



MOTOROLA

User Guide

Motorola SURFboard®

SVG6x82 Series Wireless Voice Gateway*

*SVG6582

SVG6682



© 2013 Motorola Mobility, LLC. All rights reserved.

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

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

- **Read This Before You Begin** — When using your equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock, and injury to persons, including the following:
- Read all of the instructions listed here and/or in the user manual before you operate this device. Give particular attention to all safety precautions. Retain the instructions for future reference.
- This device must be installed and used in strict accordance with manufacturer's instructions, as described in the user documentation that is included with the device.
- Comply with all warning and caution statements in the instructions. Observe all warning and caution symbols that are affixed to this device.
- To prevent fire or shock hazard, do not expose this device to rain or moisture. The device must not be exposed to dripping or splashing. Do not place objects filled with liquids, such as vases, on the device.
- This device was qualified under test conditions that included the use of the supplied cables between system components. To ensure regulatory and safety compliance, use only the provided power and interface cables and install them properly.
- Different types of cord sets may be used for connections to the main POWER supply circuit. Use only a main line cord that complies with all applicable device safety requirements of the country of use.
- Installation of this device must be in accordance with national wiring codes and conform to local regulations.
- Operate this device only from the type of power source indicated on the device's marking label. If you are not sure of the type of power supplied to your home, consult your dealer or local power company.
- Do not overload outlets or extension cords, as this can result in a risk of fire or electric shock. Overloaded AC outlets, extension cords, frayed power cords, damaged or cracked wire insulation, and broken plugs are dangerous. They may result in a shock or fire hazard.
- Route power supply cords so that they are not likely to be walked on or pinched by items placed upon or against them. Pay particular attention to cords where they are attached to plugs and convenience receptacles, and examine the point where they exit from the device.
- Place this device in a location that is close enough to an electrical outlet to accommodate the length of the power cord.
- Place the device to allow for easy access when disconnecting the power cord of the device from the AC wall outlet.
- Do not connect the plug into an extension cord, receptacle, or other outlet unless the plug can be fully inserted with no part of the blades exposed.
- Place this device on a stable surface.
- Avoid damaging the cable modem with static by touching the coaxial cable when it is attached to the earth-grounded coaxial cable-TV wall outlet.
- Always first touch the coaxial cable connector on the cable modem when disconnecting or reconnecting the Ethernet cable from the cable modem or user's PC.
- It is recommended that the customer install an AC surge protector in the AC outlet to which this device is connected. This is to avoid damaging the device by local lightning strikes and other electrical surges.
- Postpone installation until there is no risk of thunderstorm or lightning activity in the area.
- Do not 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 cover the device or block the airflow to the device with any other objects. Keep the device away from excessive heat and humidity and keep the device free from vibration and dust.



- Wipe the device with a clean, dry cloth. Never use cleaning fluid or similar chemicals. Do not spray cleaners directly on the device or use forced air to remove dust.
- For added protection, unplug the device from the wall outlet and disconnect the cables to avoid damage to this device due to lightning and power surges.
- 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 104° F (40° C).

SAVE THE ABOVE INSTRUCTIONS

Note to CATV System Installer — This reminder is provided to call the CATV system installer’s attention to Article 820.93 and 820.100 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.

IMPORTANT VoIP SERVICE INFORMATION



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

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

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

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

FCC STATEMENTS

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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



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

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

FCC Radiation Exposure Statement

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter except those already approved in this filing.

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.

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.

FCC RADIATION EXPOSURE STATEMENT

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

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

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

WIRELESS LAN INFORMATION

This device is a wireless network product that uses Direct Sequence Spread Spectrum (DSSS) 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, Revision G, and Revision N), as defined and approved by the Institute of Electrical Electronics Engineers
- The Wireless Fidelity (Wi-Fi) certification as defined by the Wireless Ethernet Compatibility Alliance (WECA).



Restrictions on the Use of Wireless Devices

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

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

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



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

Note: The use of the 5150-5250 MHz frequency band is restricted to Indoor Use Only.

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 [Changing the Default Password](#) in the SVG6x82 User Guide for instructions or visit the Motorola website.

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.



Contents

Safety and Regulatory Information	i
Tables	vi
Figures	vi
Getting Started	1
Introduction.....	1
In the Box	1
System Requirements	1
Contact Information	2
Product Overview	3
Front Panel.....	3
Wi-Fi Protected Setup (WPS)	4
Rear Panel.....	5
Gateway Label	5
Installing the Gateway	7
Connecting to Your Computer	7
Testing the Gateway Connections	8
Setting Up an Internet Connection	8
Setting Up a Wireless Network Connection	10
Setting Up a Wireless Network on Your Computer	10
Using the WPS Pairing Button.....	10
Testing Your Wireless Network Connection	11
Accessing the Gateway	12
Starting the Gateway Web Manager	12
Gateway Web Manager Menu Options.....	14
Getting Help.....	14
Exiting the SVG6x82 Web Manager	14
Protecting Your Wireless Network	15
Changing the Default User Name and Password.....	15
Setting Up the Firewall	17
Basic Firewall	18
Firewall Web Filter	18
Firewall Local Log	19
Firewall Remote Log	20
Setting Up the DMZ Host.....	21
Monitoring Your Network	22
Viewing the Gateway Software Information	22
Viewing the Gateway Status	23
Backing up Your Gateway Configuration	24
Restoring Your Gateway Configuration	24
Troubleshooting	25



Solutions	25
Front Panel LED Icons and Error Conditions	26
Warranty Information.....	27

Tables

Table 1 – SVG6x82 Package Contents	1
Table 2 – SVG6x82 Front Panel LED Icons.....	3
Table 3 – SVG6x82 Rear Panel Ports & Connectors.....	5
Table 4 – SVG6x82 Main Menu	14
Table 5 – Troubleshooting Solutions.....	25
Table 6 – Front Panel LED Icons and Error Conditions	26

Figures

Figure 1 – SVG6x82 Front View.....	3
Figure 2 – SVG6x82 Rear View.....	5
Figure 3 – Sample SVG6x82 Gateway Label	6
Figure 4 – SVG6x82 Connection Diagram	7
Figure 5 – SVG6x82 Login Window	12
Figure 6 – SVG6x82 Status Connection Page	13
Figure 7 – SVG6x82 Main Menu Bar	14
Figure 8 – Status Security Page-Change User Name	16
Figure 9 – Change User Password	16
Figure 10 – Firewall Main Page	17
Figure 11 – Firewall Basic Web Content Filter Page	18
Figure 12 – Firewall Web Filtering Page.....	19
Figure 13 – Firewall Local Log Page	19
Figure 14 – Firewall Remote Log Page.....	20
Figure 15 – Advanced DMZ Host Page	21
Figure 16 – SVG6x82 Status Software Page	22
Figure 17 – SVG6x82 Status Connection Page	23
Figure 18 – SVG6x82 Basic Backup/Restore Settings Page.....	24



1

Getting Started

Introduction




The Motorola SURFboard® SVG6x82 Series Wireless Voice Gateway is a combination wireless cable modem and router with VoIP capabilities that provides wireless high-speed data and multimedia service access on your home network. The SVG6x82 includes a Wi-Fi Pairing option for quick and easy connections for your wireless devices.

This guide provides instructions for installing and configuring the SVG6x82, setting up a secure wireless network connection, and managing your gateway and network configurations.

In the Box

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

Table 1 – SVG6x82 Package Contents

ITEM	DESCRIPTION
Power Cord 	Provides power to the gateway through an electrical outlet connection
Ethernet Cable 	Standard Category 5, or higher, cable for connecting to the network
Software License & Regulatory Card 	Contains software license, warranty, and safety information for the gateway

System Requirements

- High-speed Internet access account
- Compatible operating systems:
 - o Windows® 8
 - o Windows Vista™, Service Pack 1 or later
 - o Windows 7
 - o Windows XP, Service Pack 2 or later
 - o Mac® 10.4 or higher
 - o UNIX®
 - o Linux®



Contact Information

For technical support and additional Motorola product information, please visit the Motorola Support website at www.motorola.com/us/support. Or call the following telephone number:

- Motorola Broadband Technical Support: **1-877-466-8646** (USA)

When you call, you will need the following information from the gateway product label located on the bottom of the gateway:

- Gateway model number (**SVG6582** or **SVG6682**)
- HFC MAC ID
- Gateway serial number (**S/N**)



2




Product Overview

Front Panel







Figure 1 – SVG6x82 Front View

Table 2 – SVG6x82 Front Panel LED Icons

BUTTON/LED ICON	FLASHING	ON
WPS button	Not applicable — no LED on button	Not applicable — no LED on button See Wi-Fi Protected Setup (WPS) for more information
 POWER	Not applicable — LED does not flash	Green: Power is properly connected
 RECEIVE	Scanning for a downstream (receive) channel connection	Green: Non-bonded downstream channel is connected Blue*: High-speed Internet connection with bonded downstream channels
 SEND	Scanning for an upstream (send) channel connection	Green: Non-bonded upstream channel is connected Blue*: High-speed Internet connection with bonded upstream channels



BUTTON/LED ICON	FLASHING	ON
 ONLINE	Scanning for an Internet connection	Green: Gateway is connected to the network
 WIRELESS	Not applicable — LED does not flash.	Green: 2.4 GHz wireless connection is made between the SVG6x82 and another Wi-Fi enabled device on your network — printer, tablet, laptop, etc. Amber: Turns ON during the wireless pairing process. LED turns green after five minutes.
 WIRELESS	This Wireless LED is available on the SVG6682 only Not applicable — LED does not flash.	Green: 5 GHz wireless connection is made between the SVG6682 and another Wi-Fi enabled device on your network — printer, tablet, laptop, etc. Amber: Turns ON during the wireless pairing process. LED turns green after five minutes.
 TELEPHONE	Green: Telephone is off-hook; dialing or call in progress	Green: Telephone is connected and activated; on-hook

*Indicates DOCSIS 3.0 operation (high-speed Internet access) which may not be available in all locations. Check with your service provider for availability in your area.

Note: To increase the bandwidth available for receiving and transmitting data, your service provider may implement bonded channels for RECEIVE and SEND channel connections.

Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) is a wireless network setup option that provides a quick and easy solution for setting up a secure wireless network connection for any WPS-enabled device; such as a computer or printer. WPS automatically configures your wireless network connections and sets up wireless security.



Rear Panel

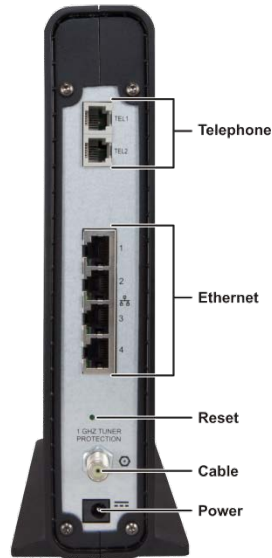





Figure 2 – SVG6x82 Rear View

Table 3 – SVG6x82 Rear Panel Ports & Connectors

PORT NAME	DESCRIPTION
TEL 1 TEL 2	<ul style="list-style-type: none"> • VoIP connection for a single or two-line telephone • VoIP connection for a single-line telephone
 1 2 3 4 ETHERNET	Four one-gigabit Ethernet ports for RJ-45 cable connections
RESET	If you experience a problem, you can push this recessed button to reset the gateway. Note: It may take from 5 to 30 minutes for the gateway to find and lock on the appropriate communications channels.
 CABLE	Coaxial cable connector
 POWER	+12VDC Power connector

Gateway Label

The SVG6x82 gateway product label is located on the bottom of the gateway. It contains unique gateway ID information that you may need when contacting your service provider.



To receive Internet access, you may have to provide the following information listed on the gateway label:

- Gateway model number (**SVG6582** or **SVG6682**)
- MAC address (**HFC MAC ID**)
- Gateway serial number (**S/N**)
- Wi-Fi Security Key

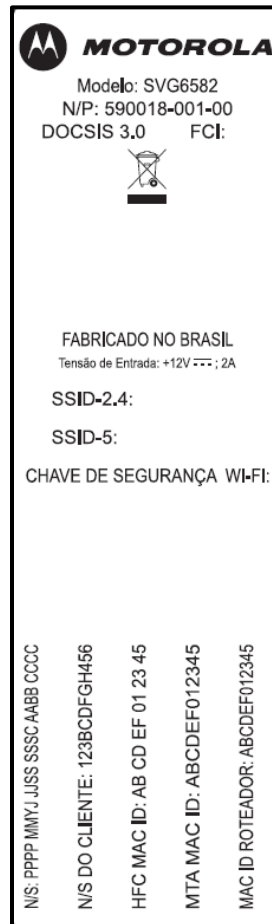


Figure 3 – Sample SVG6x82 Gateway Label



3

Installing the Gateway



- **This product is for indoor use only. Do not route the Ethernet cable outside of the building. Exposure of the cables to lightning could create a safety hazard and damage the product.**
- **Contact your cable service provider before connecting your gateway to existing telephone wiring. DO NOT connect the telephone cable from the TEL port to a traditional telephone (PSTN) service; only connect it to a telephone.**

Connecting to Your Computer

Before installing the SVG6x82:

- Check with your service provider to ensure high-speed Internet service is available in your area. A high-speed Internet connection provided by an Internet service provider is needed to set up a wireless network.
- Choose a central location in your home where your computer and gateway are preferably near existing cable and electrical wall outlets.
- Make sure your computer is powered OFF.

Note: The following procedure steps you through the wired Ethernet connection process to make sure the gateway is properly connected and your network access is working.

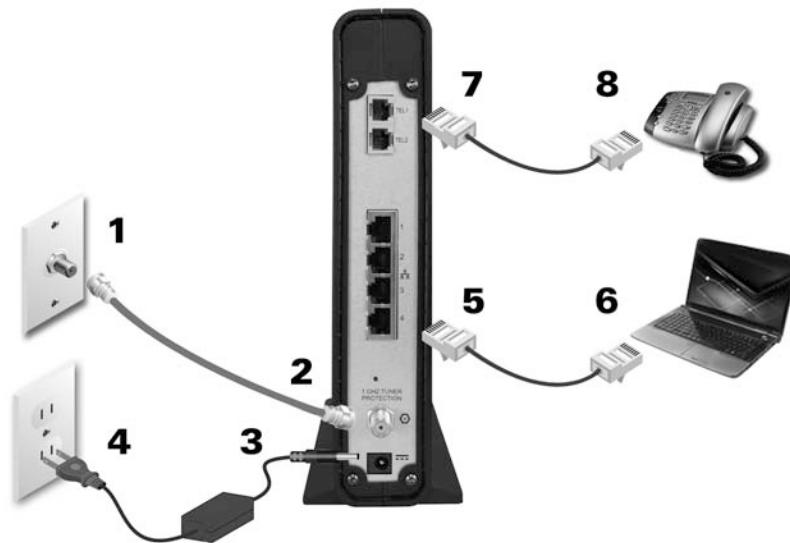


Figure 4 – SVG6x82 Connection Diagram

1. Check that a coaxial cable is connected to a cable wall outlet or RF splitter.
2. Connect the other end of the coaxial cable to the Cable connector on the gateway.
Hand-tighten the connectors to avoid damaging them.



3. Connect the Ethernet cable to any open Ethernet port on the gateway.
4. Connect the other end of the Ethernet cable to the Ethernet port on your computer.
Repeat steps 3 and 4 for each additional computer or other device.
5. Plug the telephone cord of a single- or two-line telephone into your telephone.
6. Plug the other end of the telephone cord into the TEL 1 port on the gateway.
7. Use the TEL 1 port to connect two-line telephones.
Note: *Contact a VoIP service provider to activate this service.*
8. For a second telephone, plug the telephone cord of a single-line telephone into the TEL 2 port on the gateway.
9. Plug the power cord into the Power port on the gateway.
10. Plug the other end of the power cord into an electrical wall outlet. This automatically powers ON the gateway.

Testing the Gateway Connections

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

1. Power ON your computer and then log on.
2. Check that all the LEDs on the front panel of the gateway first FLASH in sequential order and then light SOLID. See **Front Panel** for additional LED status information.
If an LED did not light SOLID, contact your service provider for assistance.
3. Contact your service provider to activate (provision) the gateway.
Note: *Your service provider may allow for automatic activation which will automatically launch a special website when you open a web browser.*
4. Once your gateway is provisioned, open a web browser on your computer, such as Internet Explorer, Firefox, Google Chrome, or Safari.
5. Type a valid URL (for example, www.motorola.com) in the address bar and then click or press **Enter**.

If the web page did not open, contact your service provider for assistance or proceed to **Connecting the Gateway to the Internet** to manually set up the network options on your computer.

Setting Up an Internet Connection

IMPORTANT! Your computer may already be configured to automatically connect to the Internet. If so, **do not** change the network options before contacting your service provider for assistance.

If you cannot access the Internet after completing the gateway installation, you may have to manually set up your computer to connect to the Internet. To do this, you will have to enable the network options on your computer to automatically obtain an IP address and DNS server address.

Please note, operating system-specific commands for configuring computer network options are not provided in this document.



The general steps provided below can be used for the following Microsoft Windows platforms:

- Windows 7
- Windows Vista
- Windows XP

For specific commands, refer to the documentation for the Windows operating system running on your computer for specific commands.

1. Click the **Start** button from the Taskbar on your desktop and then click **Control Panel** and **Network Connections**.

Note: *Additional selections may be necessary for Windows 7 systems.*

2. Step through to open the Local Area Connection Properties window.
3. Select **Internet Protocol (TCP/IP)** option and click **Properties** to open the Internet Protocol (TCP/IP) Properties window.
4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
5. Click **OK** to save the TCP/IP settings and close the Internet Protocol (TCP/IP) Properties window.
6. Step through to close the remaining windows and exit.
7. To verify the IP address, open a command prompt window using the **Start** button from the Taskbar on your desktop.
8. Type **ipconfig** and press **Enter** to display the IP configuration.
9. To renew the IP address, type **ipconfig /renew** and press **Enter**. A new IP address for your computer will display.
10. Type **exit** and then press **Enter** to return to Windows.

If you still cannot access the Internet, contact your service provider.



4

Setting Up a Wireless Network Connection

You must have computer access to a high-speed Internet service to set up a wireless network connection or connect wireless devices to the SVG6x82. Also, make sure the SVG6x82 and your computer are connected through an Ethernet connection. Choose one of the following two options to set up your wireless network connection:

- Setting Up a Wireless Network on Your Computer
- Using the WPS Pairing Button

After setting up your wireless network connection, check that the wireless network connection was set up properly. See [Testing Your Wireless Network Connection](#) for more information.

Setting Up a Wireless Network on Your Computer

Note: The steps for setting up a wireless network may differ slightly depending on the Windows operating system installed on your computer. The following steps apply for Windows 7 systems.

1. From the Windows taskbar, click **Start** button and then click **Control Panel, Network and Sharing Center**.
2. Click **Set up a new connection or network**.
3. Click **Connect to the Internet**.

Note: The **You are already connected to the Internet** message may appear. Ignore this message and proceed with the next step.

4. Click **Set up a new connection anyway** and then click **Wireless**.
5. Scroll down and click the **MOTOROLA** wireless network name (see the **SSID** number listed on the SVG6x82 gateway label).
6. Enter **Network security key code** in the Security key field (see **Wi-Fi Security** code listed on the SVG6x82 gateway label) and then click **OK** to complete the wireless network connection.
A Connected status message showing the wireless network connection should display.
7. Close the Wireless Network Connection window.

Using the WPS Pairing Button

Note: To use the WPS Pairing button option, your computer hardware must support WPS and also have WPA security compatibility.

The WPS option automatically assigns a random wireless network name (SSID) and Wi-Fi Security Key to the SVG6x82 and other WPS-enabled devices to connect to your wireless network.

1. Power ON the gateway and other WPS-enabled devices that you want to connect to a wireless network.
2. Press and hold the WPS button located on the top of the SVG6x82 for five or more seconds.
3. Press the WPS button on your WPS-enabled computer or other device.
4. Repeat step 3 for each additional WPS-enabled device you are connecting to your wireless network.



Testing Your Wireless Network Connection

Perform the following test to verify that the SVG6x82 and other wireless devices can connect to your wireless network:

1. If connected, disconnect the Ethernet cable from your computer and the SVG6x82.
2. Open a web browser on your computer.
3. Type a valid URL (for example, **www.motorola.com/us**) in the address bar, and then click or press **Enter**.

If the web page did not open, please contact your service provider for assistance.



5

Accessing the Gateway

Use the SVG6x82 Modem Web Manager to view the various configuration settings and operational status of the gateway.

Starting the Gateway Web Manager

Note: Use the following default username and password to log on to the SVG6x82 Web Manager for the first time. For network security purposes, it is recommended that you change the user name and password after logging on. See [Changing the Default Password](#) for more information.

1. Open any web browser on the computer connected to the SVG6x82.
2. In the Address bar, type **http://192.168.0.1** for the Gateway Web Manager IP address, and then press **Enter**. The gateway Login window displays.
3. Type the default username and password. Both entries are case-sensitive.

Username: **admin**

Password: **motorola**

Login

Login
Please enter username and password to login.

Username

Password

Figure 5 – SVG6x82 Login Window

4. Click **Login** to open the SVG6x82 Web Manager. The SVG6x82 Status Connection page displays.



Status

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

Startup Procedure

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

Downstream Bonded Channels

Channel	Lock Status	Modulation	Channel ID	Frequency	Power	SNR	Correctables	Uncorrectables
1	Locked	unknown	0	960500000 Hz	-12.2 dBmV	0.0 dB	0	0
2	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB	0	0
3	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB	0	0
4	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB	0	0
5	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB	0	0
6	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB	0	0
7	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB	0	0
8	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB	0	0

Upstream Bonded Channels

Channel	Lock Status	US Channel Type	Channel ID	Symbol Rate	Frequency	Power
1	Not Locked	Unknown	0	0 Ksym/sec	0 Hz	0.0 dBmV
2	Not Locked	Unknown	0	0 Ksym/sec	0 Hz	0.0 dBmV
3	Not Locked	Unknown	0	0 Ksym/sec	0 Hz	0.0 dBmV
4	Not Locked	Unknown	0	0 Ksym/sec	0 Hz	0.0 dBmV

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

Figure 6 – SVG6x82 Status Connection Page

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

The Status Connection page provides the following information relating to the SVG6x82 network connection:

- Downstream Bonded Channels – use lower cable frequencies to transmit data
- Upstream Bonded Channel – use higher cable frequencies to receive data

Note: Click **Refresh** (press **F5**) in your web browser any time you want to update the information on this page.



To prevent unauthorized access and configuration to your wireless network, it is recommended that you immediately change the default password after logging on to the gateway for the first time. See [Changing the Default User Name and Password](#) for more information.



Gateway Web Manager Menu Options

The SVG6x82 main menu options are displayed along the top of the SVG6x82 Web Manager page and the related submenu options are displayed along the left side of each menu page:



Figure 7 – SVG6x82 Main Menu Bar

Table 4 – SVG6x82 Main Menu

MENU OPTION	FUNCTION
Status	Provides information about the gateway hardware and software, MAC address, gateway IP address, serial number, and related information. Additional pages provide diagnostic tools and also allow you to change your gateway user name and password.
Basic	Views and configures the gateway IP-related configuration data, including Network Configuration, WAN Connection Type, DHCP, and DDNS
Advanced	Configures and monitors how the gateway routes IP traffic
Firewall	Configures and monitors the gateway firewall
Wireless	Configures and monitors the gateway wireless networking features
MTA	Monitors the telephone features of the gateway
Logout	Closes the SVG6x82 Configuration Web Manager

Getting Help

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

Exiting the SVG6x82 Web Manager

To log out and close the SVG6x82 Web Manager:

- Click **Logout** on the SVG6x82 Menu Options bar.



6

Protecting Your Wireless Network

After you have successfully connected the SGB7682 and your wireless devices, you should configure the gateway to protect your wireless network from unwanted and unauthorized access. Use the SVG6x82 web-based configuration manager to change various default configuration settings on the SVG6x82.

Note: If your gateway was obtained as part of a service package, your service provider may require alternative configuration methods. If you cannot access any of the HTML pages in the SVG6x82 Web Manager, please contact your service provider for assistance.

Changing the Default User Name and Password



To prevent unauthorized access and configuration to your wireless network, it is recommended that you immediately change the default password after logging on to the gateway for the first time.

The most important recommendation towards securing your wireless home network is to change the default administrator password on your SVG6x82 and other wireless devices as well.

To ensure that your wireless home network is secure, it is recommended that you follow these best practices:

- Always create a secure password that is not easily guessed
- Use phrases instead of names that may be easier for you to remember
- Use a combination of upper and lowercase letters, numbers, and symbols
- Continue to change your admin password on a regular basis

To change the default user name and password:

1. Log in to the SGB6782 from any web browser on your computer.
2. Type the Gateway Web Manager IP address, **http://192.168.0.1**, in the Address bar and then press **Enter**. The gateway Login window displays.
3. Type the default username and password as they appear below.
Username: **admin**
Password: **motorola**
4. Click **Login** to open the SVG6x82 Web Manager. The SVG6x82 Status Connection page displays.
5. Click **Security** from the Status submenu options on the left side of the page. The Status Security page displays.



Figure 8 – Status Security Page-Change User Name

6. Check that **Change Username** is displayed in the selection box.
7. Complete each field entry, but note the following:
 - o All fields (for example, Current Username & Password) are case-sensitive
 - o **Note:** For first-time logons, the Current Username is **admin**, Current Password is **motorola**
 - o Username is your current user name
 - o Make sure **No** is selected for **Restore Factory Defaults**.
8. Click **Apply** to update your user name.
9. Click **Change Username** drop-down arrow to display **Change Password**.

Figure 9 – Change User Password

10. Complete each field entry, but note the following:
 - o Username is the Current Username
 - o All fields are case-sensitive



- o Make sure **No** is selected for **Restore Factory Defaults**.
 - o Find a secure place to write down and keep your new password
11. Click **Apply** to update the password.

Setting Up the Firewall

You can use the Firewall pages to configure the SVG6x82 firewall filters and firewall alert notifications on your wireless network. The firewall protects the SVG6x82 LAN from undesired attacks and other intrusions from the Internet.

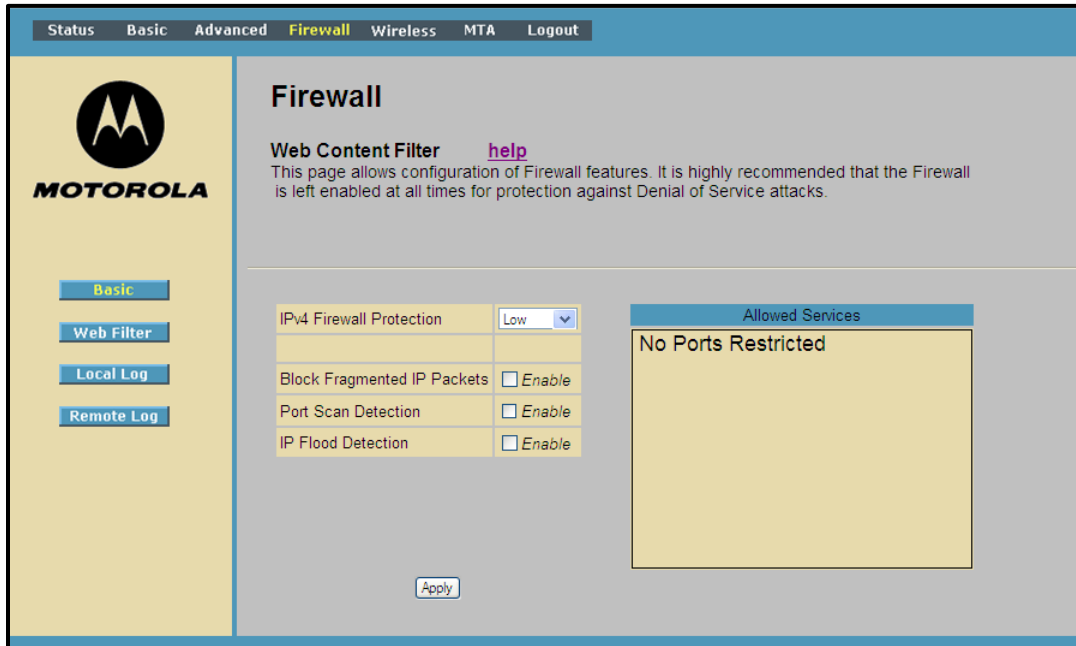


Figure 10 – Firewall Main Page

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 pages for improper packets and intrusion attempts.
- Provides comprehensive logging for all
 - o User authentications
 - o Rejected internal and external connection requests
 - o Session creation and termination
 - o Outside attacks (intrusion detection)

You can also configure the firewall filters to set rules for port usage.



Basic Firewall

The Web Content Filter page has various settings related to blocking or exclusively allowing different types of data through the CMRG from the WAN to the LAN. There are three security firewall protection levels (low, medium, and high) which correspond to the number of services allowed.

Firewall Protection turns ON the Stateful Packet Inspection (SPI) firewall features. Block Fragmented IP packets prevents all fragmented IP packets from passing through the firewall. Port Scan Detection detects and blocks port scan activity originating on both the LAN and WAN. IP Flood Detection detects and blocks packet floods originating on both the LAN and WAN.

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

To open the Firewall Basic Web Content Filter page:

1. Click **Firewall** on the SVG6x82 Menu Options bar.
2. Click **Basic** from the Status submenu options.

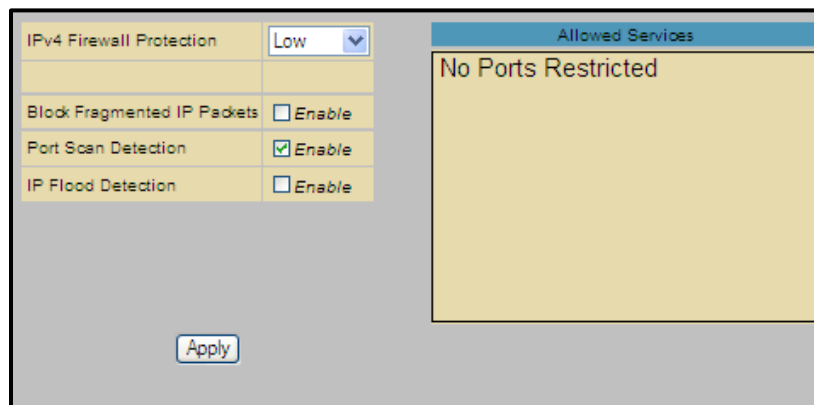


Figure 11 – Firewall Basic Web Content Filter Page

3. Click the Firewall Protection drop-down to select the protection level or turn OFF security protection.
 - o **High** - Safest configuration, highest security
 - o **Medium** - Common configuration, modest risk
 - o **Low** - Minimum security, higher risk
 - o **Off** - No security, highest risk
4. Click **Enable** for each Web filter you want to set for the firewall and then click **Apply**.

Firewall Web Filter

The Firewall web filter page allows you to filter outbound connections, restrict or grant access to specified MAC addresses. To open the Firewall Web Filtering page:

1. Click **Firewall** on the SVG6x82 Menu Options bar.
2. Click **Web Filter** from the Status submenu options.
3. Click **Create** and enter the information for each web filter you want to create.

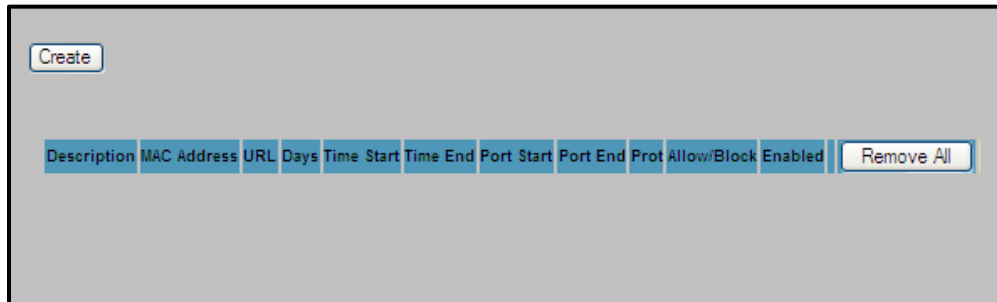


Figure 12 – Firewall Web Filtering Page

Firewall Local Log

You can set up email to enable automatic email alerts. The Local Event Log can send out firewall attack reports in two ways:

- Individual emails are sent out automatically each time the firewall is under attack
- A local log is stored within the gateway and displayed in table form on the Local Log page. Individual emails will now be sent to the specified address each time an attack is detected.

To open the Firewall Local Log page:

1. Click **Firewall** on the SVG6x82 Menu Options bar.
2. Click **Local Log** from the Status submenu options.

Figure 13 – Firewall Local Log Page

3. Enter your email address for the Contact Email Address field.
4. Enter the SMTP email account, user name, and password in the next fields.

Note: *The Outgoing mail server address is provided by your service provider.*
5. Select **Enable** checkbox if you want to receive firewall email alerts, and then click **Apply**.
6. Click **E-mail Log** to send a summary of the Event Log Table to the contact specified contact email address.
7. Click **Clear Log** to clear the table.



Firewall Remote Log

This Firewall configuration sends firewall attack reports to a standard SysLog server so that multiple instances can be logged over a period of time. You can select individual attack or configuration items to send to the SysLog server so that only the items of interest will be monitored. You can log any of the following:

- **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.
- **Known Internet attack types** - 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.

Note: The SysLog server must be on the same network as the Private LAN behind the Configuration Manager (typically **192.168.0.x**).

To open the Firewall Remote Log page:

1. Click **Firewall** on the SVG6x82 Menu Options bar.
2. Click **Remote Log** from the Status submenu options.

Send selected events

Permitted Connections

Blocked Connections

Known Internet Attacks

Product Configuration Events

to SysLog server at 192.168.0.

Apply

Figure 14 – Firewall Remote Log Page

3. Select all the desired event types that you want to monitor.
4. Enter the last byte (from **10** to **254**) of the IP address of the SysLog server.

Note: 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.

5. Click **Apply**.



Setting Up the DMZ Host

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. DMZ host lets you specify the default recipient of WAN traffic that NAT is unable to translate to a known local computer.

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

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.

To open the DMZ Host page:

1. Click **Advanced** on the SVG6x82 Menu Options bar.
2. Click **DMZ Host** from the Status submenu options.

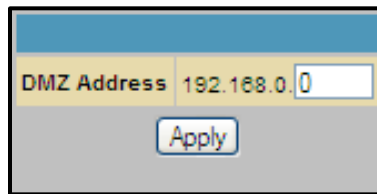


Figure 15 – Advanced DMZ Host Page

3. Enter the last byte (from **10** to **254**) of the IP address of the computer you want to set up as the DMZ host.
4. Click **Apply** to activate the selected computer.



7

Monitoring Your Network

Use the SVG6x82 Status pages to obtain information about the gateway hardware and software, MAC address, gateway IP address, serial number; and to monitor the gateway system connection.

Viewing the Gateway Software Information

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

To open the Status Software page:

1. Click **Status** on the SVG6x82 Menu Options bar.
2. Click **Software** from the Status submenu options.

Information	
Standard Specification Compliant	DOCSIS 3.0
Hardware Version	1
Software Version	SVG6X82-6.5.1.3145-ENG-00-301-DIAG
Cable Modem MAC Address	00:23:ed:6e:78:e6
Cable Modem Serial Number	380001220000284801010460
CM certificate	Installed
Status	
System Up Time	0 days 00h:12m:46s
Network Access	Denied
Cable Modem IP Address	---:---:---:---

Figure 16 – SVG6x82 Status Software Page

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



Viewing the Gateway Status

The Status Connection page displays information about the RF upstream and downstream channels, including downstream channel frequency, upstream channel ID, and upstream and downstream signal power and modulation.

This page also displays IP lease information, including the current IP address of the cable modem, the duration of both leases, the expiration time of both leases, and the current system time from the DOCSIS timeserver.

To open the Status Connection page:

1. Click **Status** on the SVG6x82 Menu Options bar.
2. Click **Connection** from the Status submenu options.

Status

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

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

Downstream Bonded Channels								
Channel	Lock Status	Modulation	Channel ID	Frequency	Power	SNR	Correctables	Uncorrectables
1	Locked	unknown	0	960500000 Hz	-12.2 dBmV	0.0 dB	0	0
2	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB	0	0
3	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB	0	0
4	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB	0	0
5	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB	0	0
6	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB	0	0
7	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB	0	0
8	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB	0	0

Upstream Bonded Channels						
Channel	Lock Status	US Channel Type	Channel ID	Symbol Rate	Frequency	Power
1	Not Locked	Unknown	0	0 Ksym/sec	0 Hz	0.0 dBmV
2	Not Locked	Unknown	0	0 Ksym/sec	0 Hz	0.0 dBmV
3	Not Locked	Unknown	0	0 Ksym/sec	0 Hz	0.0 dBmV
4	Not Locked	Unknown	0	0 Ksym/sec	0 Hz	0.0 dBmV

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

Figure 17 – SVG6x82 Status Connection Page



Backing up Your Gateway Configuration

You can save a back up copy of the current gateway configuration settings to your local computer. You can use the backup file to restore your custom configuration settings in the event that you made changes that you no longer want.

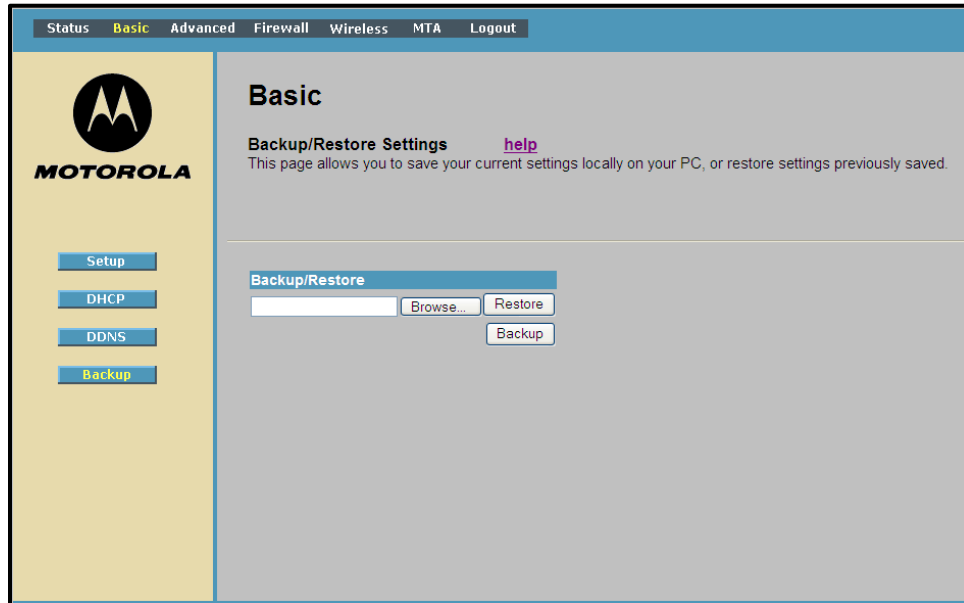


Figure 18 – SVG6x82 Basic Backup/Restore Settings Page

To create a back up copy of your gateway settings:

1. Click **Basic** on the SVG6x82 Menu Options bar.
2. Click **Backup** from the Basic submenu options.
3. Type the path and file name where you want to store the backup file on your computer, or click **Browse** to search for a location.
4. Click **Backup** to create a backup file of your SVG6x82 configuration settings.

Restoring Your Gateway Configuration

WARNING! This will delete all of your current gateway configuration settings.

You can restore a previously saved configuration setting (usually named **GatewaySettings.bin**, unless you renamed it before saving). If necessary, you can reset the SVG6x82 gateway configuration to its original factory settings.

If necessary, you can reset the SVG6x82 gateway configuration to its original factory settings.

1. Click **Basic** on the SVG6x82 Menu Options bar.
2. Type the path and file name where you want to store the backup file on your computer, or click **Browse** to search for the file.
3. Click **Restore**. The gateway will reboot when the settings are restored.



8

Troubleshooting

If the solutions listed in this section do not solve your problem, contact your service provider for assistance.

You may have to reset the SVG6x82 gateway configuration to its original factory settings if the gateway is not functioning properly.

Your service provider may ask for the status of the LEDs as described in [Front Panel LED Icons and Error Conditions](#).

Solutions

Table 5 – Troubleshooting Solutions








MODEM PROBLEM	POSSIBLE SOLUTION
POWER LED Icon is OFF	<ul style="list-style-type: none"> • Check the power connection to the gateway and electrical outlet. • Check that the electrical outlet is working (is the outlet controlled by a light switch?). <p>If so, disconnect and find another electrical outlet.</p>
Cannot Send or Receive Data	<ul style="list-style-type: none"> • Check each end of the coaxial cable connection on the gateway and cable outlet. Hand tighten, if necessary. • Check the Ethernet cable to make sure it is properly connected to the gateway and computer. • On the front panel, check the status of the LED icons and refer to Front Panel LED Icons and Error Conditions to identify the problem. • If you have cable television, check your television to ensure your cable service is operating properly. <p><i>Note: If none of the above solutions resolve the problem, contact your service provider for further assistance.</i></p>
WPS (Wi-Fi Pairing) is not working	<ul style="list-style-type: none"> • Check if WPS is enabled. <p>Open the SVG6x82 Gateway Web Manager, select Wireless on the menu bar and then select the Basic submenu option. If Disabled is set for Wireless, click the Wireless drop-down to select Enabled and then click Apply.</p>



Front Panel LED Icons and Error Conditions

The SVG6x82 front panel LED icons provide status information for the following error conditions:

Table 6 – Front Panel LED Icons and Error Conditions

LED ICON	STATUS	IF, DURING STARTUP:	IF, DURING NORMAL OPERATION
 POWER	OFF	Modem is not properly plugged into the electrical outlet	Modem is unplugged
 RECEIVE	FLASHING	Downstream receive channel cannot be acquired	Downstream channel is lost
 SEND	FLASHING	Upstream send channel cannot be acquired	Upstream channel is lost
 ONLINE	FLASHING	IP registration is unsuccessful	IP registration is lost
 WIRELESS	ON	No connected device is detected	Device is disconnected
 WIRELESS	ON	No connected device is detected	Device is disconnected
 TELEPHONE	OFF	No connected device is detected	Device is disconnected



Warranty Information

SURFboard SVG6x82 DOCSIS 3.0 Wireless Voice Gateway

Motorola Mobility, LLC (“Motorola”)

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

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

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

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

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

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



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

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



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

<http://www.motorola.com>

590934-001-a 05/2013

