



Motorola SURFboard[®]

SVG1501 Wireless Voice Gateway Series*

User Guide

*SVG1501
SVG1501E
SVG1501U
SVG1501UE



© 2009 Motorola, Inc. All rights reserved. No part of this publication may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from Motorola, Inc.

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

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



Safety and Regulatory Information

IMPORTANT SAFETY INSTRUCTIONS

When using your telephone equipment, always follow basic safety precautions to reduce the risk of fire, electric shock, and injury to persons, including the following:

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



- Postpone installation until there is no risk of thunderstorm or lightning activity in the area.
- 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.
- 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.
- 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.
- Use only the power cord and batteries indicated in this manual. Do not dispose of batteries in a fire. They may explode. Check with local codes for possible special disposal instructions.
- 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.
- **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.
- Disconnect TNV circuit connector(s) before disconnecting power.
- Disconnect TNV circuit connector before removing cover.
- 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.
- Upon completion of any service or repairs to this device, ask the service technician to perform safety checks to determine that the device is in safe operating condition.
- Do not open the device. Do not perform any servicing other than that contained in the installation and troubleshooting instructions. Refer all servicing to qualified service personnel.
- This device should not be used in an environment that exceeds 40° C.

SAVE THESE INSTRUCTIONS

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

CARING FOR THE ENVIRONMENT BY RECYCLING



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

Recycling your Motorola Equipment

Please do not dispose of this product with your residential or commercial waste. Some countries or regions, such as the European Union, have set up systems to collect and recycle electrical and electronic waste items. Contact your local authorities for information about practices established for your region. If collection systems are not available, call Motorola Customer Service for assistance. Please visit www.motorola.com/recycle for instructions on recycling.



IMPORTANT VOIP SERVICE INFORMATION



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

When using this VoIP device, you CANNOT make any calls, including an emergency call. E911 location services WILL NOT be available, under the following circumstances:

- Your broadband ISP connection goes down, is lost, or otherwise fails.
- You lose electrical power.

When using this VoIP device, you may be able to make an emergency call to an operator, but E911 location services may not be available under the following circumstances:

- 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.
- You are using a non-U.S. telephone number.
- 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.

INDUSTRY CANADA (IC) STATEMENT

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

- This device may not cause interference, and
- This device must accept any interference, including interference that may cause undesired operation of the device.

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

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

IC RADIATION EXPOSURE STATEMENT

IMPORTANT NOTE: This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

WIRELESS LAN INFORMATION

This device is a wireless network product that uses Direct Sequence Spread Spectrum (DSSS) and Orthogonal Frequency-Division Multiple Access (OFDMA) radio technologies. The device is designed to be interoperable with any other wireless DSSS and OFDMA products that comply with:

- The IEEE 802.11 Standard on Wireless LANs (Revision B and Revision G), as defined and approved by the Institute of Electrical and Electronics Engineers.
- The Wireless Fidelity (Wi-Fi) certification as defined by the Wireless Ethernet Compatibility Alliance (WECA).



RESTRICTIONS ON THE USE OF WIRELESS DEVICES

In some situations or environments, the use of wireless devices may be restricted by the proprietor of the building or responsible representatives of the organization. For example, using wireless equipment in any environment where the risk of interference to other devices or services is perceived or identified as harmful.

If you are uncertain of the applicable policy for the use of wireless equipment in a specific organization or environment, you are encouraged to ask for authorization to use the device prior to turning on the equipment.



The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of the devices included with this product, or the substitution or attachment of connecting cables and equipment other than specified by the manufacturer. Correction of the interference caused by such unauthorized modification, substitution, or attachment is the responsibility of the user.

The manufacturer and its authorized resellers or distributors are not liable for any damage or violation of government regulations that may arise from failing to comply with these guidelines.

SECURITY WARNING: This device allows you to create a wireless network. Wireless network connections may be accessible by unauthorized users. For more information on how to protect your network, see [Setting Up Your Wireless LAN](#) or visit the Motorola website.

INTERNATIONAL DECLARATION OF CONFORMITY

We, Motorola, Inc., 101 Tournament Drive, Horsham, PA 19044, U.S.A., declare under our sole responsibility that the SURFboard SVG1501 Wireless Voice Gateway Series to which this declaration relates is in conformity with one or more of the following standards:

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

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

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



Table of Contents

Safety and Regulatory Information

Overview

Contact Information	1
Standard Features.....	1
SVG1501 LAN Choices	2
USB Connection (SVG1501U Only).....	2
Wireless LAN	2
Wired Ethernet LAN.....	4
Front Panel.....	5
Rear Panel.....	6
MAC Label	7

Getting Started

Inside the Box.....	8
Before You Begin.....	9
Signing Up for Service.....	9
System Requirements	9
Connecting the SVG1501	10
Connecting the SVG1501U.....	11
Wall Mounting the SVG1501	12
Wall Mounting Template.....	14
Setting Up Internet Access	15
Configuring TCP/IP in Windows XP	15
Configuring TCP/IP in Windows Vista	15
Verifying the IP Address in Windows XP	16
Verifying the IP Address in Windows Vista.....	16
Renewing Your IP Address	17
Setting Up a Wi-Fi Network.....	17

Basic Configuration

Starting the SVG1501 Configuration Manager (CMGR)	18
SVG1501 Menu Options Bar	19
Getting Help.....	20
Exiting the SVG1501 Configuration Manager	20

Status Pages

Status Software Page	21
Status Connection Page	21
Status Security Page	22
Changing the SVG1501 Default Password	22
Status Diagnostics Page.....	23



Ping Utility	23
Traceroute Utility	24
Status Event Log Page	25
Basic Pages	
Basic Setup Page	26
Basic DHCP Page	27
Basic DDNS Page	29
Basic Backup Page	30
Restoring Your SVG1501 Configuration	30
Backing Up Your SVG1501 Configuration	30
Advanced Pages	
Advanced Options Page	31
Advanced IP Filtering Page	33
Advanced MAC Filtering Page	34
Setting a MAC Address Filter	34
Advanced Port Filtering Page	35
Advanced Port Forwarding Page	35
Advanced Port Triggers Page	37
Advanced DMZ Host Page	38
Setting Up the DMZ Host	38
Advanced Routing Information Protocol Setup Page	38
Firewall Pages	
Firewall Web Content Filter Page	40
Firewall Local Log Page	41
Firewall Remote Log Page	41
Parental Control Pages	
Parental Control User Setup Page	43
Parental Control Basic Setup Page	45
Parental Control Time of Day Filter Page	46
Parental Control Local Log Page	46
Wireless Pages	
Wireless 802.11 Radio Page	47
Wireless 802.11 Primary Network Page	48
Wireless 802.11 Advanced Page	50
Wireless 802.11 Access Control Page	52
Wireless 802.11 Wi-Fi Multimedia Page	53
Wireless 802.11 Bridging Page	54
Setting Up Your Wireless LAN	55
Encrypting Wireless LAN Transmissions	55
Installing Wireless Clients	56
Installing a Wireless Client for WPA	57
Configuring a Wireless Client for WEP	57



Configuring a Wireless Client with the Network Name (SSID).....	57
VPN Pages	
VPN Basic Page	58
VPN IPsec Page	59
VPN L2TP/PPTP Page	63
VPN Event Log Page	64
MTA Pages	
MTA Status Page.....	65
MTA DHCP Page	65
MTA QoS Page	66
MTA Provisioning Page	67
MTA Event Log Page.....	68
Troubleshooting	
Solutions	69
Front-Panel LEDs and Error Conditions	70
Software License	



1

Overview

The Motorola SURFboard® SVG1501 Wireless Voice Gateway can be used in households with one or more computers capable of wireless connectivity for remote access to the wireless voice gateway.

This user guide provides product overview and set-up information for the SVG1501. It also provides instructions for installing the wireless voice gateway and configuring the wireless LAN, Ethernet, router, DHCP, and security settings.

Note: All references to the SVG1501 used throughout this guide also apply to the SVG1501U, SVG1501E, and SVG1501UE, unless noted otherwise. All SVG1501U references also apply to the SVG1501UE.

Contact Information

- For any questions or assistance with the SVG1501 Wireless Voice Gateway, contact your Internet Service provider.
- For information on customer service, technical support, or warranty claims; see the Motorola SVG1501 Software License, Warranty, Safety, and Regulatory Information card provided with the SVG1501 Wireless Voice Gateway.

Standard Features

The SVG1501 Wireless Voice Gateway offers the following features:

- Combination of five separate products in one compact unit — a DOCSIS® 2.0 cable modem, IEEE 802.11g wireless access point (Wi-Fi® certified), Ethernet 10/100Base-T connections, two VoIP Internet telephone connections, and firewall
- Advanced firewall for enhanced network security from undesired attacks over the Internet
- Data encryption and network access control for wireless transmissions
- Easy wireless installation and security setup wizard
- Integrated high-speed cable modem for continuous broadband access
- One broadband connection for up to 245 computers
- IEEE 802.11g wireless access for home or small networking
- Voice-over-Internet Protocol (VoIP) telephone service with two telephone lines
- Secure Wireless Fidelity (Wi-Fi) broadband connection for Wi-Fi enabled devices



- Four 10/100Base-T Ethernet uplink ports supporting half- or full-duplex connections with auto-MDIX capability
- Universal Serial Bus (USB) connection for a single PC (SVG1501U models only)
- Routing for a wireless LAN (WLAN) or a wired Ethernet LAN
- Built-in DHCP server to configure a combined wired and/or wireless Class C private LAN
- Virtual private network (VPN) pass-through operation supporting IPSec, PPTP, or L2TP to securely connect remote computers over the Internet
- SVG1501 Configuration Manager (CMGR) which provides easy configuration of wireless, Ethernet, router, DHCP, and security settings
- Telephone modem and fax support
- VoIP telephone service through your cable connection offering many traditional telephone services, such as:
 - Local and long distance calling
 - Three-way calling
 - Voicemail
 - Number redial
 - Speed dial
 - Caller ID, Call Waiting, Call Forwarding, and Call Return

SVG1501 LAN Choices

You can connect up to 245 client computers to the SVG1501 using one or any combination of the following network connections:

- Universal Serial Bus (USB) – SVG1501U models only
- Wireless LAN (WLAN)
- Ethernet local area network (LAN)
- Wi-Fi connections to Wi-Fi enabled devices

USB Connection (SVG1501U Only)

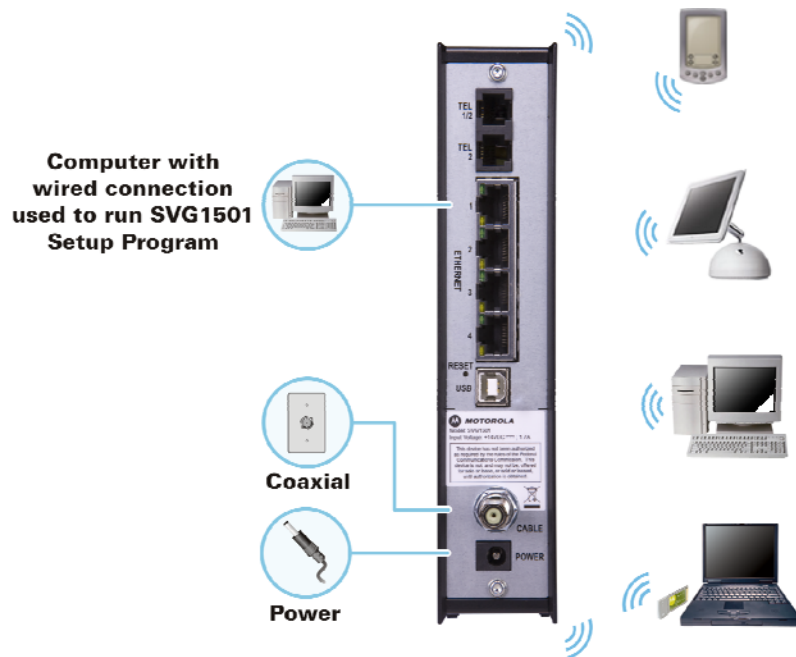
You can connect a single computer running Windows XP or Windows Vista to the SVG1501U USB V2.0 port.

Wireless LAN

A wireless network eliminates the need for wiring to connect computers throughout the home or office. Each computer or device on a WLAN must be Wi-Fi enabled with either a built-in or external wireless adapter.

Laptops — Use a built-in wireless notebook adapter, a wireless PCMCIA slot adapter, or a wireless USB adapter.

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



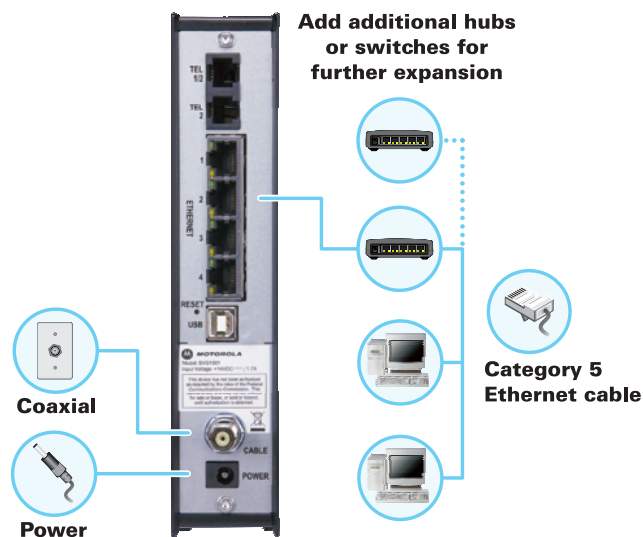
Sample Wireless Network Connections (SVG1501U model shown)

Your maximum wireless operation distance depends on the type of materials through which the signal must pass and the location of your SVG1501 and clients (stations). Motorola cannot guarantee wireless operation for all supported distances in all environments.



Wired Ethernet LAN

You can connect any PC with an Ethernet LAN port to the SVG1501 Ethernet connection. Because the SVG1501 Ethernet port supports auto-MDIX, you can use a straight-through or cross-over cable to connect a hub, switch, or computer. Use category 5, or better, cabling for all Ethernet connections.



Sample Ethernet to Computer Connection (SVG1501U model shown)

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

- Connect a hub or switch to any Ethernet port on the SVG1501.
- Use Ethernet hubs, switches, or routers to connect up to any combination of 245 computers and wireless clients to the SVG1501.



Front Panel

The SVG1501 front panel contains indicator lights and the **WPS** button which is used to configure Wi-Fi Protected Security (WPS) on compatible clients connected to the SVG1501 network.

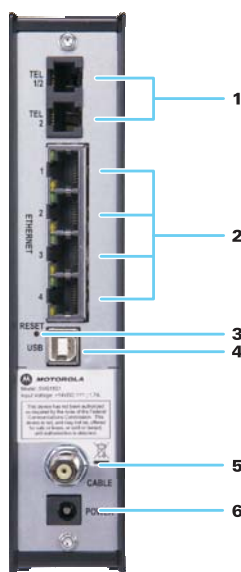


The SVG1501 front panel LED indicators provide the following status for power, communications, and errors:

LED	Flashing	On
1 POWER	Not applicable — LED does not flash	Green: Power is properly connected
2 RECEIVE	Scanning for a downstream channel connection	Green: Downstream channel is connected
3 SEND	Scanning for an upstream channel connection	Green: Upstream channel is connected
4 ONLINE	Scanning for Internet connection; transmitting or receiving data over the Internet	Green: Startup process completed
5 TEL1 TEL 2	Telephone is off-hook; dialing or call in progress	Green: Telephone is connected and activated; on-hook
6 WIRELESS	Green: Wi-Fi enabled with encrypted wireless data activity. Long/short flash indicates Wireless pairing with Client card in progress. Amber: Wi-Fi enabled with unencrypted wireless data activity.	Green: Wireless pairing successfully established between SVG1501 and another Wi-Fi enabled device on your network — cellular telephone, PDA, laptop, etc. Amber: Mobile pairing successful. Turns green after five minutes.



Rear Panel



Both the SVG1501 and SVG1501U (shown above) rear panels contain the following cabling port and connectors:

Item	Description
1 TEL1/2 TEL 2	VoIP connection for a single or two-line telephone VoIP connection for a single-line telephone
2 ETHERNET 1 2 3 4	Use any Ethernet port to connect an Ethernet-equipped computer, hub, bridge, or switch using an RJ-45 cable. Activity LED — Green LED defines the activity of the Ethernet connector. When LED is ON, there is no data traffic and a connection is stabilized. When LED is FLASHING, data is being transmitted upstream or downstream. When LED is OFF, the unit is not powered or there is no Ethernet connection. 10/100 LED — Indicates the connection data rate. When Green LED is ON, the connection is at a 100Base-T rate. When Amber LED is ON, the connection is at a 10Base-T rate.
3 RESET	Resets the wireless voice gateway. It may take 5 to 30 minutes to find and lock on the appropriate communications channels. Press and hold the RESET button for five seconds or longer to restore the factory default settings.
4 USB	For Windows only, you can use the USB port to connect a PC to the



Item	Description
	SVG1501U. You cannot connect a Macintosh or UNIX® computer to the USB port on the SVG1501U. Note: USB connector is available on SVG1501U models only.
5	CABLE Connects the SVG1501 to a cable wall outlet.
6	POWER Provides power to the SVG1501.

MAC Label

The SVG1501 Media Access Control (MAC) label, located on the bottom of the SVG1501, contains a unique, 48-bit value that identifies each Ethernet network device. To receive data service, you will need to provide the MAC address marked **HFC MAC ID** to your Internet Service provider. To receive VoIP service, you may need to provide the **MTA MAC ID** to your VOIP provider.










2

Getting Started

Inside the Box

Verify that the following items are included in the box with the SVG1501:

Item		Description
Power cord		Connects the SVG1501 to an AC electrical outlet
10/100Base-T Ethernet cable		Connects the SVG1501 to the network via the Ethernet port. Cable must be standard Cat 5 or greater.
Software License & Regulatory Card		Contains software license, warranty, and safety information for the SVG1501.
SVG1501 Installation CD-ROM		Contains the SVG1501 Wi-Fi Wizard, software license agreement, multi-language SVG1501 User Guides, and USB drivers (for SVG1501U models only).
SVG1501 Install Sheet		Provides basic information for setting up the SVG1501

You will need a 75-ohm coaxial cable with F-type connectors to connect the SVG1501 to the nearest cable outlet. If a TV is connected to the cable outlet, you may need a 5- to 900 MHz RF splitter and two additional coaxial cables to use the TV and the SVG1501.



Before You Begin

Take the following precautions before installing the SVG1501:

- Wait until there is no risk of thunderstorm or lightning activity in the area.
- To avoid potential shock, always unplug the power cord from the wall outlet or other power source before disconnecting it from the SVG1501 rear panel.
- To prevent overheating the SVG1501, do not block the ventilation holes on the sides of the unit. Do not open the unit. Refer all service to your Internet Service provider.
- Do not connect both the Ethernet and USB cables to the same computer. Connect to either Ethernet or USB.

Check that you have the required cables, adapters, and adapter software. Verify that the proper drivers are installed for the Ethernet adapter on each networked computer. For information on WLAN setup, see [Setting Up Your Wireless LAN](#).

Signing Up for Service

You must sign up with an Internet Service provider to access the Internet and other online services.

- For data service, you will need to provide the MAC address marked **HFC MAC ID** printed on the [MAC label](#).

System Requirements

Your computer must meet the following minimum requirements:

- Computer with Pentium® class or better processor
- Windows XP, Windows Vista, Macintosh, or UNIX operating system with available operating system CD-ROM
- Any web browser, such as Microsoft Internet Explorer, Netscape Navigator®, or Mozilla® Firefox®



Connecting the SVG1501

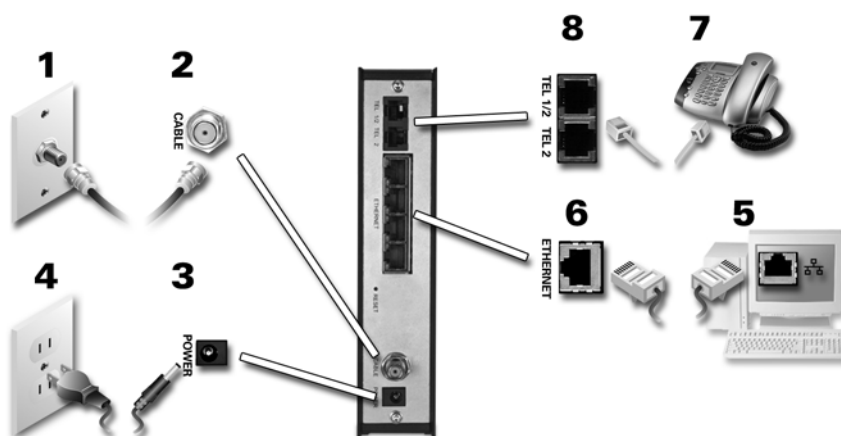
CAUTION: To reduce the risk of fire, use only No. 26 or larger UL Listed or CSA Certified Telecommunication Line Cord or national equivalent to connect a telephone line to your SVG1501.

Contact your service provider before connecting your Motorola SVG1501 to your existing telephone wiring. Do not connect the telephone wire to a traditional telephone (PSTN) service.

Before starting, be sure the computer is turned on and the SVG1501 power cord is unplugged.

1. Connect the coaxial cable to the cable outlet or splitter, and then to the Cable connector on the SVG1501.
Hand-tighten the connectors to avoid damaging them.
2. Plug the power cord into the Power port on the SVG1501 and then 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. The first time you plug in the SVG1501, allow 5- to 30 minutes to find and lock on the appropriate communications channels.
3. Connect the Ethernet cable to the Ethernet port on the computer and then to the Ethernet port on the gateway.
4. Plug the telephone cord of a single or two-line telephone into the telephone and then into the TEL 1/2 port on the rear of the SVG1501.

Note: Contact a VoIP service provider to activate this service.



5. For a second telephone, plug the telephone wire of a single-line telephone into the TEL 2 port on the rear of the SVG1501.
6. Check that the LEDs on the front panel cycle through the following sequence:



SVG1501 LED Activity During Startup

LED	Description
POWER	Turns on when AC power is connected to the SVG1501. Indicates power is connected properly.
RECEIVE	Flashes while scanning for the downstream receive channel. Changes to solid green when the receive channel is locked.
SEND	Flashes while scanning for the upstream send channel. Changes to solid green when the send channel is locked.
ONLINE	Flashes during SVG1501 registration and configuration. Changes to solid green when the SVG1501 is registered.

Connecting the SVG1501U

CAUTION: Before plugging in the USB cable on the SVG1501U, load the SVG1501 Installation CD-ROM in CD-ROM drive.

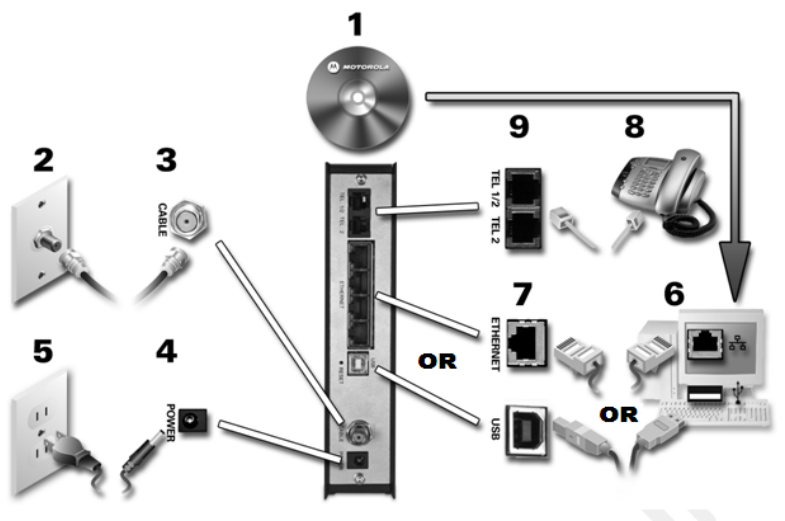
Do not connect the Ethernet and USB cables on the same computer at any time.

Before starting, be sure the computer is turned on and the SVG1501U power cord is unplugged.

1. Insert the SVG1501 Installation CD-ROM into the CD-ROM drive and install the applicable USB drivers.
2. Connect one end of the coaxial cable to the cable outlet or splitter.
3. Connect the other end of the coaxial cable to the Cable connector on the SVG1501U. Hand-tighten the connectors to avoid damaging them.
4. Plug the power cord into the Power port on the SVG1501U.
5. 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. The first time you plug in the SVG1501U, allow it 5- to 30 minutes to find and lock on the appropriate communications channels.

6. Connect the USB or Ethernet cable to the appropriate port on the computer.
7. Connect the other end of the USB or Ethernet cable to the appropriate port on the gateway.



8. Plug the telephone cord of a single or two-line telephone into the telephone.
9. Plug the other end of the telephone cord of a single or two-line telephone into the TEL 1/2 port on the rear of the gateway.

Note: Contact a VoIP service provider to activate this service.

10. For a second telephone, plug the telephone wire of a single-line telephone into the TEL 2 port on the rear of the SVG1501.
11. Check that the LEDs on the front panel cycle through the proper sequence, see [SVG1501 LED Activity During Startup](#).

Wall Mounting the SVG1501

You can optionally mount the SVG1501 on a wall:

- Locate the unit as specified by the local or national codes governing residential or business cable TV and communications services.
- Follow all local standards for installing a network interface unit/network interface device (NIU/NID).
- Make sure the AC power plug is disconnected from the wall outlet and all cables are removed from the back of the SVG1501 before starting the installation.
- Decide if you want to mount the SVG1501 horizontally or vertically.

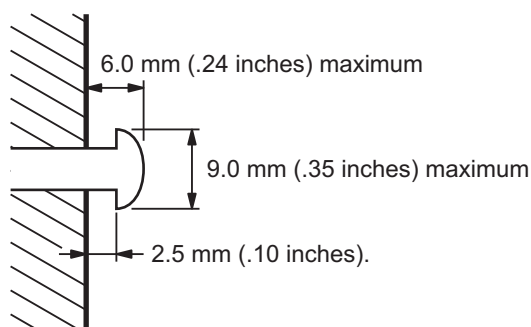
If possible, mount the unit to concrete, masonry, a wooden stud, or some other solid wall material. Use anchors if necessary (for example, if you must mount the unit on drywall).



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

Do the following to mount your SVG1501 on the wall:

1. Print a copy of the [Wall Mounting Template](#).
2. Measure the printed template with a ruler to ensure that it is the correct size.
3. Use a center punch to mark the center of the holes.
4. On the wall, locate the marks for the mounting holes.
5. Drill the holes to a depth of at least 1 1/2 inches (3.8 cm). Use M3.5 x 38 mm (#6 x 1 1/2 inch) screws with a flat underside and maximum screw head diameter of 9.0 mm to mount the SVG1501.
6. Using a screwdriver, turn each screw until part of it protrudes from the wall, as shown in the following wall mounting screw dimensions illustration.



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

7. Place the SVG1501 so the keyholes on the back of the unit are aligned above the mounting screws.
8. Slide the SVG1501 down until it stops against the top of the keyhole opening.
9. After mounting, reconnect the coaxial cable input and Ethernet connection.
10. Plug the power cord into the +12VDC connector on the voice gateway and the electrical outlet.
11. Route the cables to avoid any safety hazards.



Wall Mounting Template

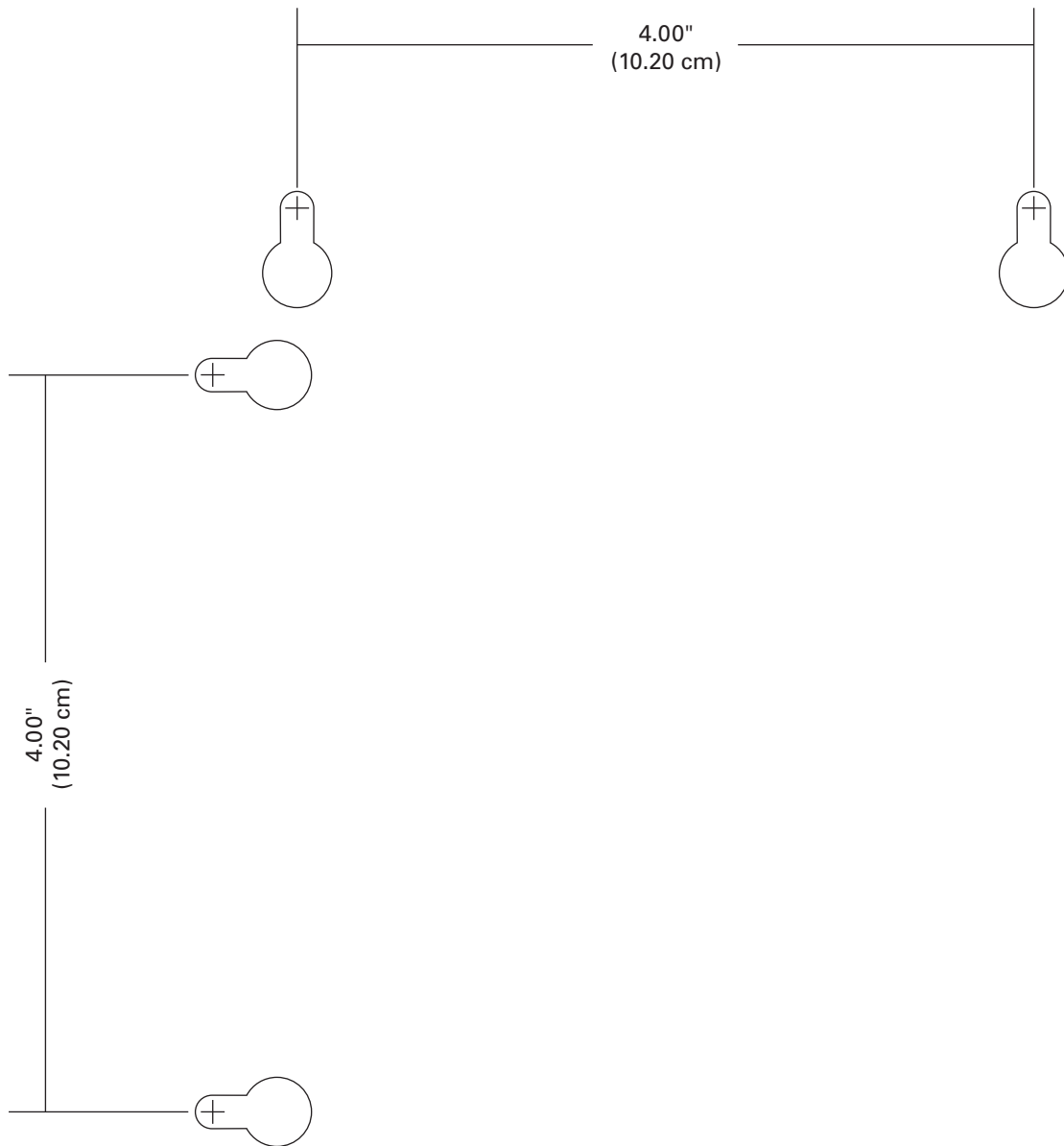


Figure 1 Wall Mounting Template



Setting Up Internet Access

After installing the SVG1501, check that you can connect to the Internet. You can retrieve an IP address for your computer's network interface using one of the following options:

- Retrieve the statically-defined IP address and DNS address
- Automatically retrieve the IP address using the Network DHCP server

The Motorola SVG1501 Wireless Voice Gateway provides a DHCP server on its LAN. Motorola recommends that you configure your LAN to obtain the IPs for the LAN and DNS server automatically.

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

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

Configuring TCP/IP in Windows XP

1. Open the **Control Panel**.
2. Double-click **Network Connections** to list the Dial-up and LAN or High-Speed Internet connections.
3. Right-click the network connection for your network interface.
4. Select **Properties** from the drop-down menu to display the Local Area Connection Properties window. Be sure Internet Protocol (TCP/IP) is checked.
5. Select **Internet Protocol (TCP/IP)** and click **Properties** to display the Internet Protocol (TCP/IP) Properties window.
6. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
7. Click **OK** to save the TCP/IP settings and exit the TCP/IP Properties window.
8. Close the Local Area Connection Properties window and then exit the Control Panel.
9. When you complete the TCP/IP configuration, continue with [Verifying the IP Address in Windows XP](#).

Configuring TCP/IP in Windows Vista

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



- Vista may prompt you for an administrator password or confirmation. Type the password or confirmation, then click **Continue**.
7. Click **Networking** tab, then select **Internet Protocol Version 4 (IPv4)**.
 8. Click **Properties** to display the Internet Protocol Version 4 (TCP/IPv4) Properties window.
 9. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
 10. Click **OK** to save the TCP/IP settings and close the Internet Protocol Version 4 (TCP/IPv4) Properties window.
 11. Click **OK** to close the Local Area Connection Properties window.
 12. Close the remaining windows and exit the Control Panel.
 13. When you complete the TCP/IP configuration, continue with Verifying the IP Address in Windows Vista.

Verifying the IP Address in Windows XP

To check the IP address:

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

If an Auto-configuration IP Address displays, this indicates possible cable network problems or an improper connection between your computer and the SVG1501.

Check the following:

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

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

Verifying the IP Address in Windows Vista

Do the following to verify the IP address:

1. On the Windows Desktop, click **Start**.
2. Click **All Programs**.
3. Click **Accessories**.
4. Click **Command Prompt** to open a command prompt window.
5. Type **ipconfig** and press **Enter** to display the IP address.

If an Auto-configuration IP Address displays, this indicates an improper connection between your computer and the SVG1501, or there are possible cable network problems.



Renewing Your IP Address

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

1. Open a command prompt window.
2. At the command prompt, type **ipconfig /renew** and press **ENTER** to obtain a new IP address.
3. Type **exit** and press **ENTER** to close the command prompt window.

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

Setting Up a Wi-Fi Network

Do the following to set up a Wi-Fi network using the WPS button on the SVG1501:

1. Power on the SVG1501 Wireless Voice Gateway.
2. Power on the WPS-enabled devices you want to have access to the network, such as a PC, router, or telephone.

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

3. Press **WPS** button on the SVG1501.
4. If applicable, press **WPS** button on the other WPS devices.



3

Basic Configuration

For normal operation, you do not need to change most default settings.

CAUTION: To prevent unauthorized configuration, change the default password immediately when you first configure the SVG1501. See [Changing the SVG1501 Default Password](#).

Firewalls are not foolproof. Choose the most secure firewall policy you can. See [Firewall Pages](#) for more information.

Starting the SVG1501 Configuration Manager (CMGR)

Use the SVG1501 Configuration Manager (CMGR) to change and view settings on your SVG1501.

1. Open the web browser on a computer connected to the SVG1501 over an Ethernet connection.

Note: Do not attempt to configure the SVG1501 over a wireless connection.

2. In the Address or Location field of your browser, type **http://192.168.0.1** and press **ENTER**.
3. Type **admin** in the Username field (this field is case-sensitive).
4. Type **motorola** in the Password field (this field is case-sensitive).

Login

Login
Please enter username and password to login.

Username

Password

5. Click **Login** to display the SVG1501 Status Connection page.



Startup Procedure			
Procedure	Status	Comment	
Acquire Downstream Channel		Locked	
Connectivity State	OK	Operational	
Boot State	OK	Operational	
Configuration File			
Security	Disabled	Disabled	
Downstream Channel			
Lock Status	Locked	Modulation	QAM64
Channel ID	0	Symbol rate	5056941
Downstream Frequency	447000000 Hz	Downstream Power	14.3 dBmV
SNR	36.4 dBmV		
Upstream Channel			
Lock Status	Locked	Modulation	QAM16
Channel ID	1	Symbol rate	640 Ksym/sec
Upstream Frequency	21008000 Hz	Upstream Power	28.5 dBmV
CM IP Address	Duration	Expires	
-----	D: -- H: -- M: -- S: --	-----	

The Status Connection page provides RF Downstream and Upstream channel status information on the network connection of the SVG1501.

If you have problems starting the SVG1501 Configuration Manager (CMGR), see [Troubleshooting](#) for more information.

SVG1501 Menu Options Bar

The SVG1501 Menu Options bar is displayed at the top of the SVG1501 Configuration Manager window.



Configuration Manager Menu Options Bar

Menu Option Pages	Function
Status	Provides information about the SVG1501 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 SVG1501 user name and password.
Basic	Views and configures SVG1501 IP-related configuration data, including Network Configuration, WAN Connection Type, DHCP, and DDNS.
Advanced	Configures and monitors how the SVG1501 routes IP traffic



Menu Option Pages	Function
Firewall	Configures and monitors the SVG1501 firewall
Parental Control	Configures and monitors the SVG1501 parental control feature
Wireless	Configures and monitors the SVG1501 wireless networking features
VPN	Configures and monitors SVG1501 operation with a VPN
MTA	Monitors the telephone features of the SVG1501
Logout	Exits the SVG1501 Configuration Manager

Getting Help

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

Exiting the SVG1501 Configuration Manager

To log off and close the SVG1501 Configuration Manager:

- Click **Logout** on the SVG1501 Menu Options bar.



4

Status Pages

Use the SVG1501 Status pages to get information about the SVG1501 hardware and software, MAC address, cable modem IP address, serial number; and to monitor your cable system connection, access additional diagnostic tools, and change your SVG1501 user name and password.

Status Software Page

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

Information	
Standard Specification Compliant	DOCSIS 2.0
Hardware Version	1
Software Version	SVG1501E-2.9.9.9-LAB-98-98-SH
Cable Modem MAC Address	00:1e:5a:8c:e1:1a
Cable Modem Serial Number	150100000000000000000003
CM certificate	Installed
Status	
System Up Time	25 days 04h:59m:58s
Network Access	Denied
Cable Modem IP Address	---.---.---.---

Status Connection Page

Check the HFC and IP network connectivity status of the SVG1501.

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

Startup Procedure			
Procedure	Status	Comment	
Acquire Downstream Channel		Locked	
Connectivity State	OK	Operational	
Boot State	OK	Operational	
Configuration File			
Security	Disabled	Disabled	
Downstream Channel			
Lock Status	Locked	Modulation	QAM64
Channel ID	0	Symbol rate	5056941
Downstream Frequency	447000000 Hz	Downstream Power	13.1 dBmV
SNR	37.7 dBmV		
Upstream Channel			
Lock Status	Locked	Modulation	QAM16
Channel ID	1	Symbol rate	640 Ksym/sec
Upstream Frequency	21008000 Hz	Upstream Power	31.0 dBmV
CM IP Address	Duration	Expires	
---.---.---.---	D: -- H: -- M: -- S: --	--- -- --:--:--	



Status Security Page

Define administrator access privileges by changing your SVG1501 user name and password, and reset your user name and password to the default setting.

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

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

Changing the SVG1501 Default Password

CAUTION: To prevent unauthorized configuration, immediately change the default password when you first configure your Motorola SVG1501.

1. In the Password Change Username field, type your new user name.
2. In the New Password field, type your new password (this field is case-sensitive).
3. In the Re-Enter New Password field, type your new password again (this field is case-sensitive).
4. In the Current Username Password field, type your old password.
5. Under Restore Factory Defaults, select **No**.
6. Click **Apply** to update the user name and password.

Restoring Factory Defaults

Note: You must log in using the default user name and password after applying the restore factory settings change.

1. Under Restore Factory Defaults, select **Yes**.
2. Click **Apply** to reset the user name and password to the original factory settings.
3. Log in again using the defaults. Note that both entries are case-sensitive.
User name: **admin**
Password: **motorola**



Status Diagnostics Page

Use the following diagnostic tools to troubleshoot IP connectivity problems:

- Ping (LAN)
- Traceroute (WAN)

Ping Utility

Use Ping (Packet InterNet Groper) to check connectivity between the SVG1501 and other devices on the SVG1501 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 SVG1501.

The screenshot shows the 'Select Utility' window with 'Ping' selected. The 'Ping Test Parameters' section includes: Target (192.168.0.1), Ping Size (64 bytes), No. of Pings (3), and Ping Interval (1000 ms). Below are buttons for 'Start Test', 'Abort Test', and 'Clear Results'. The 'Results' section displays: 'Pinging 192.168.0.1 with 64 bytes of data.[Complete]', three successful replies from 192.168.0.1 with 64 bytes and 0 ms response time, '3/3 replies received.', and summary statistics: 'min time=0 ms, max time=10 ms, avg time=0 ms'.

Testing Network Connectivity with the SVG1501

To check connectivity between the SVG1501 and other devices on the SVG1501 LAN, perform the following test:

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

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



Traceroute Utility

Use Traceroute to map the network path from the SVG1501 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/Q...
Time Not Established	Notice (6)	Ds Lock Failed - Reinitialize MAC...
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...
Time Not Established	Notice (6)	Ds Lock Failed - Reinitialize MAC...
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...
Time Not Established	Notice (6)	Ds Lock Failed - Reinitialize MAC...
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire FEC f...
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...
Time Not Established	Notice (6)	Ethernet link up - ready to pass packets
Thu Nov 13 14:47:40 2008	Notice (6)	Modem Is Shutting Down and Rebooting...
Thu Nov 13 14:47:40 2008	Critical (3)	Received Response to Broadcast Maintenance Request, But no Un...
Thu Nov 13 14:47:40 2008	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...
Thu Nov 13 14:43:54 2008	Information (7)	Registration Completed
Thu Nov 13 14:43:54 2008	Information (7)	Authorized
Thu Nov 13 14:43:54 2008	Information (7)	Retrieved Time SUCCESS
Thu Nov 13 14:43:54 2008	Information (7)	Retrieved TFTP Config sbv5200_cm_dual_1.1_dqos_full_pc_sbvpro...
Thu Nov 13 14:43:54 2008	Information (7)	Retrieved DHCP SUCCESS
Thu Nov 13 14:43:47 2008	Information (7)	Acquired Upstream SUCCESS
Thu Nov 13 14:43:43 2008	Information (7)	Acquired Downstream (651038118 Hz) SUCCESS
Thu Nov 13 14:43:32 2008	Notice (6)	Ds Lock Failed - Reinitialize MAC...
Thu Nov 13 14:43:32 2008	Information (7)	Retrieved Time SUCCESS
Thu Nov 13 14:43:32 2008	Information (7)	Retrieved TFTP Config sbv5200_cm_dual_1.1_dqos_full_pc_sbvpro...
Time Not Established	Information (7)	Retrieved DHCP SUCCESS
Time Not Established	Information (7)	Acquired Upstream SUCCESS



5

Basic Pages

View and configure SVG1501 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 your SVG1501 configuration on your computer

Basic Setup Page

Configure the basic features of your SVG1501 gateway related to your ISP connection.

Primary Mode	
NAPT mode	Enabled
Changes may require a reboot to take effect.	
Apply	
Network Configuration	
LAN IP Address	192 . 168 . 0 . 1
MAC Address	00:21:80:d2:80:15
WAN IP Address	--- : --- : --- : ---
MAC Address	00:21:80:d2:80:16
Duration	D: -- H: -- M: -- S: --
Expires	--- : --- : --- : ---
Release WAN Lease Renew WAN Lease	
WAN Connection Type DHCP	
Host Name	(Required by some ISPs)
Domain Name	(Required by some ISPs)
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
NAPT mode	<p>NAPT is a special case of NAT, where many IP numbers are hidden behind a number of addresses. In contrast to the original NAT, however, this does not mean there can be only that number of connections at a time.</p> <p>In NAPT mode, an almost arbitrary number of connections are multiplexed using TCP port information. The number of simultaneous connections is limited by the number of addresses multiplied by the number of available TCP ports.</p>



Field	Description
LAN	
IP Address	Enter the IP address of the SVG1501 on your private LAN.
MAC Address	Media Access Control address — a set of 12 hexadecimal digits assigned during manufacturing that uniquely identifies the hardware address of the SVG1501 Access Point.
WAN	
IP Address	The public WAN IP address of your SVG1501 device, which is either dynamically or statically assigned by your ISP.
MAC Address	Media Access Control address — a set of 12 hexadecimal digits assigned during manufacturing that uniquely identifies the hardware address of the SVG1501 Access Point.
Duration	Describes how long before your Internet connection expires. The WAN lease will automatically renew itself when it expires.
Expires	Displays the exact time and date the WAN lease expires.
Release WAN Lease	Click to release WAN lease.
Renew WAN Lease	Click to renew WAN lease.
WAN Connection Type	DHCP or Static IP. If your ISP uses DHCP, select DHCP and enter a Host Name and Domain name, if required. If your ISP uses static IP addressing, select Static IP and enter the information provided by your ISP for Static IP Address, Static IP Mask, Default Gateway, Primary DNS, and Secondary DNS.
Host Name	If WAN Connection Type is DHCP, enter a Host Name, if required.
Domain Name	If WAN Connection Type is DHCP, enter a Domain Name, if required.
MTU Size	Maximum Transmission Unit (MTU) is the largest size packet or frame that can be sent. The default value is suitable for most users.
Spoofed MAC Address	If WAN Connection Type is Static IP, enter the information provided by your ISP for Static IP Address, Static IP Mask, Default Gateway, Primary DNS, and Secondary DNS.

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

Basic DHCP Page

Configure and view the status of the optional internal SVG1501 DHCP (Dynamic Host Configuration Protocol) server for the LAN.



DHCP					
DHCP Server		<input checked="" type="radio"/> Yes <input type="radio"/> No			
Starting Local Address		192.168.0.10			
Number of CPEs		245			
Lease Time		3600			
Apply					
DHCP Clients					
MAC Address	IP Address	Subnet Mask	Duration	Expires	Select
000a5e510499	192.168.0.014	255.255.255.000	D:00 H:01 M:00 S:00	----- -:-:- -----	<input checked="" type="radio"/>
Force Available					
WINS Addresses					
Add Primary Add Secondary					
Add Tertiary					
Primary: 0.0.0.0 Secondary: 0.0.0.0 Tertiary: 0.0.0.0					
Remove WINS Address Clear All					
Current System Time: -----					

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

Field Descriptions for the Basic DHCP Page

Field	Description
DHCP Server	Select Yes to enable the SVG1501 DHCP Server. Select No to disable the SVG1501 DHCP Server.
Starting Local Address	Enter the starting IP address to be assigned by the SVG1501 DHCP server to clients in dotted-decimal format. The default is 192.168.0.2.
Number of CPEs	Sets the number of clients for the SVG1501 DHCP server to assign a private IP address. There are 245 possible client addresses. The default is 245 .
Lease Time	Sets the time in seconds that the SVG1501 DHCP server leases an IP address to a client. The default is 3600 seconds (60 minutes).
DHCP Clients	Lists DHCP client device information.
WINS Addresses	Specifies up to three Windows Internet Name Service (WINS) Server Addresses.

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 your SVG1501 to be more easily accessed from various locations on the Internet.

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

Field Descriptions for Basic DDNS Page

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

Click **Apply** to save your changes.



Basic Backup Page

Save your current SVG1501 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 SVG1501 Configuration

1. Type the path with the file name where the backup file is located on your computer, or click **Browse** to locate the file.
2. Click **Restore** to recreate your previously saved SVG1501 settings.

Backing Up Your SVG1501 Configuration

1. Type the path with the file name where you want to store your backup file on your computer, or click **Browse** to locate the file.
2. Click **Backup** to create a backup of your SVG1501 settings.



6

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 that option.

Advanced Options Page

Set the operating modes for adjusting how the SVG1501 device routes IP traffic.

Field Descriptions for the Advanced Options Page

Field	Description
WAN Blocking	Prevents the SVG1501 Configuration Manager or the PCs behind it from being visible to other computers on the SVG1501 WAN. Select Enable to turn on.
IPsec PassThrough	Enables the IPsec Pass-Through protocol to be used through the SVG1501 Configuration Manager so that a VPN device (or software) may communicate properly with the WAN. Select Enable to turn on.



Field	Description
PPTP PassThrough	Enables the Point-to-Point Tunneling Protocol (PPTP) Pass-Through protocol to be used through the SVG1501 Configuration Manager so that a VPN device (or software) may communicate properly with the WAN. Select Enable to turn on.
Remote Config Management	Allows remote access to the SVG1501 Configuration Manager. This enables you to configure the SVG1501 WAN by accessing the WAN IP address at Port 8080 of the configuration manager from anywhere on the Internet. For example, in the browser URL window, type http://WanIPAddress:8080/ to access the SVG1501 Configuration Manager remotely. Select Enable to turn on.
Multicast Enable	Allows multicast-specific traffic (denoted by a multicast specific address) to be passed to and from the PCs on the private network behind the configuration manager. Select Enable to turn on.
UPnP Enable	Turns on the Universal Plug and Play protocol (UPnP) agent in the configuration manager. If you are running a CPE (client) application that requires UPnP, select this box. Select Enable to turn on.
Rg PassThrough	Disables NAT operation allowing all client computers to act as passthrough clients. Select Enable to turn on.
PassThrough Mac Addresses	Specifies up to 32 computers as passthrough clients not subject to NAT, using their MAC addresses. To enable this feature, your cable operator may need to provide additional public IP addresses.

Click **Apply** to save changes.



Advanced IP Filtering Page

Define which local PCs will be denied access to the SVG1501 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 SVG1501 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. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>

Field Descriptions for the Advanced IP Filtering Page

Field	Description
Start Address	Enter the starting IP address range of the computers you want to deny access to the SVG1501 WAN. Enter only the least significant byte of the IP address.
End Address	Enter the ending IP address range of the computers you want to deny access to the SVG1501 WAN. Enter only the least significant byte of the IP address.
Enabled	Activate the IP address filter. Select each range of IP addresses you want to deny access to the SVG1501 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 PCs 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
MAC Addresses	Media Access Control address — a unique set of 12 hexadecimal digits assigned to a PC during manufacturing.

Setting a MAC Address Filter

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



Advanced Port Filtering Page

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 PCs. This setting is not IP address or MAC address specific. For example, to block all PCs on the private LAN from accessing HTTP sites, set the "Start Port" to **80**, "End Port" to **80**, "Protocol" to **TCP**, select **Enabled**, and then click **Apply**.

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

Apply

Field Descriptions for the Advanced Port Filtering Page

Field	Description
Start Port	Enter the starting port number.
End Port	Enter the ending port number.
Protocol	Select TCP , UDP , or Both from the drop-down list.
Enabled	Select 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 PC. This enables incoming requests on specific port numbers to reach web



servers, FTP servers, mail servers, etc. so that they can be accessible from the public Internet.

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

Commonly used Port numbers:

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

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"/>

Field Descriptions for the Advanced Port Triggers Page

Field	Description
Trigger Range	
Start Port	Starting port number of the Port Trigger range.
End Port	Ending port number of the Port Trigger range.
Target Range	
Start Port	Starting port number of the Port Trigger range.
End Port	Ending port number of the Port Trigger range.
Protocol	Select TCP , UDP , or Both from the drop-down list.
Enable	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 PC. The DMZ (De-militarized Zone) is a computer or small sub-network 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 for the DMZ Host. It has a blue header bar. Below it, there is a yellow box containing the text "DMZ Address" followed by a text input field containing "192.168.0.0". Below the input field is a grey button labeled "Apply".

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

Setting Up the DMZ Host

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

Advanced Routing Information Protocol Setup Page

Configure Routing Information Protocol (RIP) parameters related to authentication, destination IP address/subnet mask, and reporting intervals. RIP automatically identifies and uses the best and quickest route to any given destination address. The RIP protocol requires negotiation from both sides (CMRG and CMTS) of the network. The ISP usually sets this up to match their CMTS settings with the configuration in the CMRG.

Note: RIP messaging is sent upstream only when running in Static IP Addressing mode on the Basic Setup page. You must enable Static IP Addressing and then set the WAN IP network information! RIP is normally a function that is tightly controlled via the ISP. RIP Authentication Keys and IDs are normally held as secret information from the end user to prevent unauthorized RIP settings.



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

Field Descriptions for the Advanced RIP Setup Page

Field	Description
RIP Enable	Enables or disables the RIP protocol. RIP helps the router dynamically adapt to the changes in the network. Now obsolete by newer routing protocols, such as OSPF and ISIS.
RIP Authentication	Adds a plain text password or a shared key to the RIP packet for the CPE and the wireless router to authenticate each other.
RIP Authentication Key	Encrypts the plain text password that is enclosed in each RIP packet. If you are using the shared key authentication in RIP, you need to provide a key.
RIP Authentication Key ID	Identifies the key to create the authentication data for the RIP packet and indicates the authentication algorithm.
RIP Reporting Interval	Determines how long before a RIP packet is sent to the CPE.
RIP Destination IP Address	Sets location where the RIP packet is sent to update the routing table in your CPE.
RIP Destination IP Subnet Mask	Specifies which CPE you want to receive the RIP packet.



7

Firewall Pages

Use the Firewall Pages to configure the firewall filters and firewall alert notifications. The firewall protects the SVG1501 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 checked="" type="checkbox"/> Enable
Port Scan Detection	<input type="checkbox"/> Enable
IP Flood Detection	<input checked="" type="checkbox"/> Enable
Firewall Protection	<input checked="" type="checkbox"/> Enable



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 SVG1501 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 modem 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
Permitted Connections	Select to have the server e-mail you logs of who is connecting to your network.
Blocked Connections	Select to have the server e-mail you logs of who is blocked from connecting to your network.



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

Click **Apply**.



8

Parental Control Pages

Use Parental Control Pages to configure access restrictions to a specific device connected to the SVG1501 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.

The screenshot displays the 'User Configuration' web interface. At the top, there is an 'Add User' button. Below this, the 'User Settings' section includes a dropdown menu set to '1. Default', an 'Enable' checkbox, and a 'Remove User' button. The 'Password' and 'Re-Enter Password' fields are empty. The 'Trusted User' checkbox is also unchecked. The 'Content Rule' section has a 'White List Access Only' checkbox and a dropdown set to '1. Default'. The 'Time Access Rule' dropdown is set to 'No rule set'. The 'Session Duration' and 'Inactivity time' fields are both set to '0 min'. An 'Apply' button is located at the bottom of the settings section.

The 'Trusted Computers' section contains a text box with the instruction: 'Optionally, the user profile displayed above can be assigned to a computer to bypass the Parental Control login on that computer.' Below this is a time input field showing '00 : 00 : 00 : 00 : 00 : 00' and an 'Add' button. At the bottom, there is a text box containing 'No Trusted Computers' and a 'Remove' button.



Field Descriptions for the Parental Control User Setup Page

Field	Description
Add User Button	Add a user to set parental controls for a specific user.
User Settings	Select the user for whom you want to modify access restrictions. Select Enable to select the user. Click Remove User to delete the user from Parental Controls.
Password	Enter a user password to log onto the Internet.
Re-Enter Password	Enter the password again for confirmation.
Trusted User	Select users who will have full access to Internet content. Select Enable to override set filters without having to turn off filter settings.
Content Rule	Specify which websites each user is allowed to access. Select White List Access Only , then choose a user from the drop-down list.
Time Access Rule	Set a rule to restrict when a selected user can use the Internet.
Session Duration	Set the amount of time a selected user can use the Internet.
Inactivity time	Set the amount of inactivity time before the Internet automatically closes for a selected user.
Trusted Computers	Enter a user's CPE MAC address so that CPE can access the Internet without being censored by the Parental Control. When done, click Add .

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

Add New Policy

1. Default Remove Policy

Keyword List	Blocked Domain List	Allowed Domain List
anonymizer	anonymizer.com	
<input type="text"/>	<input type="text"/>	<input type="text"/>
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

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 SVG1501 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
-----------------	--------	--------	------	--------



9

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 (00:90:4C:A3:09:42)	
Wireless	Enabled
Country	UNITED STATES
Output Power	100%
Channel	1
	Current : 1
Apply	Restore Wireless Defaults

Field Descriptions for the Wireless 802.11 Radio Page

Field	Description
Wireless Interfaces	Shows the MAC address of the installed wireless card. It is not configurable.
Wireless	Shows if the wireless network is enabled or disabled
Country	Restricts the channel set based on the country's regulatory requirements. This is a display-only field.
Output Power	Sets a percentage of the output power of the hardware's maximum capability.
Channel	Selects the channel for access point (AP) operation. the list of available channels depends on the designated country. For this field, the channel selected on the wireless clients on your WLAN must be the same as the channel selected on the SVG1501.



Wireless 802.11 Primary Network Page

Configure your primary wireless network.

Motorola (00:90:4C:A3:09:42)

Primary Network	Enabled	Automatic Security Configuration
Network Name (SSID)	Motorola	WPS
Closed Network	Disabled	WPS Config State: Unconfigured
WPA	Disabled	The physical button on the AP will provision wireless clients using Wi-Fi Protected Setup (WPS)
WPA-PSK	Disabled	Device Name: MotorolaAP
WPA2	Disabled	WPS Setup AP PIN: 12345670 [Configure]
WPA2-PSK	Disabled	WPS Add Client Add a client: <input type="radio"/> Push-Button <input checked="" type="radio"/> PIN [Add]
WPA/WPA2 Encryption	Disabled	PIN: []
WPA Pre-Shared Key	[]	
	<input type="checkbox"/> Show Key	
RADIUS Server	0.0.0.0	
RADIUS Port	1812	
RADIUS Key	[]	
Group Key Rotation Interval	0	
WPA/WPA2 Re-auth Interval	3600	

Field Descriptions for the Wireless 802.11 Primary Network Page

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



Field	Description
WPA Pre-Shared Key Show Key	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. Show Key - displays the WPA Pre-Shared Key.
RADIUS Server	Sets the RADIUS server IP address to use for client authentication using the dotted-decimal format (xxx.xxx.xxx.xxx).
RADIUS Port	Sets the UDP port number of the RADIUS server; default is 1812.
RADIUS Key	Sets the shared secret for the RADIUS connection; key is a 0 to 255 character ASCII string.
Group Key Rotation Interval	Sets the WPA Group Rekey Interval in seconds. Set to zero to disable periodic rekeying.
WPA/WPA2 Re-auth Interval	Sets the amount of time the wireless router can wait before re-establishing authentication with the CPE.
WEP Encryption	Enables or disables Wired Equivalent Privacy encryption.
Shared Key Authentication	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.
802.1x Authentication	Uses a stronger authentication than WEP and can be used in addition..
Network Key 1 – 4	Sets the static WEP keys when WEP encryption is enabled. <ul style="list-style-type: none">• Enter five ASCII characters or 10 hexadecimal digits for a 64-bit key.• Enter 13 ASCII characters or 26 hexadecimal digits for a 128-bit key. When both WPA encryption and WEP encryption are enabled, only keys 2 and 3 are available for WEP encryption.
Current Network Key	Selects the encryption (transmit) key when WEP encryption is enabled.
PassPhrase	Sets the text to use for WEP key generation.



Wireless 802.11 Advanced Page

Configure data rates and Wi-Fi thresholds.

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

Field Descriptions for the Wireless 802.11 Advanced Page

Field	Description
54g™ Mode	Sets these network modes: 54g Auto 54g Performance 54g LRS 802.11b only 54g Auto accepts 54g, 802.11g, and 802.11b clients but optimizes performance based on the type of connected clients. 54g Performance accepts only 54g clients and provides the highest performance throughput; 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.
Basic Rate Set	Determines which rates are advertised as basic rates. Default uses the driver defaults. "All" sets all available rates as basic rates.
54g™ Protection	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.
XPress™ Technology	Enhances Wi-Fi throughput and efficiency used when there are mixed wireless networks in the surrounding area from 802.11a/b/g networks.



Field	Description
Afterburner™ Technology	Enhances Wi-Fi 802.11g standard by increasing throughput by 40 percent.
Rate	Forces the transmission rate for the AP to a particular speed. "Auto" provides best performance in nearly all situations.
Output Power	Sets the output power as a percentage of the hardware's maximum capability.
Beacon Interval	Sets the beacon interval for the AP. The default is 100, which is fine for nearly all applications.
DTIM Interval	Sets the wakeup interval for clients in Power Save mode. When a client is running in Power Save mode, Lower SVG1501 bin values provide higher performance but result in decreased client battery life; higher values provide lower performance but increased client battery life.
Fragmentation Threshold	Sets the fragmentation threshold. Packets exceeding this threshold are fragmented into packets smaller than the threshold before packet transmission.
RTS Threshold	Sets the RTS threshold. Packets exceeding this threshold cause the AP to perform an RTS/CTS exchange to reserve the wireless medium before packet transmission.



Wireless 802.11 Access Control Page

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

Wireless Interface Motorola (00:90:4C:A3:09:42)

MAC Restrict Mode Disabled

MAC Addresses

MAC Address	Age(s)	RSSI(dBm)

Apply

Connected Clients

MAC Address	Age(s)	RSSI(dBm)
No wireless clients are connected.		

Field Descriptions for the Wireless 802.11 Access Control Page

Field	Description
Wireless Interface	Shows the MAC address of the installed wireless card. It is not configurable.
MAC Restrict Mode	Selects whether wireless clients with the specified MAC address are allowed or denied wireless access. Select Disabled to allow all clients.
MAC Address	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.
Connected Clients	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).

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

Field Descriptions for the Wireless 802.11 Wi-Fi Multimedia Page

Field	Description
WMM Support	Sets WMM support to Auto, On, or Off. If enabled (Auto or on), WME Information Element is included in beacon frames.
No-Acknowledgement	Sets No-Acknowledgement support to On or Off. When On, acknowledgments for data are not transmitted.
Power Save Support	Sets Power Save support to On or Off. When On, 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.
EDCA AP Parameters	Specifies the parameters for traffic transmitted from the AP to the STA in four Access Categories: <ul style="list-style-type: none"> • Best Effort (AC_BE) • Background (AC_BK) • Video (AC_VI) • Voice (AC_VO) Admission control specifies if it is to be enforced for the Access Categories. Discard Oldest First specifies the discard policy for the queues. "On" discards oldest first; "Off" discards newest first.
EDCA STA Parameters	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="text"/>
<input type="button" value="Apply"/>	

Field Descriptions for the Wireless 802.11 Bridging Page

Field	Description
Wireless Bridging	Enable or disable wireless bridging.
Remote Bridges	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 SVG1501 as an access point for a wireless LAN (WLAN) without changing the default settings.

CAUTION: 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](#)

CAUTION: 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 SVG1501 over a wireless connection.

Connect at least one computer to the SVG1501 Ethernet port.

Configure each wireless client (station) to access the SVG1501.

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 SVG1501	Required on Each Wireless Client
If all of your wireless clients support Wi-Fi Protected Access (WPA), Motorola recommends configuring WPA on the SVG1501	If you use a local pre-shared key (WPA-PSK) passphrase, you must configure the identical passphrase on the SVG1501 and on each wireless client. Home and small-office settings typically use a local passphrase.
Otherwise, configure WEP on the SVG1501	You must configure the identical WEP key on the SVG1501 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 SVG1501 Installation CD-ROM 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-ROM for the adapter in the CD-ROM drive on the client.
2. Install the device software from the CD.
3. Insert the adapter in the PCMCIA or PCI slot or connect it to the USB port.
4. Configure the adapter to obtain an IP address automatically.

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

Configuring Wireless Clients

If You:	You Need to do this on each client,:
Configured WPA on the SVG1501	Configure a Wireless Client for WPA or WPA2
Configured WEP on the SVG1501	Configure a Wireless Client for WEP
Configured the Wireless Network Name on the SVG1501	Configure a Wireless Client with the Network Name (SSID)
Configured a MAC Access Control List on the SVG1501	No client configuration required



Installing a Wireless Client for WPA

If you enabled WPA and set a PSK Passphrase by configuring WPA on the SVG1501, you must configure the same passphrase (key) on each wireless client. The SVG1501 cannot authenticate a client if:

- WPA is enabled on the SVG1501 but not on the client
- The client passphrase does not match the SVG1501 PSK Passphrase

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

Configuring a Wireless Client for WEP

If you enabled WEP and set a key by configuring WEP on the SVG1501, you must configure the same WEP key on each wireless client. The SVG1501 cannot authenticate a client if:

- Shared Key Authentication is enabled on the SVG1501 but not on the client
- The client WEP key does not match the SVG1501 WEP key

For all wireless adapters, you must enter the 64-bit or 128-bit WEP key generated by the SVG1501.

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

Configuring a Wireless Client with the Network Name (SSID)

After you specify the network name on the Wireless Basic Page, many wireless cards or adapters automatically scan for an access point, such as the SVG1501 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 SVG1501.



10

VPN Pages

The **VPN** pages allow you to configure and manage VPN tunnels. You can click any VPN submenu option to view or change the configuration information for that option.

VPN Basic Page

Enable VPN protocols and manage VPN tunnels.

L2TP / PPTP				
L2TP Server	Disabled ▾			
PPTP Server	Disabled ▾			
<input type="button" value="Configure"/>				
IPsec				
IPsec Endpoint	Enabled ▾			
#	Name	Status	Control	Configure
1		NOT Connected	N/A	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
2		NOT Connected	N/A	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="button" value="Add New Tunnel..."/>				

Field	Description
L2TP Server	Enable or disable the Layer 2 Tunneling Protocol
PPTP Server	Enable or disable the Point-to-Point Protocol
IPsec Endpoint	Enable or disable the Internet Protocol Security protocol
Add New Tunnel	Create a new tunnel configuration and append it to the table. Click Edit to add the name and constructs of the tunnel for that tunnel.



VPN IPsec Page

You can configure multiple VPN tunnels to various client computers and store different tunnels, but you cannot enable them for ease of use with connections and/or client computers that are not constantly used.

For each tunnel configuration you store, its unique IPsec parameters are stored using the IPsec Settings section at the bottom of the page. Click **Show Advanced Settings** at the bottom of the page to display the advanced features that control IPSEC key management and negotiation with the far endpoint.

Tunnel	1	Delete Tunnel
Name	<input type="text"/>	Add New Tunnel
	Disabled	Apply
Local endpoint settings		
Address group type	IP subnet	
Subnet	192 . 168 . 0 . 0	
Mask	255 . 255 . 255 . 0	
Identity type	IP address	
Identity	<input type="text"/>	
Remote endpoint settings		
Address group type	IP subnet	
Subnet	0 . 0 . 0 . 0	
Mask	255 . 255 . 255 . 0	
Identity type	IP address	
Identity	<input type="text"/>	
Network address type	IP address	
Remote Address	0.0.0.0	
IPsec settings		
Pre-shared key	EnterAKey	
Phase 1 DH group	Group 1 (768 bits)	
Phase 1 encryption	DES	
Phase 1 authentication	MD5	
Phase 1 SA lifetime	28800 seconds	
Phase 2 encryption	DES	
Phase 2 authentication	MD5	
Phase 2 SA lifetime	3600 seconds	
Show Advanced Settings		
Apply		

Field	Description
Tunnel	Configure each tunnel individually. Preset tunnels are listed by their preset name.



Field	Description
Name	<p>Assign a generic name for a group of settings to a single tunnel.</p> <p>After entering the appropriate tunnel name for the first time, click Add New Tunnel to create a heading for the tunnel settings selected from the Tunnel drop-down list. If you do not assign a name, the tunnels are sequentially numbered.</p>
Enable drop-down	<p>After you name and configure a VPN tunnel, you can store it as disabled or enabled via the Enable/Disable drop-down list.</p> <p>Click Apply to toggle Enable/Disable.</p>
Local Endpoint Settings Address group type	<p>Set the local VPN access group as one of the following group types:</p> <p>Single IP address — for one computer, enter the IP address for the specific computer</p> <p>IP address range — for a small range of computers, enter the starting and ending IP addresses for the group of consecutive IP address that will have access to the VPN tunnel</p> <p>IP Subnet — for an entire subnet/network, enter the Subnet and Mask for IP address range and IP Subnet. Enter the starting and ending IP addresses for the group of consecutive IP addresses that are to have access to the VPN tunnel.</p>
Identity Type	<p>Define the local endpoint identity type to automatically use the WAN IP address of the router or as a user-specified IP address, fully qualified domain name (FQDN), or e-mail address. The far endpoint uses this to identify the VPN termination point and handshake.</p> <p>The remote VPN endpoint on the other side of the tunnel should match these settings for its remote endpoint settings.</p>
Identity	<p>Enter the identity string.</p> <p>For IP address, enter <i>x.x.x.x</i>.</p> <p>For FQDN, enter <i>yourdomain.com</i></p> <p>For email address identity, enter <i>yourname@yourdomain.com</i></p> <p>The remote VPN endpoint on the other side of the tunnel should match these settings for its remote endpoint settings.</p>



Field	Description
Remote Endpoint Settings Address group type	<p>Set the remote VPN access group to one of the following group types:</p> <p>Single IP address — for one computer, enter the IP address for the specific computer</p> <p>IP address range — for a small range of computers, enter the starting and ending IP addresses for the group of consecutive IP addresses to have access to the VPN tunnel.</p> <p>IP Subnet — for an entire subnet/network, enter the Subnet and Mask</p> <p>For IP address range and IP Subnet, enter the starting and ending IP addresses for the group of consecutive IP addresses to have access to the VPN tunnel.</p> <p>The remote VPN endpoint on the other side of the tunnel should match these settings for its local endpoint settings.</p>
Identity type	<p>Define the remote endpoint identity type to automatically use the remote endpoint IP address, or as a user-specified IP address, fully qualified domain name (FQDN), or e-mail address. This is the identity that the far endpoint uses for identification of the VPN termination point and handshake.</p> <p>The remote VPN endpoint on the other side of the tunnel should match these settings for its local endpoint settings.</p>
Identity	<p>Enter the identity string:</p> <p>For IP address, enter x.x.x.x.</p> <p>For FQDN, enter <i>yourdomain.com</i></p> <p>For email address identity, enter <i>yourname@yourdomain.com</i></p> <p>The remote VPN endpoint on the other side of the tunnel should match the settings here for its local endpoint settings.</p>
Network address type	<p>Select the remote endpoint's WAN address type: IP address or Fully Qualified Domain Name (FQDN)</p>
Remote Address	<p>Enter either the IP address of the remote endpoint or its FQDN.</p>
IPsec Settings	<p>Associate one of the two phases of Security Association (SA) to the VPN tunnel. Phase 1 creates an IKE SA. After Phase 1 is completed, Phase 2 creates one or more IPSEC SAs, which are then used to key IPSEC sessions.</p>
Pre-shared key	<p>Enter the "Pre-shared Key" field if one side of the VPN tunnel is using a unique firewall identifier (or Pre-shared Key).</p>



Field	Description
Phase 1 DH group	<p>Select one of the Diffie-Hellman groups: 768 bits, 1024 bits, or 1536 bits.</p> <p>Diffie-Hellman is a cryptographic technique that uses public and private keys for encryption and decryption. The higher the number of bits, the more secure the encryption. Options: Group 1 (768 bits), Group 2 (1024 bits), or Group 5 (1536 bits).</p>
Phase 1 encryption	<p>Secure the VPN connection between endpoints: DES, 3DES, AES-128, AES-192, or AES-256.</p> <p>Select any encryption but make the far endpoints match. Common encryption settings are 3DES and AES.</p>
Phase 1 authentication	<p>Set Authentication, another level of security, to SHA or MD5. Motorola recommends SHA because it is more secure but you can use either authentication provided the other end of the VPN tunnel uses the same method.</p>
Phase 1 SA lifetime	<p>Specify the lifetime of individual rotating keys.</p> <p>Enter the number of seconds for the key to last until a re-key negotiation between each endpoint is negotiated. The default setting is 28,800 seconds.</p> <p>A smaller lifetime is generally more secure, since it would give an attacker a smaller amount of time to try to crack the key, however key negotiation takes up bandwidth, so network throughput is sacrificed with small lifetimes. Entries are typically in the thousands or tens of thousands of seconds.</p>



VPN L2TP/PPTP Page

Configure L2TP and PPTP server options.

PPP Address Range	
Start	10 . 0 . 0 . 1
End	10 . 0 . 0 . 254
PPP Security	
MPPE Encryption	Enabled
<input type="button" value="Apply"/>	
Users	
Username	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
<input type="button" value="Add"/>	
User List	
User list is empty.	
L2TP Server	
Preshared Phrase	<input type="text"/>
<input type="button" value="Apply"/>	

Field	Description
PPP Address Range Start End	Specify the starting and ending IP address range so that when the tunnel is set up, the client and server side get their IP address from this specified range.
PPP Security MPPE Encryption	Enable or disable Microsoft Point to Point Encryption (MPPE). is a type of link encryption, meaning that data sent along this tunnel is encrypted, used in PPTP.
Username	Authenticates the tunnel that was created between the client and the server
Password	Enter a user password for authentication.
Confirm Password	Enter the password again for confirmation.
Preshared Phrase	Authenticates the Layer 2 Tunneling Protocol (L2TP) server.



VPN Event Log Page

View the VPN Event Log, which shows a history of VPN connections and activity in chronological order and the IP address of remote and local endpoints on the tunnel.

Time	Description
Event log is empty.	
Refresh	Clear

- Click **Refresh** to update the Event Log table to show any changes since the web page was last loaded.
- Click **Clear** to clear the log table of its current contents. Only the most recent data appears.



11

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 1	On-Hook
Line 2	On-Hook

MTA DHCP Page

Displays the MTA DHCP lease information.

Lease Paramteres	
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

This 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



MTA Provisioning Page

This page displays the MTA provisioning details about your SVG1501 VoIP telephone connection.

MTA Config File	
Filename	http://sbvprov3.swdev.net/001A6600B06.bin
Contents	<pre> MTA Config File Contents ===== .1.3.6.1.4.1.4491.2.2.1.1.1.7.0.1 .1.3.6.1.2.1.2.2.1.7.9.1 .1.3.6.1.2.1.2.2.1.7.10.1 .1.3.6.1.4.1.4491.2.2.2.1.1.10.0.2 .1.3.6.1.4.1.4491.2.2.2.1.1.8.0.24 .1.3.6.1.4.1.4491.2.2.2.1.1.9.0.40 .1.3.6.1.4.1.4491.2.2.2.1.1.12.0.2427 .1.3.6.1.4.1.4491.2.2.2.1.1.5.0.FFC00000 .1.3.6.1.4.1.4491.2.2.2.1.1.6.0.FFC00000 .1.3.6.1.4.1.4491.2.2.2.1.1.7.0.FFC00000 .1.3.6.1.4.1.4491.2.2.2.1.2.1.1.18.9.10 .1.3.6.1.4.1.4491.2.2.2.1.2.1.1.18.10.10 .1.3.6.1.4.1.4491.2.2.2.1.2.1.1.27.9.1 .1.3.6.1.4.1.4491.2.2.2.1.2.1.1.27.10.1 .1.3.6.1.4.1.4491.2.2.2.1.2.1.1.28.9.8 .1.3.6.1.4.1.4491.2.2.2.1.2.1.1.28.10.8 .1.3.6.1.4.1.4491.2.2.2.1.2.1.1.2.9.2427 .1.3.6.1.4.1.4491.2.2.2.1.2.1.1.2.10.2427 .1.3.6.1.4.1.4491.2.2.2.1.2.1.1.1.9.SBVPROV3-CA-SWDEV.NET .1.3.6.1.4.1.4491.2.2.2.1.2.1.1.1.10.SBVPROV3-CA-SWDEV.NET .1.3.6.1.4.1.1166.1.200.2.36.0.128 Vendor Specific TLV (TLV-43) Start: VendorID 0803002040 Vendor Specific TLV (TLV-43) End: Num of TLV processed (in hex) 1D </pre>
Enterprise MIBs	
OID	Value
emtaInhibitSwDownloadDuringCall	false(2)
emtaFirewallEnable	true(1)
emtaRingWithDCOffset	false(2)
emtaIncludedInCmMaxCpe	false(2)
emtaDhcpOption	packetCableAndCableHomeObsolete(177)
emtaUseAlternateTelephonyRootCert	false(2)
emtaEnableDQoS Lite	false(2)
emtaInhibitNcsSyslog	true(1)
emtaMaintenanceWindowBegin	Thu Jan 01 00:00:00 1970
emtaMaintenanceWindowDuration	0
emtaMaintenanceControlMask	0xffffffff [maintenanceOnCmReset(0) maintenanceOnMtaReset(2) maintenanceOnCMSLoss(3)]
emtaMaintenanceQuarantineTimeout	120
emtaMaintenanceDisconnectedTimeout	120
emtaMaintenanceRFDiscconnectTimeout	300
emtaSignalingAnnouncementCtrl	0x00
emtaSignalingVoiceJitterBufferType	jitterBufferTypeAdaptive(2)
emtaSignalingVoiceJitterNomValue	30
emtaSignalingVoiceJitterMinValue	0
emtaSignalingVoiceJitterMaxValue	60
emtaSignalingDataJitterNomValue	120
emtaSignalingDtmToneRelayRFC2833Support	true(1)
emtaSignalingRtpBaseReceiveUdpPort	53456
emtaSignalingEndptConnectionCleanupTimeout	0
emtaSignalingEmtaResetCleanupTimeout	0
emtaSignalingT38FaxRelaySupport	true(1)



MTA Event Log Page

This page displays the MTA Event Log information and diagnostic messages generated by the MTA for technicians.

Time	Priority	ID	Text
Endpoint			
2007-08-08 16:25:06	5-Information	35	MTA Last 24 Hours: Count of No ACK rec'd from Call Agent=0
mta001a66080b06.swdev.net/206.19.81.247			
2007-08-08 16:25:06	5-Information	35	MTA Last 24 Hours: Average Latency for Response to MGCP Messages=0 ms
mta001a66080b06.swdev.net/206.19.81.247			
2007-08-08 16:25:06	5-Information	35	MTA Last 24 Hours: Average Latency via RTCP Packets=0 ms
mta001a66080b06.swdev.net/206.19.81.247			
2007-08-08 16:25:06	5-Information	35	MTA Last 24 Hours: Maximum Jitter Measurements=0
mta001a66080b06.swdev.net/206.19.81.247			
2007-08-08 16:25:06	5-Information	35	MTA Last 24 Hours: Average Jitter Measurements=0
mta001a66080b06.swdev.net/206.19.81.247			
2007-08-07 16:25:06	5-Information	35	MTA Last 24 Hours: Count of No ACK rec'd from Call Agent=0



12

Troubleshooting

If the solutions listed here do not solve your problem, contact your service provider. Before calling your service provider, try pressing **RESET** on the SVG1501 rear panel.

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

Resetting the SVG1501 may take 5- to 30 minutes. Your service provider may ask for the front panel LED status, see [Front-Panel LEDs and Error Conditions](#).

Solutions

Table 1 – Troubleshooting Solutions

Problem	Possible Solution
Power light is off	Check that the SVG1501 is properly plugged into the electrical outlet. Check that the electrical outlet is working. Press the RESET button.
Cannot send or receive data	Note the status of the LEDs on the front panel, and refer to Front-Panel LEDs and Error Conditions to identify the error. If you have cable TV, check that the TV is working and the picture is clear. If you cannot receive regular TV channels, the data service will not function. Check the coaxial cable at the SVG1501 and wall outlet. Hand-tighten, if necessary. Check the IP address. Follow the steps for verifying the IP address for your system described in Setting Up Internet Access . Call your service provider if you need an IP address. Check that the Ethernet cable is properly connected to the SVG1501 and the computer. Verify connectivity of any device connected via the Ethernet port, by checking the LINK LEDs on the rear panel.



Problem	Possible Solution
Wireless client(s) cannot send or receive data	<p>Perform the first four checks in “Cannot send or receive data.”</p> <p>Check the Security Mode setting on the Wireless Primary Network Page:</p> <ul style="list-style-type: none"> • If you enabled WPA and configured a passphrase on the SVG1501, be sure each affected wireless client has the identical passphrase. If this does not solve the problem, check whether the wireless client supports WPA. • If you enabled WEP and configured a key on the SVG1501, 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 SVG1501. • To temporarily eliminate the Security Mode as a potential issue, disable security. <p>After resolving your problem, be sure to re-enable wireless security.</p> <ul style="list-style-type: none"> • On the Wireless Access Control Page, be sure the MAC address for each affected wireless client is correctly listed.
Slow wireless transmission speed with WPA enabled	<p>On the Wireless Primary Network Page, check whether the WPA Encryption type is TKIP. If all of your wireless clients support AES, change the WPA Encryption to AES.</p>

Front-Panel LEDs and Error Conditions

The SVG1501 front panel LEDs provide status information for the following error conditions:

Table 2 – Front-Panel LEDs and Error Conditions

LED	Status	if, During Startup:	if, During Normal Operation:
POWER	OFF	SVG1501 is not properly plugged into the power outlet	The SVG1501 is unplugged
RECEIVE	FLASHING	Downstream receive channel cannot be acquired	The downstream channel is lost
SEND	FLASHING	Upstream send channel cannot be acquired	The upstream channel is lost
ONLINE	FLASHING	IP registration is unsuccessful	The IP registration is lost



Software License

SURFboard SVG1501 Wireless Voice Gateway

Motorola, Inc.

Home & Networks Mobility Solutions Business ("Motorola")

101 Tournament Drive

Horsham, PA 19044

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

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

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

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

You may:

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

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

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

You may not:

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



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

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

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

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

U.S. GOVERNMENT RESTRICTED RIGHTS

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



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

<http://www.motorola.com>

MOTOROLA and the Stylized M logo are registered in the US Patent and Trademark Office. All other product or service names are the property of their respective owners. ©2009 Motorola, Inc. All rights reserved.
567299-001-c
04/2009