting .....</b>	<b>46</b>



---

Solutions.....	46
Front Panel LEDs and Error Conditions.....	47
<b>Warranty Information .....</b>	<b>48</b>





# 1





## Getting Started

The Motorola SURFboard® SVG1202 Wireless Voice Gateway is designed for use in households with one or more computers capable of wireless and/or wired connectivity.

This guide provides product overview and setup information for the SVG1202. It also provides instructions for installing and configuring the gateway.

### Inside the Box

Before installing the gateway, check that the following items are included in the box with the gateway. If any items are missing, please contact Motorola Broadband Technical Support at **1-877-466-8646**.

ITEM		DESCRIPTION
<b>Power Supply</b>		Provides power to the gateway using an electrical outlet
<b>10/100Base-T Ethernet Cable</b>		Standard Category 5, or higher, cable for connecting to the network
<b>Software License &amp; Regulatory Card</b>		Contains software license, warranty, and safety information for the gateway
<b>SVG1202 Install Sheet</b>		Provides basic information for connecting the gateway

### Minimum System Requirements

The SVG1202 is compatible with the following operating systems:

- Windows® 7
- Windows Vista™, Service Pack 1 or later
- Windows XP, Service Pack 2 or later
- Mac® 10.4 or later
- UNIX®
- Linux®

### Contact Information

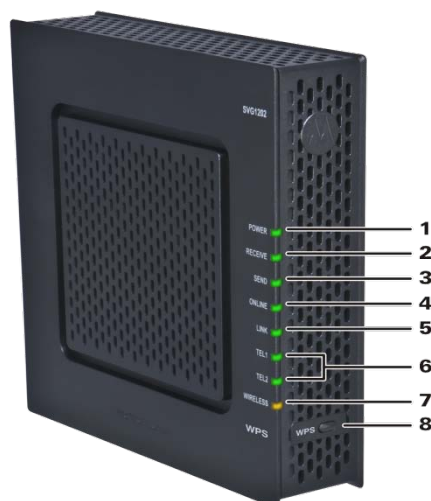
For additional product information, please visit the Motorola support website:  
[www.motorola.com/us/support](http://www.motorola.com/us/support)



# 2

## Product Overview

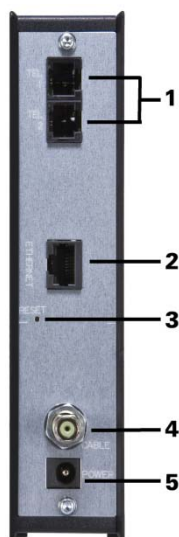
### Front Panel



LED	BLINKING	ON (SOLID)
1 <b>POWER</b>	Not applicable — icon does not flash	<b>Green:</b> Power is properly connected
2 <b>RECEIVE</b>	Scanning for a downstream (receive) channel connection	<b>Green:</b> Non-bonded downstream channel is connected
3 <b>SEND</b>	Scanning for an upstream (send) channel connection	<b>Green:</b> Non-bonded upstream channel is connected
4 <b>ONLINE</b>	Scanning for an Internet connection	<b>Green:</b> Startup process completed
5 <b>LINK</b>	Transmitting or receiving data on the Ethernet port	<b>Green:</b> A device is connected to the Ethernet (10Base-T) or Fast Ethernet (100Base-T) port
6 <b>TEL1 TEL2</b>	Telephone is off-hook; dialing or call is in progress	<b>Green:</b> Telephone is connected and activated; on-hook
7 <b>WIRELESS</b>	<b>Green:</b> Wi-Fi enabled with encrypted wireless data activity; long/short blinking indicates wireless pairing in progress <b>Amber:</b> Wi-Fi enabled with unencrypted wireless data activity	<b>Green:</b> Wireless pairing successfully established between the gateway and another Wi-Fi enabled device on your network — printer, PDA, laptop, etc. <b>Amber:</b> Wireless pairing was successful; LED turns solid green after five minutes
8 <b>WPS button</b>	Configures a Wi-Fi Protected Setup (WPS) enabled device to connect to a wireless network	



## Rear Panel



PORT/CONNECTOR	DESCRIPTION
<b>1 TEL 1</b>	VoIP connection for a single or two-line telephone
<b>TEL 2</b>	VoIP connection for a single-line telephone
<b>2 ETHERNET</b>	Ethernet port for an RJ-45 cable connection
<b>3 RESET</b>	Resets the gateway; may take from 5 to 30 minutes to scan and connect to the appropriate communications channels
	Press and hold the RESET switch for five seconds or longer to restore the factory default settings
<b>4 CABLE</b>	Coaxial cable connector
<b>5 POWER</b>	+12VDC Power connector

## MAC Label

The SVG1202 Media Access Control (MAC) label is located on the bottom of the gateway. It contains specific ID information for the gateway.

To receive data service, you may have to provide the MAC address (**HFC MAC ID**) and serial number located on the label to your Internet service provider.

To receive VoIP service, you may have to provide the **MTA MAC ID** to your VoIP provider.



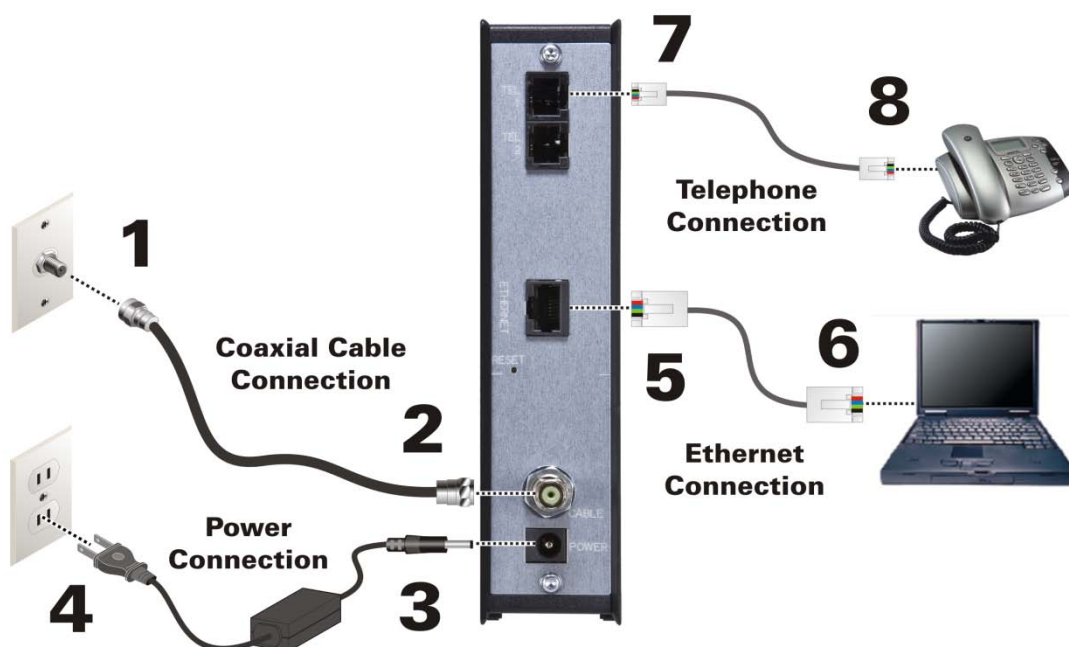
# 3

## Connecting the Gateway



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

### Installing the SVG1202



Before installing the gateway, choose a location where the computer and gateway are preferably near existing cable and electrical wall outlets. Also, make sure the computer is powered OFF.

1. Verify that the coaxial cable is connected to a cable outlet or splitter.
2. Connect the other end of the coaxial cable to the Cable connector on the gateway. Hand-tighten the connectors to avoid damaging them.
3. Plug the power cord into the Power port on the gateway.
4. Plug the other end of the power cord into an electrical wall outlet. This automatically powers ON the gateway. You do not need to unplug the gateway when it is not in use.

**Note:** The first time you plug in the gateway, allow from 5 to 30 minutes for the gateway to scan and connect to the appropriate communications channels.

5. Connect the Ethernet cable to the Ethernet port on the gateway.
6. Connect the other end of the Ethernet cable to the Ethernet port on the computer.
7. Plug the telephone cord of a single or two-line telephone into the telephone.
8. Plug the other end of the telephone cord into the Tel 1 port on the gateway.

**Note:** You must contact a VoIP service provider to activate the telephone service.



9. For a second telephone, plug the telephone cord of a single-line telephone into the Tel 2 port on the gateway.
10. Check that the LEDs on the front panel cycle through one by one in the following sequence:

### SVG1202 LED Activity During Startup

LED	DESCRIPTION
<b>POWER</b>	Turns solid green when AC power is connected to the gateway. Indicates power is connected properly.
<b>RECEIVE</b>	Blinks while scanning for a downstream (receive) channel. Turns solid green when the downstream channel is connected.
<b>SEND</b>	Blinks while scanning for an upstream (send) channel. Turns solid green when the upstream channel is connected.
<b>ONLINE</b>	Blinks during gateway registration and configuration. Turns solid green when the gateway is registered.
<b>LINK</b>	Turns solid when an Ethernet connection is made between the gateway and computer.

## Testing the Connections

Perform the following connectivity test to verify that all the components were connected properly:

1. Power ON the computer and log in.
2. Check that the POWER, RECEIVE, SEND, and LINK front panel LEDs on the gateway are either solid or blinking. See [Front Panel](#) for additional status information.

**Note:** The ONLINE LED should turn solid after the gateway is provisioned (activated).

## Wall Mounting the Gateway



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

You will need a screwdriver and two M3 (#6) screws.

1. Print the [Wall Mounting Template](#).

**Note:** You can mount the gateway horizontally or vertically.

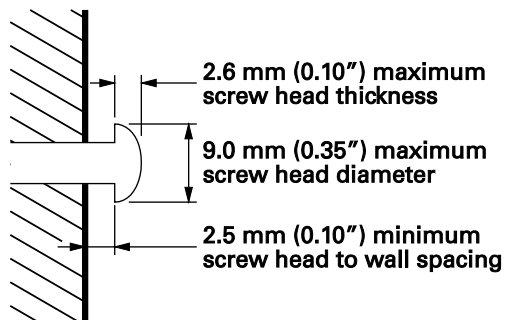
2. Remove all cables (power, coaxial, and Ethernet) from the gateway.
3. Choose a location on the wall to mount the gateway.

#### Notes:

- Locate the unit according to 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).



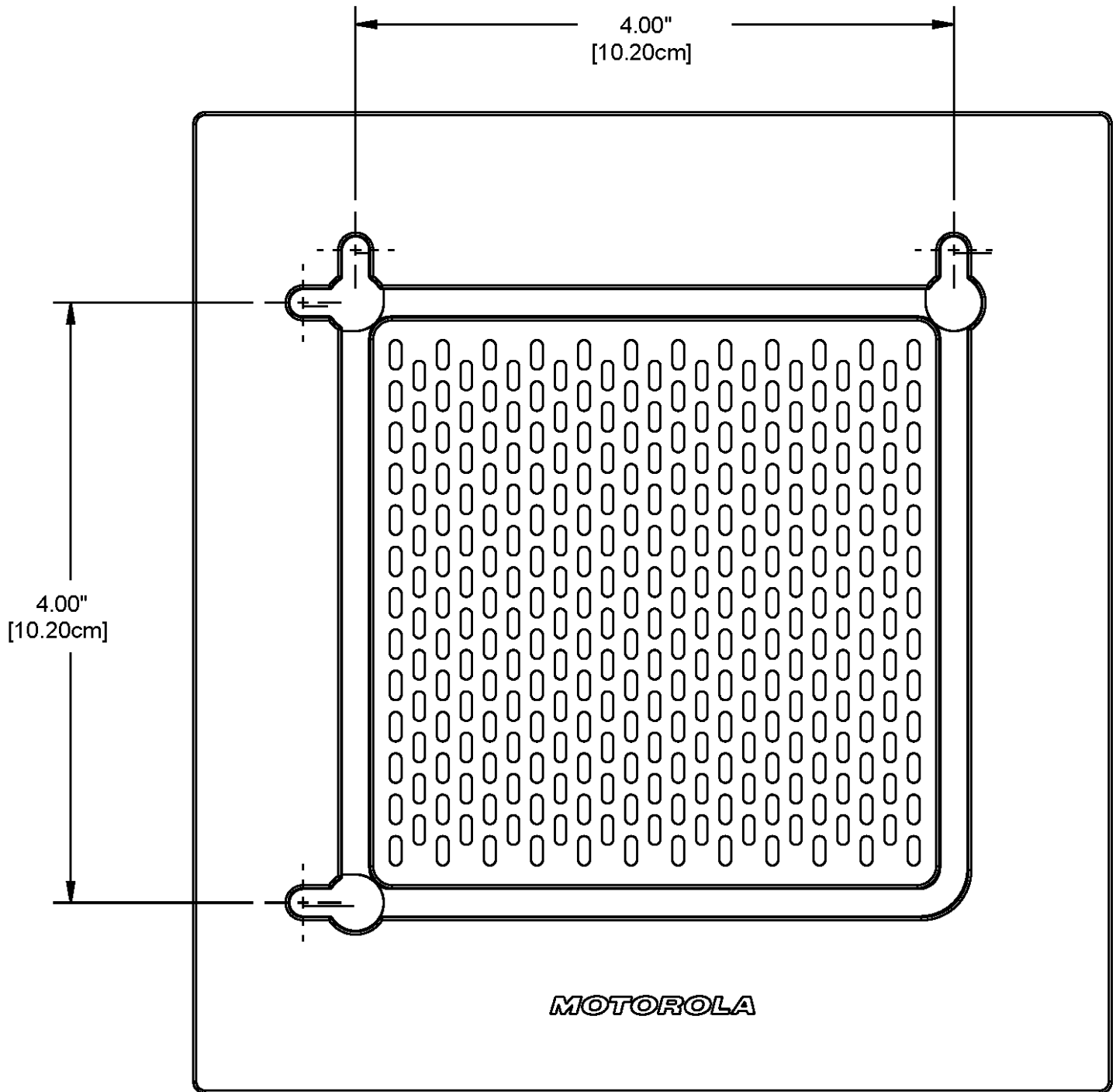
- It is recommended that you mount the gateway to concrete, masonry, a wooden stud, or some other solid wall material. Use anchor bolts if necessary (for example, if you mount the unit on drywall).
4. Position and secure the wall mounting template on the wall to mark the holes.



5. Select an appropriate depth and diameter to drill the holes to a depth of at least 1½ inches (3.8 cm).  
**Note:** There must be .10 inch (2.5 mm) between the wall and underside of the screw head.
6. Insert the #6 screws in the holes and then attach the gateway.
7. Verify the gateway is still securely attached to the wall.
8. Reconnect the coaxial, Ethernet, power cables.
9. Plug the power cord into an electrical outlet.
10. Arrange the cables to prevent any safety hazards.



## Wall Mounting Template





# 4

## Connecting to the Internet

### Before You Begin



**To prevent unauthorized user access, change the default username and password before proceeding. See [Changing the SVG1202 Default Password](#) for more information.**

**For security reasons, DO NOT configure your SVG1202 Wireless Voice Gateway over a wireless network connection.**

After installing the gateway, you are now ready to connect your computer and other network devices to the Internet. To do this, you may have to enable the network options on your computer to automatically obtain an IP address and DNS server address. Follow the steps in this section for your operating system.

**Note:** Your computer may already be configured to automatically connect to the Internet. If so, **do not** perform any of the steps in this section.

### Configuring TCP/IP for Windows 7

1. Click **Start** and then select **Network, Properties**.
2. Click **Network and Internet** to open the Network and Internet window.
3. Click **Network and Sharing Center** to open the Network and Sharing Center window.
4. Click **Change adapter settings** to open the Network Connections window.
5. Right-click the network connection for your network interface.
6. Select *Properties* to open the Local Area Connection Properties window.
7. Select *Internet Protocol Version 4 (TCP/IPv4)* and click **Properties** to open the Internet Protocol Properties window.
8. Select *Obtain an IP address automatically* and *Obtain DNS server address automatically*.
9. Click **OK** to save the TCP/IP settings and close the Internet Protocol Version 4 (TCP/IPv4) Properties window.
10. Click **Close** to close the Local Area Connection Properties window.
11. Close the remaining windows and exit the Control Panel.
12. When you complete the TCP/IP configuration, verify the IP address. See [Verifying the IP Address in Windows 7](#) for more information.

### Configuring TCP/IP for Windows Vista

1. Click **Start** and then right-click **Network**.
2. Click **Network and Internet** to open the Network and Internet window.
3. Click **Network and Sharing Center** to open the Network and Sharing Center window.
4. Click **Manage Network Connections**.
5. Right-click on the Local Area Connection you want to configure (if more than one is listed).
6. Click **Properties** to open the Connection Properties window.
7. Click **Continue**, if prompted for administrator permission.
8. Click **Networking** tab.





9. Select *Internet Protocol Version4 (TCP/IPv4)* and then click **Properties**.
10. Verify that the **Obtain an IP address automatically** and **Obtain DNS server address automatically** options are both selected.
11. Click **Advanced**. Use the following table to verify the Advanced TCP/IP Settings:

IP SETTINGS TAB	DNS TAB	WINS TAB
DHCP Enabled listed IP address box	DNS server addresses box is empty	WINS addresses box is empty
Default gateways box is empty	Append primary and connection specific DNS suffixes is selected	Enable LMHOSTS lookup is checked
Automatic metric is selected	Append parent suffixes of the primary DNS suffix is checked	Default: Use NetBIOS setting from the DHCP server is selected
	Register this connection's addresses in DNS is checked	
	Append these DNS suffixes (in order) is not selected	

12. Click **OK**.
13. Click **Alternate Configuration** and verify that *Automatic private IP address* is selected.
14. Click **OK**. A prompt to restart your computer will display.

## Configuring TCP/IP for Windows XP

1. Click **Start** and then select **Settings** and **Control Panel**.
2. Click **Network and Internet Connections** or **Network Connections** (will vary according to settings).
3. Click **Local Area Connection**.
4. Click **Properties** to open the Local Area Connection Properties window.
5. Verify *Internet Protocol (TCP/IP)* is selected, then click **Properties**.
6. Verify that *Obtain an IP address automatically* and *Obtain DNS server address automatically* are both selected.
7. Click **OK** to save the TCP/IP settings.
8. Click **OK** to exit.
9. When you complete the TCP/IP configuration, verify the IP address. See [Verifying the IP Address in Windows XP](#) for more information.

## Renewing the IP Address in Windows 7 or Vista

1. Click **Start** and then click **Start Search**.
  2. Type **cmd** and then right-click **cmd.exe** from the drop-down list.
  3. Select *Run as administrator*.
  4. Type **ipconfig /renew** and press **Enter**. A new IP address for your computer will display.
  5. Type **exit** and press **Enter** to return to Windows.
- If you still cannot access the Internet, contact your Internet Service Provider.



---

## Renewing the IP Address in Windows XP

1. Click **Start** and then click **Run**.
2. Type **cmd** and click **OK** to open a command prompt window.
3. Type **ipconfig /renew** and press **Enter**. A new IP address for your computer will display.
4. Type **exit** and press **Enter** to return to Windows.

If you still cannot access the Internet, contact your Internet Service Provider.

## Verifying the IP Address in Windows 7 or Vista

1. Click **Start** and then click **All Programs**.
2. Click **Accessories**.
3. Click **Run** to open the Run window.
4. Type **cmd** and click **OK** to open a command prompt window.
5. Type **ipconfig** and press **Enter** to display the IP Configuration.

## Verifying the IP Address in Windows XP

1. Click **Start** and then click **Run**.
2. Type **cmd** and click **OK**.
3. Type **ipconfig** and press **Enter** to display your IP configuration.

## Setting Up a Wi-Fi Network Connection

Do the following to set up a Wi-Fi network connection using the WPS button on the SVG1202 Wireless Voice Gateway:

1. Power ON the gateway.
2. Power ON the WPS-enabled devices you want to have access to the network, such as a computer, router, or telephone.

The Wi-Fi network will automatically detect the WPS devices.

3. Press **WPS** button on the gateway.
4. If applicable, press **WPS** button on the other WPS devices.



# 5

## Monitoring Your Gateway

Use the SVG1202 Gateway Configuration Manager to change various default configuration settings on the gateway.

**Note:** If the gateway was obtained as part of a service package, your service provider may require alternative configuration methods. If you cannot access any of the HTML pages in the Configuration Manager, please contact your service provider for assistance.

### Starting the Gateway Configuration Manager

1. Open any web browser on a computer connected to the gateway.
2. In the Address bar, type **http://192.168.0.1** for the Gateway Configuration Manager IP address, and then press **Enter**. The gateway Login screen displays.
3. Type the default username and password. Both entries are case-sensitive.  
Username: **admin**  
Password: **motorola**

**Login**

**Login**  
Please enter username and password to login.

Username:

Password:

4. Click **Login** to open the SVG1202 Configuration Manager (CMGR).  
The following SVG1202 Status page displays:

**Status**

Connection [help](#)  
This page displays information on the status of the cable modem's HFC and IP network connectivity.

Startup Procedure		
Procedure	Status	Comment
Acquire Downstream Channel	In Progress	In Progress
Connectivity State	In Progress	Not Synchronized
Boot State	In Progress	Unknown
Security	Disabled	Disabled

Downstream Channel			
Lock Status	In Progress	Modulation	unknown
Channel ID	0	Symbol rate	Unknown
Downstream Frequency	623750000 Hz	Downstream Power	-0.1 dBmV
SNR	0.0 dB		

Upstream Channel			
Lock Status	Not Locked	Modulation	QPSK
Channel ID		Symbol rate	0 Ksym/sec
Upstream Frequency		Upstream Power	9.4 dBmV

Current System Time: -----

**Note:** If you cannot access the HTML pages in the Gateway Configuration Manager, please contact your service provider for assistance.



## SVG1202 Menu Options Bar

The SVG1202 Menu Options bar is displayed at the top of the SVG1202 Configuration Manager window.



### Configuration Manager Menu Options Bar

MENU OPTIONS	FUNCTION
<b>Status</b>	Provides information about the gateway hardware and software, MAC address, voice gateway IP address, serial number, and related information. Additional pages provide diagnostic tools and allow you to change your gateway user name and password.
<b>Basic</b>	Views and configures the gateway IP-related configuration data, including Network Configuration, WAN Connection Type, DHCP, and DDNS
<b>Advanced</b>	Configures and monitors how the gateway routes IP traffic
<b>Firewall</b>	Configures and monitors the gateway firewall
<b>Parental Control</b>	Configures and monitors the gateway Parental Control features
<b>Wireless</b>	Configures and monitors the gateway wireless networking features
<b>MTA</b>	Monitors the telephone features of the gateway
<b>Logout</b>	Closes the SVG1202 Configuration Manager



## Changing the SVG1202 Default Password



To prevent unauthorized configuration, immediately change the default password when you first configure the gateway.

1. From the Status Security page, click **Security** from the Status menu options.

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. Complete each field entry, but note the following:
  - Password Change Username is your new user name.
  - New Password is case sensitive.
  - Current Username Password is your old password.
3. Select **No** for Restore Factory Defaults.
4. Click **Apply** to update the user name and password.

## Restoring Factory Defaults

**Note:** After applying the restore factory settings change, you will have to log in using the default user name and password.

Under Restore Factory Defaults, select **Yes**.

1. Click **Apply** to reset the user name and password to the original factory settings.
2. Log in again using the following defaults. Note that both entries are case-sensitive.

User name: **admin**

Password: **motorola**

## Getting Help

To retrieve help information for any menu option, click **help** on that page.

## Exiting the SVG1202 Configuration Manager

To log off and close the SVG1202 Configuration Manager:

- Click **Logout** on the SVG1202 Menu Options bar.



# 6

## Status Pages

Use the SVG1202 Status pages to get information about the gateway hardware and software, MAC address, gateway IP address, serial number; and to monitor the gateway system connection, access additional diagnostic tools, and change your gateway user name and password.

### Status Software Page

Displays status information for the gateway software.

Information	
Standard Specification Compliant	DOCSIS 2.0
Hardware Version	1
Software Version	SVG1202-2.1.0.0-GA-07-LTSH
Cable Modem MAC Address	00:23:ed:ac:03:5c
Cable Modem Serial Number	361399116500018101010000
CM certificate	Installed
Status	
System Up Time	0 days 02h:13m:20s
Network Access	Denied
Cable Modem IP Address	-----

### Status Connection Page

Check the HFC and IP network connectivity status of the gateway.

- Click **Refresh** in your web browser to refresh this information.

The screenshot shows the Motorola web interface for the Status Connection page. The navigation menu includes Status, Basic, Advanced, Firewall, Parental Control, Wireless, MTA, and Logout. The main content area is titled 'Status' and includes a 'Connection help' link. A descriptive text states: 'This page displays information on the status of the cable modem's HFC and IP network connectivity.' Below this, there are three tables: 'Startup Procedure', 'Downstream Channel', and 'Upstream Channel'. At the bottom, it shows 'Current System Time: -----'.

Startup Procedure		
Procedure	Status	Comment
Acquire Downstream Channel	In Progress	In Progress
Connectivity State	In Progress	Not Synchronized
Boot State	In Progress	Unknown
Security	Disabled	Disabled

Downstream Channel			
Lock Status	In Progress	Modulation	unknown
Channel ID	0	Symbol rate	Unknown
Downstream Frequency	823750000 Hz	Downstream Power	-0.1 dBmV
SNR	0.0 dB		

Upstream Channel			
Lock Status	Not Locked	Modulation	QPSK
Channel ID		Symbol rate	0 Ksym/sec
Upstream Frequency		Upstream Power	9.4 dBmV

Current System Time: -----



## Status Security Page

Define administrator access privileges by changing your gateway user name and password, and reset your user name and password to the default setting. See [Changing the SVG1202 Default Password](#) and [Restoring Factory Defaults](#) for more information.

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"/>	

## Status Diagnostics Page

Use the following diagnostic tools to troubleshoot IP connectivity problems:

- Ping LAN
- Ping WAN
- Traceroute (WAN)

## Ping Utility

Use Ping (Packet InterNet Groper) to check connectivity between the gateway and other devices on the gateway LAN by sending a small packet of data and then waiting for a reply. A Ping reply confirms that the computer is connected to the gateway.

Select Utility	
Ping LAN	<input type="button" value="v"/>
Ping Test Parameters	
Target	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="0"/> <input type="text" value="1"/>
Ping Size	<input type="text" value="64"/> bytes
No. of Pings	<input type="text" value="3"/>
Ping Interval	<input type="text" value="1000"/> ms
<input type="button" value="Start Test"/> <input type="button" value="Abort Test"/> <input type="button" value="Clear Results"/>	
Results	
Pinging 192.168.0.1 with 64 bytes of data:[Complete] Reply from 192.168.0.1: bytes = 64, time = 0 ms Reply from 192.168.0.1: bytes = 64, time = 0 ms Reply from 192.168.0.1: bytes = 64, time = 0 ms 3/3 replies received. min time=0 ms, max time=10 ms, avg time=0 ms	



## Testing Network Connectivity with the SVG1202

Perform the following test to check connectivity between the gateway and other devices on the SVG1202 LAN:

1. Select **Ping LAN** 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.
9. When done, click **Clear Results** to delete the Ping results in the Results pane.

## Traceroute Utility

Use Traceroute to map the network path from the SVG1202 Configuration Manager to a public host.

Select Utility	
Traceroute	

Traceroute Parameters	
Target	<input type="text"/> IP address or Name
Max Hops	<input type="text" value="255"/>
Data Size	<input type="text" value="32"/> bytes
Base Port	<input type="text" value="33434"/>
Resolve Host	<input type="text" value="Off"/>

Results
Waiting for input...

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





## Status Event Log Page

Review critical system events in chronological order in the SNMP Event log.

Time	Priority	Description
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/QPSK symbol timing
Time Not Established	Notice (6)	Ethernet link up - ready to pass packets
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/QPSK symbol timing
Time Not Established	Notice (6)	Ethernet link down - not ready to pass packets
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/QPSK symbol timing

Clear Log

## Status Configuration Page

Reboot the gateway after making any configuration changes.

Downstream Frequency (Hz)	<input type="text" value="579000000"/>
Upstream Channel Id	<input type="text" value="1"/>
Downstream Frequency Plan	<input type="text" value="North America"/>
<input type="button" value="Save Changes"/> <input type="button" value="Reboot"/>	



# 7

## Basic Pages

View and configure SVG1202 IP-related configuration data, including Network Configuration, WAN Connection Type, DHCP, and DDNS in Basic Pages. The Backup option allows you to save a copy of the SVG1202 configuration on your computer.

### Basic Setup Page

Configure the basic features of the SVG1202 gateway related to your service provider's connection.

**Primary Mode**  
**NAPT mode** Enabled  
 Changes may require a reboot to take effect.  
 Apply

**Network Configuration**

<b>LAN</b>	<b>IP Address</b>	192 . 168 . 0 . 1
	<b>MAC Address</b>	00 23:ed:ac:7b:22
<b>WAN</b>	<b>IP Address</b>	---:---:---
	<b>MAC Address</b>	00 23:ee:da:93:17
	<b>Duration</b>	D: -- H: -- M: -- S: --
	<b>Expires</b>	---:---:---:---

Release WAN Lease Renew WAN Lease

**WAN Connection Type** DHCP  
**MTU Size** 0 (256-1500 octets. 0 = use default)  
**Spoofed MAC Address** 00 : 00 : 00 : 00 : 00 : 00  
 Changes may require a reboot to take effect.  
 Apply

#### Field Descriptions for the Basic Setup Page

FIELD	DESCRIPTION
<b>NAPT mode</b>	NAPT is a special case of NAT, where many IP numbers are hidden behind a number of addresses. In contrast to the original NAT, however, this does not mean there can be only that number of connections at a time. In NAPT mode, an almost arbitrary number of connections are multiplexed using TCP port information. The number of simultaneous connections is limited by the number of addresses multiplied by the number of available TCP ports.
<b>LAN</b>	
<b>IP Address</b>	Enter the IP address of the SVG1202 on your private LAN.
<b>MAC Address</b>	Media Access Control address — a set of 12 hexadecimal digits assigned during manufacturing that uniquely identifies the hardware address of the SVG1202 Access Point.
<b>WAN</b>	
<b>IP Address</b>	The public WAN IP address of your SVG1202 device, which is either dynamically or statically assigned by your ISP.
<b>MAC Address</b>	Media Access Control address — a set of 12 hexadecimal digits assigned during manufacturing that uniquely identifies the hardware address of the SVG1202 Access Point.




FIELD	DESCRIPTION
<b>WAN (continued)</b>	
<b>Duration</b>	Describes how long before your Internet connection expires. The WAN lease will automatically renew itself when it expires.
<b>Expires</b>	Displays the exact time and date the WAN lease expires.
<b>Release WAN Lease</b>	Click to release WAN lease.
<b>Renew WAN Lease</b>	Click to renew WAN lease.
<b>WAN Connection Type</b>	DHCP or Static IP. If your ISP uses DHCP, select <b>DHCP</b> and enter a Host Name and Domain name, if required. If your ISP uses static IP addressing, select <b>Static IP</b> and enter the information provided by your ISP for Static IP Address, Static IP Mask, Default Gateway, Primary DNS, and Secondary DNS.
<b>MTU Size</b>	Maximum Transmission Unit (MTU) is the largest size packet or frame that can be sent. The default value is suitable for most users.
<b>Spoofed MAC Address</b>	If WAN Connection Type is Static IP, enter the information provided by your ISP for Static IP Address, Static IP Mask, Default Gateway, Primary DNS, and Secondary DNS.

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

## Basic DHCP Page

Configure and view the status of the optional internal SVG1202 DHCP (Dynamic Host Configuration Protocol) server for the LAN.



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

**DHCP**

<b>DHCP Server</b>	<input checked="" type="radio"/> Yes <input type="radio"/> No	
<b>Starting Local Address</b>	192.168.0.2	
<b>Number of CPEs</b>	253	
<b>Lease Time</b>	3600	

**DHCP Clients**

**Reserve new IP address**

MAC address <small>(e.g. 11:22:33:aa:bb:cc)</small>	IP Address	Host name
<input type="text"/>	192.168.0.	<input type="text"/>
<input type="button" value="Add"/>		

MAC Address	IP Address	Subnet Mask	Duration	Expires	Select
00:1b:38:bf:df:08	192.168.0.003	255.255.255.000	D:00	-----	<input type="radio"/>
			H:01	-----	
			M:00	-----	
			S:00	-----	

**Current System Time:**-----



### Field Descriptions for the Basic DHCP Page

FIELD	DESCRIPTION
<b>DHCP Server</b>	Select <b>Yes</b> to enable the SVG1202 DHCP Server. Select <b>No</b> to disable the SVG1202 DHCP Server.
<b>Starting Local Address</b>	Enter the starting IP address to be assigned by the SVG1202 DHCP server to clients in dotted-decimal format. The default is <b>192.168.0.2</b> .
<b>Number of CPEs</b>	Sets the number of clients for the SVG1202 DHCP server to assign a private IP address. There are 245 possible client addresses. The default is <b>245</b> .
<b>Lease Time</b>	Sets the time in seconds that the SVG1202 DHCP server leases an IP address to a client. The default is <b>3600</b> seconds (60 minutes).
<b>DHCP Clients</b>	Lists the DHCP client device information.

Click **Apply** to save your changes.

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

## Basic DDNS Page

Set up the Dynamic Domain Name System (DDNS) service to assign a static Internet domain name to a dynamic IP address. This allows the gateway to be easily accessed from various Internet locations.

### Field Descriptions for Basic DDNS Page

FIELD	DESCRIPTION
<b>DDNS Service</b>	Select <b>Disable</b> or <b>wwwDynDNS.org</b> to enable the DDNS Service
<b>User Name</b>	Enter your DynDNS user name
<b>Password</b>	Enter your DynDNS Password
<b>Host Name</b>	Enter your DDNS Host Name
<b>IP Address</b>	Lists IP information
<b>Status</b>	Shows <b>Enabled</b> or <b>Disabled</b> for the DDNS service status



## Basic Backup Page

Save your current SVG1202 configuration settings locally on your computer or restore previously saved configurations.

The screenshot shows a web interface titled "Backup/Restore". It contains a text input field for a file path, a "Browse..." button to the right of the input field, a "Restore" button to the right of the "Browse..." button, and a "Backup" button centered below the "Restore" button.

## Restoring Your SVG1202 Configuration

1. Type the path and file name of the backup file located on your computer, or click **Browse** to locate the file.
2. Click **Restore** to recreate your previously saved SVG1202 settings.

## Backing Up Your SVG1202 Configuration

1. Type the path and file name where you want to store the backup file on your computer, or click **Browse** to locate the file.
2. Click **Backup** to create a backup of your SVG1202 settings.



# 8

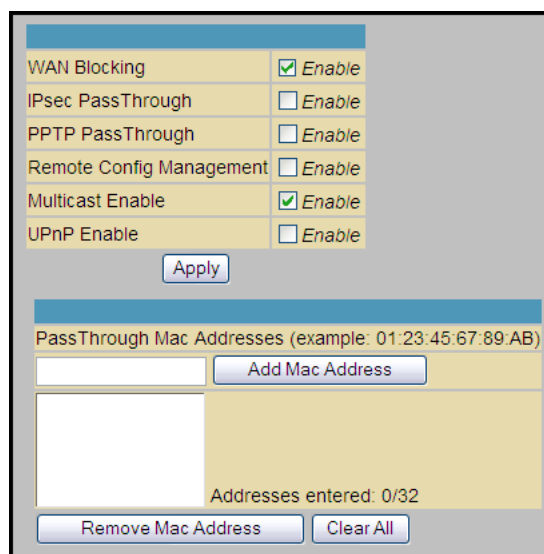
## Advanced Pages

Configure IP Filtering, MAC Filtering, Port Filtering, Port Forwarding, Port Triggers, DMZ Host, and Routing Information Protocol (RIP) Setup.

Click any Advanced submenu option to view or change the advanced configuration information for it.

### Advanced Options Page

Set the operating modes for adjusting how the SVG1202 device routes IP traffic.



#### Field Descriptions for the Advanced Options Page

FIELD	DESCRIPTION
<b>WAN Blocking</b>	Prevents the SVG1202 Configuration Manager or the computers behind it from being visible to other computers on the SVG1202 WAN.  Select <b>Enable</b> to turn on.
<b>IPsec PassThrough</b>	Enables the IPsec Pass-Through protocol to be used through the SVG1202 Configuration Manager so that a VPN device (or software) may communicate properly with the WAN.  Select <b>Enable</b> to turn on.
<b>PPTP PassThrough</b>	Enables the Point-to-Point Tunneling Protocol (PPTP) Pass-Through protocol to be used through the SVG1202 Configuration Manager so that a VPN device (or software) may communicate properly with the WAN.  Select <b>Enable</b> to turn on.



FIELD	DESCRIPTION
<b>Remote Config Management</b>	<p>Allows remote access to the SVG1202 Configuration Manager. This enables you to configure the SVG1202 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 <b>http://WanIPAddress:8080/</b> to access the SVG1202 Configuration Manager remotely.</p> <p>Select <b>Enable</b> to turn on.</p>
<b>Multicast Enable</b>	<p>Allows multicast-specific traffic (denoted by a multicast specific address) to be passed to and from the computers on the private network behind the configuration manager.</p> <p>Select <b>Enable</b> to turn on.</p>
<b>UPnP Enable</b>	<p>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.</p> <p>Select <b>Enable</b> to turn on.</p>
<b>PassThrough Mac Addresses</b>	<p>Specifies up to 32 computers as passthrough clients not subject to NAT, using their MAC addresses.</p> <p>To enable this feature, your cable operator may need to provide additional public IP addresses.</p>

Click **Apply** to save changes.



## Advanced IP Filtering Page

Define which local computers will be denied access to the SVG1202 WAN by configuring IP address filters to block Internet traffic to specific network devices on the LAN. You enter the LSB (Least-significant byte) of the IP address; the upper bytes of the IP address are set automatically from the SVG1202 Configuration Manager's IP address.

You can 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"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>

### Field Descriptions for the Advanced IP Filtering Page

FIELD	DESCRIPTION
<b>Start Address</b>	Enter the starting IP address range of the computers you want to deny access to the SVG1202 WAN. Enter only the least significant byte of the IP address.
<b>End Address</b>	Enter the ending IP address range of the computers you want to deny access to the SVG1202 WAN. Enter only the least significant byte of the IP address.
<b>Enabled</b>	Activate the IP address filter. Select each range of IP addresses you want to deny access to the SVG1202 WAN.

Click **Apply** to activate and save your settings.





## Advanced MAC Filtering Page

Define up to 20 Media Access Control (MAC) address filters to prevent computers from sending outgoing TCP/UDP traffic to the WAN via their MAC addresses. 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 Addresses (example: 01:23:45:67:89:AB)

Add MAC Address

Addresses entered: 0/20

Remove MAC Address Clear All

### Field Descriptions for the Advanced MAC Filtering Page

FIELD	DESCRIPTION
<b>MAC Addresses</b>	Media Access Control address — a unique set of 12 hexadecimal digits assigned to a computer during manufacturing.

## Setting a MAC Address Filter

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



## Advanced Port Filtering Page

Define port filters to prevent all devices from sending outgoing TCP/UDP traffic to the WAN on specific IP port numbers. Specify a starting and ending port range to determine what TCP/UDP traffic is allowed out to the WAN on a per port basis.

**Note:** The specified port ranges are blocked for ALL computers. This setting is not IP address or MAC address specific. For example, to block all computers on the private LAN from accessing HTTP sites, enter the following:

- Start Port: **80**
- End Port: **80**
- Protocol: **TCP**
- Checkmark: **Enabled**
- 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"/>

### Field Descriptions for the Advanced Port Filtering Page

FIELD	DESCRIPTION
<b>Start Port</b>	Enter the starting port number
<b>End Port</b>	Enter the ending port number
<b>Protocol</b>	Select <b>TCP</b> , <b>UDP</b> , or <b>Both</b> from the drop-down list
<b>Enabled</b>	Checkmark to activate the IP port filters



## Advanced Port Forwarding Page

Run a publicly accessible server on the LAN by specifying the mapping of TCP/UDP ports to a local computer. This enables incoming requests on specific port numbers to reach web servers, FTP servers, mail servers, etc. so that they can be accessible from the 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"/>

Commonly used Port numbers:

Application	Port
HTTP	80
FTP	21
TFTP	69
SMTP	25
POP3	110
NNTP	119
Telnet	23
IRC	194
SNMP	161
Finger	79
Gopher	70
Whois	43
rtelnet	107
LDAP	389
UUCP	540

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



## Advanced Port Triggers Page

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 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 or bi-directional data. If no outgoing traffic is detected on the "Trigger Range" ports for 10 minutes, the "Target Range" ports 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		
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>

### Field Descriptions for the Advanced Port Triggers Page

FIELD	DESCRIPTION
<b>Trigger Range</b> <b>Start Port</b> <b>End Port</b>	Starting port number of the Port Trigger range Ending port number of the Port Trigger range
<b>Target Range</b> <b>Start Port</b> <b>End Port</b>	Starting port number of the Port Trigger range Ending port number of the Port Trigger range
<b>Protocol</b>	Select <b>TCP</b> , <b>UDP</b> , or <b>Both</b> from the drop-down list
<b>Enable</b>	Select checkbox to activate the IP port triggers



## Advanced DMZ Host Page

Specify the default recipient of WAN traffic that NAT is unable to translate to a known local computer. The DMZ (De-militarized Zone) is a computer or small subnetwork located outside the firewall, between the trusted internal private LAN and the untrusted public Internet, that 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 is also 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.

The image shows a configuration window with a blue header bar. Below the header, there is a yellow box containing the text "DMZ Address" followed by a text input field containing the IP address "192.168.0.0". Below the input field is a grey button labeled "Apply".

You can configure one computer to be the DMZ host. This setting is generally used for computers using problem applications that use random port numbers and do not function correctly with specific port triggers or the port forwarding setups. If you set up a computer as a DMZ Host, set this back to zero when you are finished with the needed application, since this computer 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 IP address for the computer.
2. Click **Apply** to activate the selected computer as the DMZ host.



# 9

## Firewall Pages

Use the Firewall Pages to configure the firewall filters and firewall alert notifications. The firewall protects the SVG1202 LAN from undesired attacks and other intrusions from the Internet. 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.

### Firewall Web Content Filter Page

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.

You can block Java Applets, Cookies, ActiveX controls, popup windows, and Proxies. Firewall Protection turns on the Stateful Packet Inspection (SPI) firewall features.

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 type="checkbox"/> Enable
Port Scan Detection	<input type="checkbox"/> Enable
IP Flood Detection	<input checked="" type="checkbox"/> Enable
Firewall Protection	Medium

Allowed Services			
RADIUS	1812	1812	UDP
SMTP	25	25	TCP
SSH	22	22	TCP
SMTP-S	465	465	TCP
Steam	1725	1725	UDP
Steam Friends	1200	1200	UDP
Telnet-S	992	992	TCP
XBOX Live	3074	3074	TCP
XBOX Live	3074	3074	UDP
World of Warcraft	3724	3724	TCP
World of Warcraft	3724	3724	UDP
Yahoo Messenger	5050	5050	TCP

Select each Web filter you want to set for the firewall and then click **Apply**. The Web filters will activate without having to reboot the SVG1202 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

Set up notification of the firewall event log in either of the following formats:

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

## Firewall Remote Log Page

Send firewall attack reports to a standard SysLog server so multiple instances can be logged over a period of time. Select individual attack or configuration items to send to the SysLog server so that only the items of interest will be monitored. You can log permitted connections, blocked connections, known Internet attack types, and CMRG configuration events. The SysLog server must be on the same network as the Private LAN behind the Configuration Manager (typically **192.168.0.x**).

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

**Field Description for the Firewall Remote Log Page**

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



# 10

## Parental Control Pages

Use Parental Control Pages to configure access restrictions to a specific device connected to the SVG1202 LAN.

### Parental Control User Setup Page

Link each user to a specified time-access rule, content filtering rule, and login. You may also specify a user as a “trusted user” who will have access to all Internet content regardless of the filters. You can use the Trusted User checkbox as an override to grant a user full access, while storing all of the filtering settings for easy availability.

You can enable Internet session duration timers, which limit the amount of time for Internet access. Users must enter their passwords the first time to access the Internet, but not each time a new web page is accessed. You can also set the inactivity timer so that if there is no Internet access for a specified time, the user must login again.

Field Descriptions for the Parental Control User Setup Page

FIELD	DESCRIPTION
<b>Add User Button</b>	Add a user to set parental controls for a specific user.
<b>User Settings</b>	Select the user for whom you want to modify access restrictions. Select <b>Enable</b> to select the user. Click <b>Remove User</b> to delete the user from Parental Controls.
<b>Password</b>	Enter a user password to log onto the Internet.





FIELD	DESCRIPTION
<b>Re-Enter Password</b>	Enter the password again for confirmation.
<b>Trusted User</b>	Select users who will have full access to Internet content. Select <b>Enable</b> to override set filters without having to turn off filter settings.
<b>Content Rule</b>	Specify which websites each user is allowed to access. Select <b>White List Access Only</b> , then choose a user from the drop-down list.
<b>Time Access Rule</b>	Set a rule to restrict when a selected user can use the Internet.
<b>Session Duration</b>	Set the amount of time a selected user can use the Internet.
<b>Inactivity time</b>	Set the amount of inactivity time before the Internet automatically closes for a selected user.
<b>Trusted Computers</b>	Enter a user's CPE MAC address so that CPE can access the Internet without being censored by the Parental Control. When done, click <b>Add</b> .

Click **Apply** to activate and save any changes you made.

## Parental Control Basic Setup Page

Set rules to block types 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**

1. Default Add New Policy Remove Policy

Keyword List Blocked Domain List Allowed Domain List

anonymizer anonymizer.com

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

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



## Parental Control Time of Day Filter Page

Block all Internet traffic to and from specified devices on your SVG1202 network based on day and time settings. You can block Internet traffic for the entire day or for certain times within each day for specific users. You can add up to 30 categories (filter names) with different day and time settings. You enter a name for each time filter in the **Add New Policy** field.

Apply time filters for limited Internet access 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)

After creating each new time of day policy, click **Apply** to store and activate the settings. The same category names for blocking profiles appear in the Parental Control User Setup page under the "Time Access Rule" section where each user can be assigned up to four categories simultaneously.

## Parental Control Local Log Page

Generate an event log that shows a running list of the last 30 Parental Control access violations, including:

- 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"/>				



# 11

## Wireless Pages

To configure your wireless LAN (WLAN), click any Wireless submenu option to view or change the configuration information for that option. WPA or WPA2 encryption provides higher security than WEP encryption, but older wireless client cards may not support the newer WPA or WPA2 encryption methods.

### Wireless 802.11 Radio Page

Configure the Wireless Radio parameters, including the current country and channel number.

Wireless Interfaces:	Motorola (00:23:ED:AC:7B:23)
Wireless	Enabled
Country	UNITED STATES
Output Power	100%
802.11 Band	2.4 GHz
802.11 n-mode	Auto
Bandwidth	20 MHz
Sideband for Control Channel (40 MHz only)	None
Control Channel	Auto Current : 1

Apply Restore Wireless Defaults

#### Field Descriptions for the Wireless 802.11 Radio Page

FIELD	DESCRIPTION
<b>Wireless Interfaces</b>	Shows the MAC address of the installed wireless card. It is not configurable.
<b>Wireless</b>	Shows if the wireless network is enabled or disabled.
<b>Country</b>	Restricts the channel set based on the country's regulatory requirements. This is a display-only field.
<b>Output Power</b>	Sets a percentage of the output power of the hardware's maximum capability.
<b>Channel</b>	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 channel selected on the gateway.



## Wireless 802.11 Primary Network Page

Configure your primary wireless network.

### Field Descriptions for the Wireless 802.11 Primary Network Page

FIELD	DESCRIPTION
<b>Primary Network</b>	When <b>Enabled</b> , transmits beacon frames with the Primary Network SSID.
<b>Network Name (SSID)</b>	Sets the Network Name (SSID) of the Primary wireless network using a 1-32 ASCII character string.
<b>Closed Network</b>	In a closed network, users type the SSID into the client application instead of selecting the SSID from a list.
<b>WPA</b>	Enables or disables Wi-Fi Protected Access encryption.
<b>WPA-PSK</b>	Enables or disables a local WPA pre-shared key passphrase.
<b>WPA2</b>	Enables or disables Wi-Fi Protected Access 2 encryption.
<b>WPA2-PSK</b>	Enables or disables a local WPA2 pre-shared key passphrase.
<b>WPA/WPA2 Encryption</b>	Sets encryption mode to: TKIP, AES, or TKIP + AES. AES.



FIELD	DESCRIPTION
<b>WPA Pre-Shared Key</b> <b>Show Key</b>	Sets the WPA Pre-Shared Key (PSK); either an 8-63 ASCII character string or a 64-digit hex number. This is specified when the Network Authentication method is WPA-PSK. <b>Show Key</b> - displays the WPA Pre-Shared Key.
<b>RADIUS Server</b>	Sets the RADIUS server IP address to use for client authentication using the dotted-decimal format (xxx.xxx.xxx.xxx).
<b>RADIUS Port</b>	Sets the UDP port number of the RADIUS server; default is 1812.
<b>RADIUS Key</b>	Sets the shared secret for the RADIUS connection; key is a 0 to 255 character ASCII string.
<b>Group Key Rotation Interval</b>	Sets the WPA Group Rekey Interval in seconds. Set to zero to disable periodic rekeying.
<b>WPA/WPA2 Re-auth Interval</b>	Sets the amount of time the wireless router can wait before re-establishing authentication with the CPE.
<b>WEP Encryption</b>	Enables or disables Wired Equivalent Privacy encryption.
<b>Shared Key Authentication</b>	Sends an authentication request to the access point. Then the access point sends a challenge text to the CPE. The CPE encrypts challenge text which it sends to the access point. The access point decrypts and compares the message with the original challenge text. If they are the same, the access point lets the CPE connect; if it does not match, the access point does not let the CPE connect.
<b>802.1x Authentication</b>	Uses a stronger authentication than WEP.
<b>Network Key 1 – 4</b>	<b>Sets the static WEP keys when WEP encryption is enabled.</b> <b>Enter five ASCII characters or 10 hexadecimal digits for a 64-bit key.</b> <b>Enter 13 ASCII characters or 26 hexadecimal digits for a 128-bit key.</b> When both WPA encryption and WEP encryption are enabled, only keys 2 and 3 are available for WEP encryption.
<b>Current Network Key</b>	Selects the encryption (transmit) key when WEP encryption is enabled.
<b>PassPhrase</b>	Sets the text to use for WEP key generation.



## Wireless 802.11 Advanced Page

Configure data rates and Wi-Fi thresholds.

54g™ Mode	54g Auto
Basic Rate Set	Default
54g™ Protection	Auto
XPress™ Technology	Disabled
Afterburner™ Technology	Disabled
Rate	Auto
Beacon Interval	100
DTIM Interval	1
Fragmentation Threshold	2346
RTS Threshold	2347
NPHY Rate	Auto
802.11n Protection	Auto
Multicast Rate	Auto
<input type="button" value="Apply"/>	

### Field Descriptions for the Wireless 802.11 Advanced Page

FIELD	DESCRIPTION
<b>54g™ Mode</b>	Sets these network modes: <b>54g Auto</b> , <b>54g Performance</b> , <b>54g LRS</b> , and <b>802.11b</b> 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. 802.11b accepts only 802.11b clients.
<b>Basic Rate Set</b>	Determines which rates are advertised as basic rates. Default uses the driver defaults. <b>All</b> sets all available rates as basic rates.
<b>54g™ Protection</b>	Improves performance in Auto mode using RTS/CTS protection in mixed 802.11g + 802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.
<b>XPress™ Technology</b>	Enhances Wi-Fi throughput and efficiency used when there are mixed wireless networks in the surrounding area from 802.11a/b/g networks.
<b>Afterburner™ Technology</b>	Enhances Wi-Fi 802.11g standard by increasing throughput by 40 percent.
<b>Rate</b>	Forces the transmission rate for the AP to a particular speed. "Auto" provides best performance in nearly all situations.
<b>Beacon Interval</b>	Sets the beacon interval for the AP. The default is <b>100</b> , which is fine for nearly all applications.



FIELD	DESCRIPTION
<b>DTIM Interval</b>	Sets the wakeup interval for clients in Power Save mode. When a client is running in Power Save mode, lower SVG1202 bin values provide higher performance but result in decreased client battery life; higher values provide lower performance but increased client battery life.
<b>Fragmentation Threshold</b>	Sets the fragmentation threshold. Packets exceeding this threshold are fragmented into packets smaller than the threshold before packet transmission.
<b>RTS Threshold</b>	Sets the RTS threshold. Packets exceeding this threshold cause the AP to perform an RTS/CTS exchange to reserve the wireless medium before packet transmission.

## Wireless 802.11 Access Control Page

Configure the Access Control to the AP and status on the connected clients.

### Field Descriptions for the Wireless 802.11 Access Control Page

FIELD	DESCRIPTION
<b>Wireless Interface</b>	Shows the MAC address of the installed wireless card. It is not configurable.
<b>MAC Restrict Mode</b>	Selects whether wireless clients with the specified MAC address are allowed or denied wireless access. Select <b>Disabled</b> to allow all clients.
<b>MAC Address</b>	Lists wireless client MAC addresses allowed or denied wireless access 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.
<b>Connected Clients</b>	Lists connected wireless clients. As a client connects or leaves the network, it is added to or removed from the list, Age is the amount of time since data was transmitted to or received from the client.



## Wireless 802.11 Wi-Fi Multimedia Page

Configure the Wi-Fi Multimedia Quality of Service (QoS).

EDCA AP Parameters:						
	CWmin	CWmax	AIFSN	TXOP(b) Limit (usec)	TXOP(a/g) Limit (usec)	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:						
	CWmin	CWmax	AIFSN	TXOP(b) Limit (usec)	TXOP(a/g) Limit (usec)	Discard Oldest First
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	

### Field Descriptions for the Wireless 802.11 Wi-Fi Multimedia Page

FIELD	DESCRIPTION
<b>WMM Support</b>	Sets WMM support to <b>Auto</b> , <b>On</b> or <b>Off</b> . If enabled (Auto or on), WME Information Element is included in beacon frames.
<b>No-Acknowledgement</b>	Sets No-Acknowledgement support <b>On</b> or <b>Off</b> . When <b>On</b> , acknowledgments for data are not transmitted.
<b>Power Save Support</b>	Sets Power Save support <b>On</b> or <b>Off</b> . When <b>On</b> , the AP queues packets for STAs that are in Power Save mode. Queued packets are transmitted when the STA notifies the AP that it has left Power Save mode.
<b>EDCA AP Parameters</b>	Specifies the parameters for traffic transmitted from the AP to the STA in four Access Categories: <b>Best Effort (AC_BE)</b> <b>Background (AC_BK)</b> <b>Video (AC_VI)</b> <b>Voice (AC_VO)</b> Admission control specifies if it is to be enforced for the Access Categories. Discard Oldest First specifies the discard policy for the queues. <b>On</b> discards oldest first; <b>Off</b> discards newest first.
<b>EDCA STA Parameters</b>	Specifies the transmit parameters for traffic transmitted from the STA to the AP in the four Access Categories.





## Wireless 802.11 Bridging Page

Enable wireless bridging.

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

### Field Descriptions for the Wireless 802.11 Bridging Page

FIELD	DESCRIPTION
<b>Wireless Bridging</b>	Enable or disable wireless bridging.
<b>Remote Bridges</b>	Build a table of remote bridge MAC addresses authorized to establish a wireless bridge. You can connect up to four remote bridges. Typically, you must enter your AP's MAC address on the remote bridge.

## Setting Up Your Wireless LAN

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



**Prevent unauthorized eavesdropping or access by enabling wireless security after your WLAN is operational. The default settings provide no wireless security.**

To enable security for your WLAN:

- Encrypt wireless LAN transmissions
- Restrict wireless LAN access to further prevent unauthorized WLAN intrusions using the [Wireless 802.11 Access Control Page](#)



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

Do not attempt to configure the gateway over a wireless connection.

Connect at least one computer to the Ethernet port on the gateway.

Configure each wireless client (station) to access the gateway.

Place wireless components away from windows. This decreases signal strength outside the intended area.



## Encrypting Wireless LAN Transmissions

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

### Encrypting Wireless LAN Transmissions

CONFIGURE ON THE SVG1202	REQUIRED ON EACH WIRELESS CLIENT
<b>If all of your wireless clients support Wi-Fi Protected Access (WPA), Motorola recommends configuring WPA on the gateway</b>	If you use a local pre-shared key (WPA-PSK) passphrase, you must configure the identical passphrase on the gateway and on each wireless client. Home and small-office settings typically use a local passphrase.
<b>Otherwise, configure WEP on the gateway</b>	You must configure the identical WEP key on the gateway and on each wireless client.

Motorola recommends using WPA instead of WEP if all of your wireless clients support WPA encryption. WPA advantages include:

- Stronger encryption and more secure
- Authentication to ensure that only authorized users can log in to your WLAN
- Easier configuration
- Standard algorithm on all compliant products to generate a key from a textual passphrase
- Incorporation into the new IEEE 802.11i wireless networking standard

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

## Installing Wireless Clients

**Note:** Use the SVG1202 Installation CD to set client security. The passcode is located on the gateway label.

For each wireless client computer, follow the instructions supplied with the adapter and the steps below to install the wireless adapter:

1. Insert the CD 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 computer MICA or computer I slot, or connect it to the USB port.
4. Configure the adapter to obtain an IP address automatically.

On a computer 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:

### Configuring Wireless Clients

IF YOU:	YOU NEED TO DO THIS ON EACH CLIENT,:
Configured WPA on the gateway	Configure a Wireless Client for WPA or WPA2
Configured WEP on the gateway	Configure a Wireless Client for WEP
Configured the Wireless Network Name on the gateway	Configure a Wireless Client with the Network Name (SSID)
Configured a MAC Access Control List on the gateway	No client configuration required

## Installing a Wireless Client for WPA

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

- WPA is enabled on the gateway but not on the client
- The client passphrase does not match the SVG1202 PSK Passphrase



**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 gateway, you must configure the same WEP key on each wireless client. The gateway cannot authenticate a client, if:

- Shared Key Authentication is enabled on the gateway, but not on the client
- The client WEP key does not match the SVG1202 WEP key

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



**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 gateway and the proper channel and data rate. If your card requires you to manually start scanning for an access point, follow 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 gateway.



# 12

## MTA Pages

Use the Internet to make telephone calls. The Multimedia Terminal Adapter (MTA) supports basic telephone functions, such as three-way calling, voice mail, and fax transmissions.

### MTA Status Page

Displays the initialization status of the MTA.

Startup Procedure	
Task	Status
Telephony DHCP	Completed
Telephony Security	Disabled
Telephony TFTP	Completed
Telephony Call Server Registration	L1: Operational / L2: Operational
Telephony Registration Complete	Pass With Warnings

MTA Line State	
Line	State
Line 1	On-Hook
Line 2	On-Hook

### MTA DHCP Page

Displays the MTA DHCP lease information.

Lease Parameters	
FQDN	mta001a66080b06.swdev.net
IP Address/Submask	206.19.81.247 / 255.255.255.0
Gateway	206.19.81.1
Bootfile	tftp://sbvprov3.swdev.net/001A66080B06.bin
Primary DNS	198.102.87.133
Secondary DNS	0.0.0.0

Lease Timers	
Lease Time Remaining	D: 00 H: 00 M: 27 S: 58
Rebind Time Remaining	D: 00 H: 00 M: 12 S: 58
Renew Time Remaining	D: 00 H: 00 M: 01 S: 43

PacketCable DHCP Option 122	
SNMP Entity (Sub-option 3)	sbvprov3.swdev.net
Kerberos Realm (Sub-option 6)	
Provisioning Timer (Sub-option 8)	



## MTA QoS Page

Displays the MTA Quality of Service (QoS) parameters.

Error Codewords	
Unerrored Codewords	128653228
Correctable Codewords	0
Uncorrectable Codewords	0

Payload Header Suppression	
PHS Status	ON

Service Flows				
SFID	Service Class Name	Direction	Primary Flow	Packets
3543		Upstream	No	23806
3544		Downstream	No	0
4133		Upstream	No	6
4134		Downstream	No	0



# 13

## Troubleshooting

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

You may have to reset the SVG1202 gateway configuration to its original factory settings if the gateway is not functioning properly.

**Note:** Pressing *RESET* on the rear panel will restore the default settings. You will lose your custom configuration settings, including Parental Control, Firewall and Advanced settings.

### Solutions

**Table 1 – Troubleshooting Solutions**

GATEWAY PROBLEM	POSSIBLE SOLUTION
<b>Power Icon is OFF</b>	<p>Check the cable connections to the gateway and electrical outlet.</p> <p>Check that the electrical outlet is working.</p> <p>Is the outlet controlled by a light switch?</p>
<b>Cannot Send or Receive Data</b>	<p>On the front panel, note the status of the icons and refer to <a href="#">Front Panel Icons and Error Conditions</a> to identify the error.</p> <p>If you have cable television, check your television to ensure your cable service is operating properly.</p> <p>Check the coaxial cable connection at the gateway and cable outlet. Hand tighten, if necessary.</p> <p>Check the IP address. Follow the steps for verifying the IP address for your operating system in <a href="#">Verifying Your IP Address in Windows 7 or Vista</a> or <a href="#">Verifying Your IP Address in Windows XP</a>. Call your service provider if you need an IP address.</p> <p>Check that the Ethernet cable is properly connected to the gateway and the computer.</p> <p>If a device is connected via the Ethernet port, check that the ONLINE icon is ON to verify connectivity.</p> <p>Call your service provider for further assistance.</p>
<b>Wireless client(s) cannot send or receive data</b>	<p>Perform the first four checks in “Cannot send or receive data.”</p> <p>Check the Security Mode setting on the Wireless Primary Network Page:</p> <p>If you enabled WPA and configured a passphrase on the gateway, be sure each affected wireless client has the identical passphrase. If this does not solve the problem, check whether the wireless client supports WPA.</p> <p>If you enabled WEP and configured a key on the gateway, be sure each affected wireless client has the identical WEP key. If this does not solve the problem, check whether the client’s wireless adapter supports the type of WEP key configured on the gateway.</p> <p>To temporarily eliminate the Security Mode as a potential issue, disable security.</p> <p>After resolving your problem, be sure to re-enable wireless security.</p> <p>On the Wireless Access Control Page, be sure the MAC address for each affected wireless client is correctly listed.</p>



## Front Panel LEDs and Error Conditions

The SVG1202 front panel LEDs provide status information for the following error conditions:

**Table 2 – Front Panel LEDs and Error Conditions**

ICON	STATUS	IF, DURING STARTUP	IF, DURING NORMAL OPERATION
<b>POWER</b>	OFF	Gateway is not properly plugged into the electrical outlet	Gateway is unplugged
<b>RECEIVE</b>	FLASHING	Downstream receive channel cannot be acquired	Downstream channel is lost
<b>SEND</b>	FLASHING	Upstream send channel cannot be acquired	Upstream channel is lost
<b>ONLINE</b>	FLASHING	IP registration is unsuccessful	IP registration is lost
<b>LINK</b>	OFF	No connected device is detected	Device is disconnected



## Warranty Information

SURFboard SVG1202 Wireless Voice Gateway  
Motorola Mobility, Inc. ("Motorola")

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

**Cable Operator or Service Provider Arrangements.** If you **did not** purchase this Product directly from Motorola or from a Motorola authorized retail reseller, Motorola does not warrant this Product to you, the end-user. A limited warranty for this Product (including Software) may have been provided to your cable operator or Internet Service Provider ("Service Provider") from whom you obtained the Product. Please contact your Service Provider if you experience problems with this Product.

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

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

What additional provisions should I be aware of? Because it is impossible for Motorola to know the purposes for which you acquired this Product or the uses to which you will put this Product, you assume full responsibility for the selection of the Product for its installation and use. While every reasonable effort has been made to insure that you will receive a Product that you can use and enjoy, Motorola does not warrant that the functions of the Product will meet your requirements or that the operation of the Product will be uninterrupted or error-free. MOTOROLA IS NOT RESPONSIBLE FOR PROBLEMS OR DAMAGE CAUSED BY THE INTERACTION OF THE PRODUCT WITH ANY OTHER SOFTWARE OR HARDWARE. ALL WARRANTIES ARE VOID IF THE PRODUCT IS OPENED, ALTERED, AND/OR DAMAGED.

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





---

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

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

**Retail Purchasers Only.** If you purchased this Product **directly** from Motorola or from a Motorola authorized retail reseller, please call the Motorola toll-free number, **1-877-466-8646** for warranty service or technical support. Technical support charges may apply.

**Cable Operator or Service Provider Arrangements.** If you **did not** purchase this Product directly from Motorola or from a Motorola authorized retail reseller, please contact your Service Provider for technical support.



**MOTOROLA**

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

<http://www.motorola.com>  
585342-001-a 11/2011