

User Guide

SBG940 *Wireless Cable Modem Gateway*





WARNING: TO PREVENT FIRE OR SHOCK HAZARD, DO NOT EXPOSE THIS PRODUCT TO RAIN OR MOISTURE. THE UNIT MUST NOT BE EXPOSED TO DRIPPING OR SPLASHING. DO NOT PLACE OBJECTS FILLED WITH LIQUIDS, SUCH AS VASES, ON THE UNIT.

CAUTION: TO PREVENT ELECTRIC SHOCK, THIS EQUIPMENT MAY REQUIRE A GROUNDING CONDUCTOR IN THE LINE CORD. CONNECT THE UNIT TO A GROUNDING TYPE AC WALL OUTLET USING THE POWER CORD SUPPLIED WITH THE UNIT.

CAUTION: THIS PRODUCT WAS QUALIFIED UNDER TEST CONDITIONS THAT INCLUDED THE USE OF THE SUPPLIED CABLES BETWEEN SYSTEMS COMPONENTS. TO ENSURE REGULATORY AND SAFETY COMPLIANCE, USE ONLY THE PROVIDED POWER AND INTERFACE CABLES AND INSTALL THEM PROPERLY.

CAUTION: 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 PRODUCT SAFETY REQUIREMENTS OF THE COUNTRY OF USE.

CAUTION: INSTALLATION OF THIS PRODUCT MUST BE IN ACCORDANCE WITH NATIONAL WIRING CODES AND CONFORM TO LOCAL REGULATIONS.

CAUTION: DO NOT OPEN THE UNIT. DO NOT PERFORM ANY SERVICING OTHER THAN THAT CONTAINED IN THE INSTALLATION AND TROUBLESHOOTING INSTRUCTIONS. REFER ALL SERVICING TO QUALIFIED SERVICE PERSONNEL.

CAUTION: CHANGES AND MODIFICATIONS NOT EXPRESSLY APPROVED BY MOTOROLA FOR COMPLIANCE COULD VOID USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

When using this device, 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 equipment. 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 comes with the product.
- Comply with all warning and caution statements in the instructions. Observe all warning and caution symbols that are affixed to this equipment.
- Comply with all instructions that accompany this equipment.
- 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 product.
- Place this equipment in a location that is close enough to an electrical outlet to accommodate the length of the power cord.
- Place unit 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, other outlet unless the plug can be fully inserted with no part of the blades exposed.
- Place this equipment on a stable surface.



- Postpone cable modem installation until there is no risk of thunderstorm or lightning activity in the area.
- *Avoid using this product during an electrical storm.* There may be a risk of electric shock from lightning. For added protection for this product during a lightning storm, or when it is left unattended and unused for long periods of time, unplug it from the wall outlet, and disconnect the cable system. This will prevent damage to the product due to lightning and power surges.
- 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 equipment by local lightning strikes and other electrical surges.
- 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 unit with a clean, dry cloth. Never use cleaning fluid or similar chemicals. Do not spray cleaners directly on the unit or use forced air to remove dust.
- 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 re-connecting USB or Ethernet cable from the cable modem or the user's PC.
- Operate this product only from the type of power source indicated on the product's marking label. If you are not sure of the type of power supplied to your home, consult your dealer or local power company.
- Upon completion of any service or repairs to this product, ask the service technician to perform safety checks to determine that the product is in safe operating condition.

Be sure that the outside cable system is grounded, so as to provide some protection against voltage surges and built-up static charges. Article 820-20 of the NEC (Section 54, Part I of the Canadian Electrical Code) provides guidelines for proper grounding and, in particular, specifies the CATV cable ground shall be connected in the grounding system of the building, as close to the point of cable entry as practical.

Apparaten skall anslutas till jordat uttag när den ansluts ett näverk.

FCC Compliance Class B Digital Device

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.

Note: 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 installation. 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 equipment 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 equipment 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.



FCC Certification

This product contains a radio transmitter and accordingly has been certified as compliant with 47 CFR Part 15 of the FCC Rules for intentional radiators. Products that contain a radio transmitter are labeled with FCC ID and the FCC logo.

CAUTION: Exposure to Radio Frequency Radiation.

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).

Canada - Industry Canada (IC)

The wireless radio of this device complies with RSS 210 and RSS 102 of Industry Canada.

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

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

To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

Only use the antenna(s) provided with this product or an antenna approved by Motorola.

Regulatory, Safety, Software License, and Warranty Information Card

This product is provided with a separate *Regulatory, Safety, Software License, and Warranty Information* card. If one is not provided with this product, please ask your service provider or point-of-purchase representative, as the case may be.

- THIS PRODUCT IS IN COMPLIANCE WITH ONE OR MORE OF THE STANDARDS LISTED ON THE *REGULATORY, SAFETY, SOFTWARE LICENSE, AND WARRANTY INFORMATION CARD*. NOT ALL STANDARDS APPLY TO ALL MODELS.
- NO WARRANTIES OF ANY KIND ARE PROVIDED BY MOTOROLA WITH RESPECT TO THIS PRODUCT, EXCEPT AS STATED ON THE *REGULATORY, SAFETY, SOFTWARE LICENSE, AND WARRANTY INFORMATION CARD*. MOTOROLA'S WARRANTIES DO NOT APPLY TO PRODUCT THAT HAS BEEN REFURBISHED OR REISSUED BY YOUR SERVICE PROVIDER.

Copyright © 2004 by 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 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, either 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.

MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. Microsoft, Windows, Windows Me, Windows NT, and Xbox are registered trademarks and Windows XP and Xbox Live are trademarks of Microsoft Corporation. Microsoft Windows screen shots are used by permission of Microsoft Corporation. Macintosh and AppleTalk are registered trademarks of Apple Computer, Inc. Iomega is a registered trademark of Iomega Corporation. Linux is a registered trademark of Linus Torvalds. Acrobat Reader is a registered trademark of Adobe Systems, Inc. Netscape and Navigator are registered trademarks of Netscape Communications Corporation. PlayStation is a registered trademark of Sony Computer Entertainment Inc. UNIX is a registered trademark of the Open Group in the United States and other countries. Wi-Fi is a registered trademark of the Wi-Fi Alliance. All other product or service names are the property of their respective owners.



Contents

Overview	1	Setting the Firewall Policy	30
Easy Setup	2	Firewall > POLICY — advanced Page	32
Network Connection Types	2	Firewall > ALERT — basic Page	34
Powerful Features in a Single Unit	2	Firewall > ALERT — email Page	35
Sample Hybrid LAN	3	Firewall > LOGS Page	36
Optional Accessories	4	Gaming Configuration Guidelines	37
Front Panel	5	Configuring the Firewall for Gaming	37
Rear Panel	6	Configuring Port Triggers	37
Label on the Bottom of the SBG940	7	Configuring a Gaming DMZ Host	38
SBG940 LAN Choices	7	Configuring the Gateway	39
Wireless LAN	8	Gateway > STATUS Page	40
Wired Ethernet LAN	9	Gateway > WAN Page	41
USB Connection	11	Gateway > LAN — nat config Page	43
Security	12	Gateway > LAN — dhcp server config Page	44
Firewall	12	Gateway > LAN — dhcp leases Page	45
DMZ	13	Gateway > PORT FORWARDING — status Page ...	46
Port Triggering	13	Gateway > PORT FORWARDING — config Page ...	47
Wireless Security	13	Gateway > PORT TRIGGERS — predefined Page ..	48
Port Forwarding	14	Gateway > PORT TRIGGERS — custom Page	50
Virtual Private Networks	14	Gateway > LOG Page	51
Related Documentation	14	Configuring TCP/IP	52
Installation	15	Configuring TCP/IP in Windows 95, Windows 98, or	
Before You Begin	15	Windows Me	52
Precautions	16	Configuring TCP/IP in Windows 2000	55
Signing Up for Service	16	Configuring TCP/IP in Windows XP	59
Computer System Requirements	17	Verifying the IP Address in Windows 95, Windows 98,	
Connecting the SBG940 to the Cable System	18	or Windows Me	63
Cabling the LAN	18	Verifying the IP Address in Windows 2000 or Windows XP	64
Obtaining an IP Address for Ethernet	19	Setting Up Your Wireless LAN	66
Obtaining an IP Address in Windows 98,		Encrypting Wireless LAN Transmissions	67
Windows 98 SE, or Windows Me	19	Configuring WPA on the SBG940	68
Obtaining an IP Address in Windows 2000 or		Configuring WEP on the SBG940	70
Windows XP	19	Restricting Wireless LAN Access	72
Obtaining an IP Address on Macintosh or UNIX		Configuring the Wireless Network Name on the	
Systems	19	SBG940	73
Connecting a PC to the USB Port	20	Configuring a MAC Access Control List on the SBG940	75
Wall Mounting	21	Configuring the Wireless Clients	76
Wall Mounting Template	23	Configuring a Wireless Client for WPA	77
Basic Configuration	24	Configuring a Wireless Client for WEP	77
Starting the SBG940 Setup Program	25	Configuring a Wireless Client with the Network Name	
Changing the Default Password	27	(ESSID)	77
Enabling Remote Access	28		
Getting Help	29		



Wireless Pages in the SBG940 Setup Program	78
Wireless > STATUS Page	79
Wireless > NETWORK Page	80
Wireless > SECURITY — basic Page	82
Wireless > SECURITY — advanced Page	83
Wireless > STATISTICS page	84

Setting Up a USB Driver 86

Setting Up a USB Driver in Windows 98	87
Setting Up a USB Driver in Windows 2000	91
Setting Up a USB Driver in Windows Me	94
Setting Up a USB Driver in Windows XP	95
Removing the USB Driver from Windows 98 or Windows Me	96
Removing the USB Driver from Windows 2000	98
Removing the USB Driver from Windows XP	100
Running the Motorola USB Driver Removal Utility . . .	104

Troubleshooting 106

Front-Panel Lights and Error Conditions	107
---	-----

Contact Us 108

Frequently-Asked Questions 109

Specifications 111

Glossary 113

Software License 131

Overview

Thank you for purchasing a Motorola® SURFboard® Wireless Cable Modem Gateway SBG940 for your home, home office, or small business/enterprise. Applications where the SURFboard Gateway (SBG) is especially useful include:

- Households having multiple computers requiring connection to the Internet and each other
- Small businesses or home offices requiring fast, affordable, and secure Internet access
- Internet gamers desiring easier setup for:
 - Programs such as DirectX® 7 or DirectX® 8
 - Sites such as MSN Games by [Zone.com](#) or [Battle.net®](#)
- Video conferencing



The features and physical appearance of your SBG940 may differ slightly from the picture.

A home network enables you to share information between two or more computers. You can connect your home network to the Internet through the cable TV system. The SBG940 is the *central connection point* between your computers and the Internet. It directs (routes) information between the computers connected to your home network. A built-in cable modem transmits information between your home network and the Internet. An SBG940:

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

This product is subject to change. Not all features described in this guide are available on all SBG940 models.

For the most recent documentation, visit the [Cable Modems and Gateways](#) page on the Motorola Broadband website <http://broadband.motorola.com/>.



Easy Setup

It is much easier to configure a local area network (LAN) using an SBG940 than using traditional networking equipment:

- For basic operation, most default settings require no modification.
- The Setup Program provides a graphical user interface (GUI) for easy configuration of necessary wireless, Ethernet, router, DHCP, and security settings. For information about using the Setup Program, see "[Basic Configuration](#)".

Network Connection Types

The SBG940 provides different network connection types for your computers to exchange data. The connection between your computers and the SBG940 may be with a wireless or a wired connection or a combination of the two. Your network can use one or any combination of all the following network connections:

- Ethernet local area network (LAN)
- Wireless LAN (IEEE 802.11g that also supports IEEE 802.11b wireless clients)
- Universal Serial Bus (USB)

Powerful Features in a Single Unit

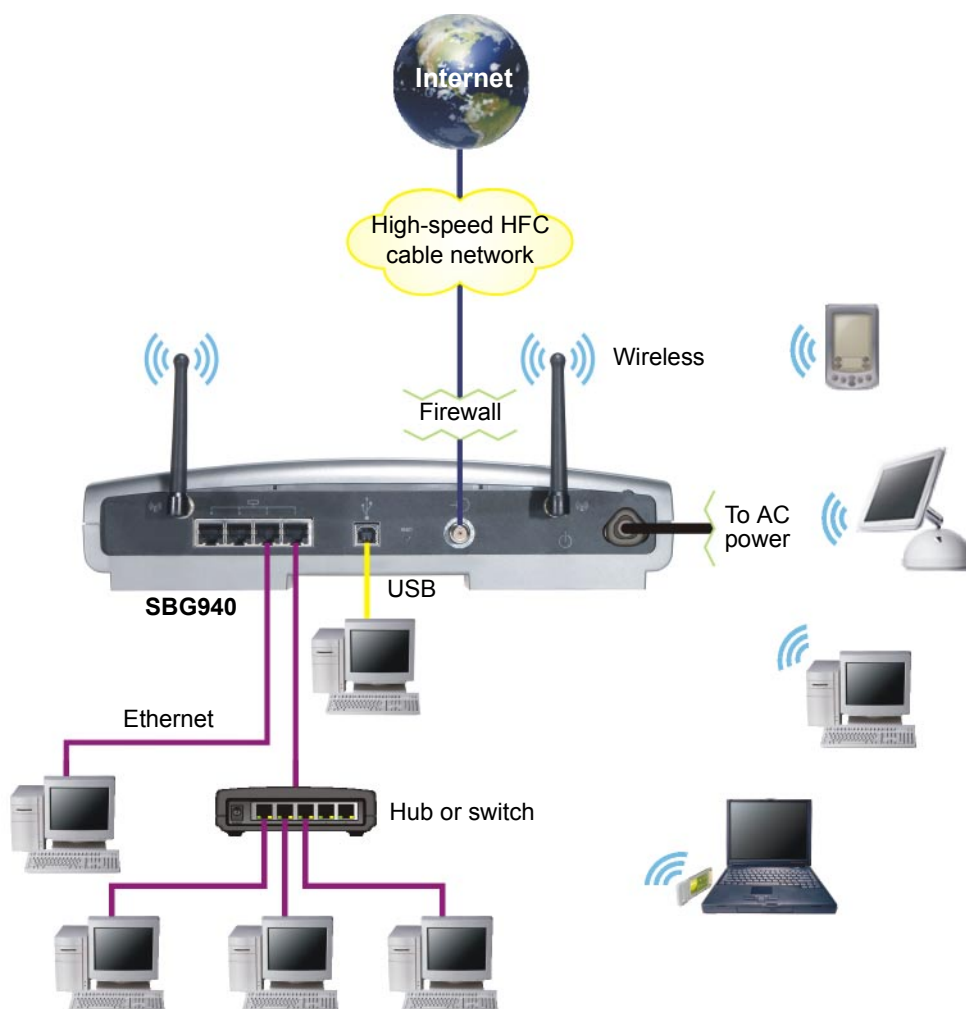
An SBG940 combines high-speed Internet access, networking, and computer security for a home or small-office LAN. An SBG940 provides:

- An integrated high-speed SURFboard cable modem for continuous broadband access to the Internet and other online services, with much faster data transfer than traditional dial-up or ISDN modems
- A single broadband connection for up to 253 computers to surf the web; all computers on the LAN communicate as if they were connected to the same physical network
- An [IEEE 802.11g](#) wireless access point to enable laptop users to remain connected while moving around the home or small office or to connect desktop computers without installing network wiring. Depending on distance, wireless connection speeds can match that of Ethernet.
- A USB connection for a single PC
- Four 10/100Base-T Ethernet uplink ports supporting half- or [full-duplex](#) connections and [Auto-MDIX](#)
- [Routing](#) for a wireless LAN (WLAN) or a wired Ethernet LAN; you can connect more than four computers using hubs and/or switches
- A built-in DHCP server to easily configure a combined wired and/or wireless Class C private LAN
- An advanced [firewall](#) supporting [stateful-inspection](#), intrusion detection, [DMZ](#), denial-of-service attack prevention, and Network Address Translation (NAT)
- Virtual private network (VPN) [pass-through](#) operation supporting IPSec, PPTP, or L2TP to securely connect remote computers over the Internet
- [Port Forwarding](#) to configure ports to run applications having special network requirements

Sample Hybrid LAN

The sample LAN illustrated on this page contains the following devices, all protected by the SBG940 firewall. Clockwise from top-right, the devices are:

- A PDA on a wireless connection
- One desktop Apple Macintosh® computer on a wireless connection
- One desktop PC on a wireless connection using a Motorola [Wireless PCI Adapter](#)
- A laptop PC on a wireless connection using a Motorola [Wireless Notebook Adapter](#)
- One PC connected to the USB port
- Three computers connected to Ethernet port one using a hub or switch
- One computer connected directly to Ethernet port two



Optional Accessories

All networks are composed of multiple devices. The SBG940 works with any IEEE 802.11g or IEEE 802.11b compliant client product. Motorola supplies a range of accessories for use with the SBG940. Some examples are:



Wireless Ethernet
Bridge WE800G



Ethernet Broadband
Router BR700



Wireless Notebook
Adapter WN825G



Wireless USB
Adapter WU830G



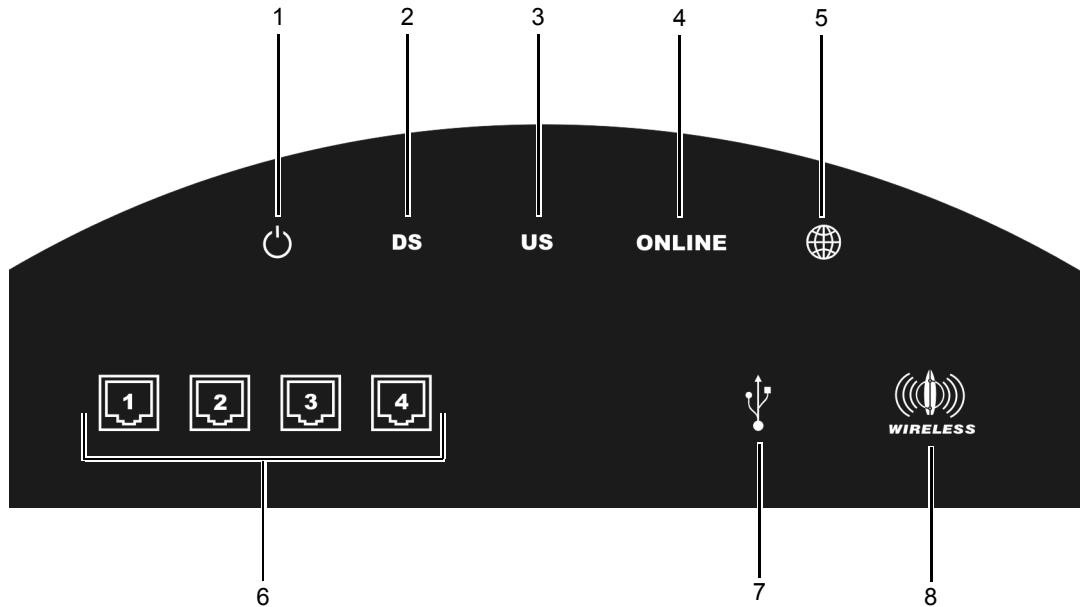
Wireless PCI Adapter
WPCI810G

For up-to-date information about accessories and home networking options, including product documentation, visit the Motorola Home Networking page http://broadband.motorola.com/consumers/home_networking.asp.



Front Panel

The front panel provides indicator lights. The display is dark unless there is a connection or activity on an interface:



Key Light Flashing

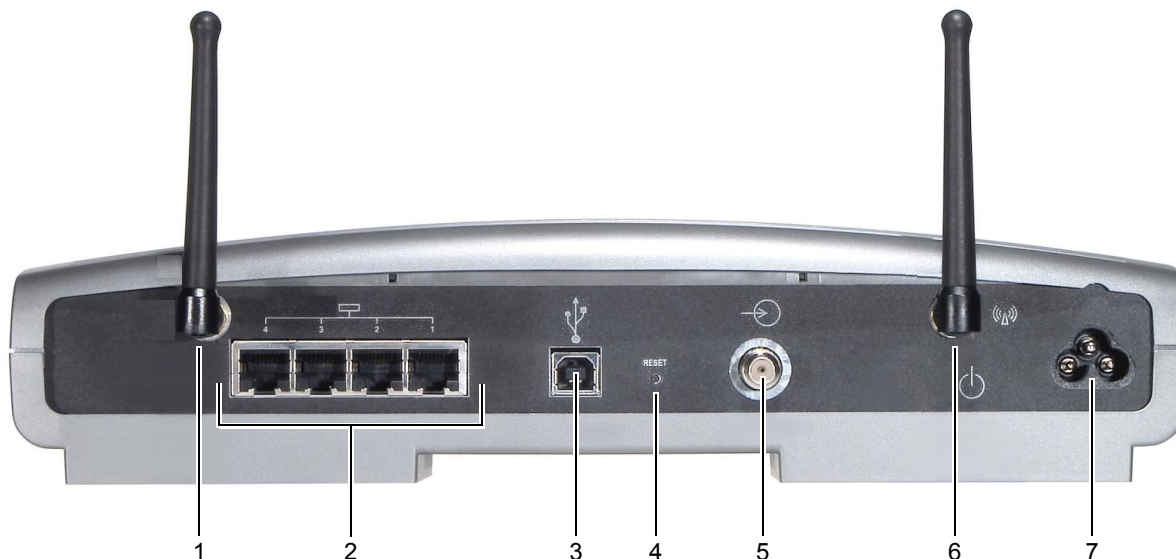
1		Never flashes
2	DS	Scanning for a receive (downstream) channel connection
3	US	Scanning for a send (upstream) channel connection
4	ONLINE	Scanning for a network connection
5		Transmitting or receiving data over the Internet
6		Ethernet activity on the port (1 to 4)
7		USB activity
8		Wireless activity

On






The AC power is connected properly
The downstream channel is connected
The upstream channel is connected
The startup process is complete and the SBG940 is online
Is never lit solid
There is a connection to the port (1 to 4): <ul style="list-style-type: none"> • Green for 100Base-T • Yellow for 10Base-T
Lights green if there is a proper USB connection
The wireless interface is on (Enable Wireless Interface is selected on the Wireless > NETWORK Page in the SBG940 Setup Program)

Rear Panel

The rear panel provides cabling connectors, status lights, and the power receptacle:



Key Item Description

- | | | |
|---|---|---|
| 1 | | An adjustable, but non-removable antenna. <i>Do not attempt to force this antenna off the unit.</i> |
| 2 |  | Use any Ethernet port to connect an Ethernet LAN cable with RJ-45 connectors to an Ethernet-equipped computer, hub, bridge, switch or Xbox or PlayStation® 2 gaming console. |
| 3 |  | For Windows <i>only</i> , use the USB port for Connecting a PC to the USB Port . You cannot connect the SBG940 USB port to a Macintosh or UNIX® computer. |
| 4 | RESET | If you experience a problem, you can push this recessed button to restart the SBG940 (see "Troubleshooting"). To reset all values to their defaults, hold down the button for more than five seconds. Resetting may take 5 to 30 minutes because the SBG940 must find and lock on the appropriate communications channels. |
| 5 |  | Use the cable connector to connect to the coaxial cable outlet. |
| 6 |  | Removable, adjustable antenna. If necessary, contact your cable provider about obtaining an optional Motorola wireless high gain antenna to increase WLAN performance and coverage. |
| 7 |  | Use the AC connector to connect to the AC power outlet. |



Label on the Bottom of the SBG940

To receive data service, you need to provide the [MAC address](#) marked **HFC MAC ID** to your cable provider:

```
CUSTOMER SN: BCDEFGHIJKL
||||| _____ |||||
SN: PPPPMYYJJSSSSCAABCCCC
||||| _____ |||||
HFC MAC ID: ABCDEF012345  _____ HFC MAC ID
||||| _____ |||||
USB CPE MAC ID: ABCDEF012345
||||| _____ |||||
GATEWAY MGMT MAC ID: ABCDEF012345
||||| _____ |||||
```

SBG940 LAN Choices

The SBG940 enables you to connect up to 253 [client](#) computers on a combination of:

- [Wireless LAN](#)
- [Wired Ethernet LAN](#)
- [USB Connection](#)

Each computer needs appropriate network [adapter](#) hardware and [driver](#) software. The clients on the Ethernet, wireless, or USB interfaces can share:

- Internet access with a single cable provider account, subject to cable provider terms and conditions
- Files, printers, storage devices, multi-user software applications, games, and video conferencing

Wireless and wired network connections use Windows networking to share files and peripheral devices such as printers, CD-ROM drives, floppy disk drives, and Iomega® Zip Drives.

Wireless LAN

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

Each computer on a WLAN requires a wireless adapter shown in “[Optional Accessories](#)”:

Laptop PCs Use a Motorola [Wireless Notebook Adapter](#) or compatible product in the PCMCIA slot.

Desktop PCs Use a Motorola [Wireless PCI Adapter](#), Wireless USB Adapter, or compatible product in the PCI slot or USB port, respectively.

Sample wireless network connections



To set up the SBG940, on a computer wired to the SBG940 over Ethernet or USB, perform the procedures in “[Setting Up Your Wireless LAN](#)”. *Do not attempt to configure the SBG940 over a wireless connection.*

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

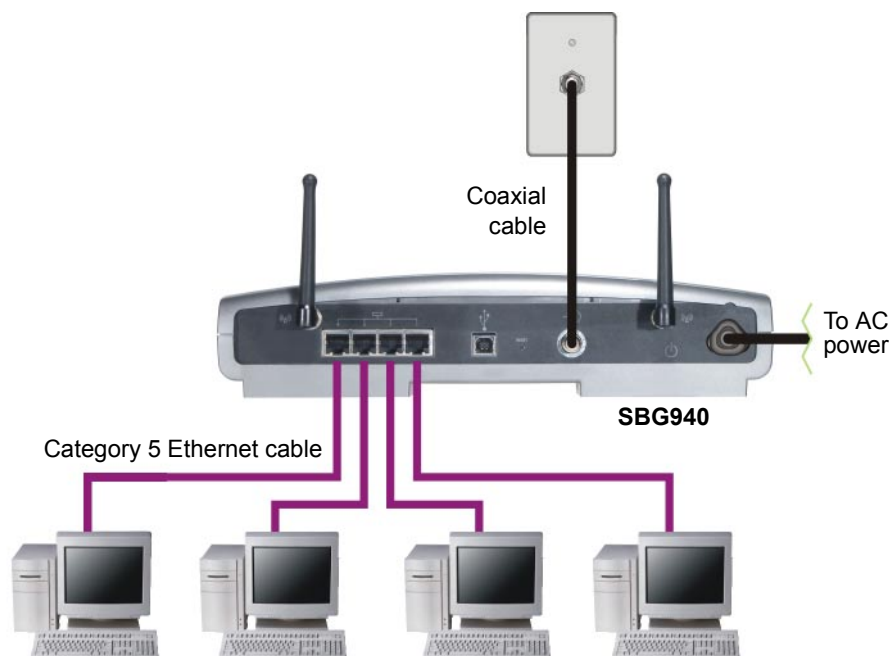
An optional Motorola high [gain](#) antenna can improve wireless performance. For information about available optional antennas for your SBG940, contact your cable provider.

Wired Ethernet LAN

Each computer on the 10/100Base-T Ethernet LAN requires an Ethernet network interface card (NIC) and driver software installed. Because the SBG940 Ethernet port supports [auto-MDIX](#), you can use straight-through or cross-over cable to connect a hub, switch, or computer. Use category 5 cabling for all Ethernet connections.

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

Sample Ethernet to computer connection

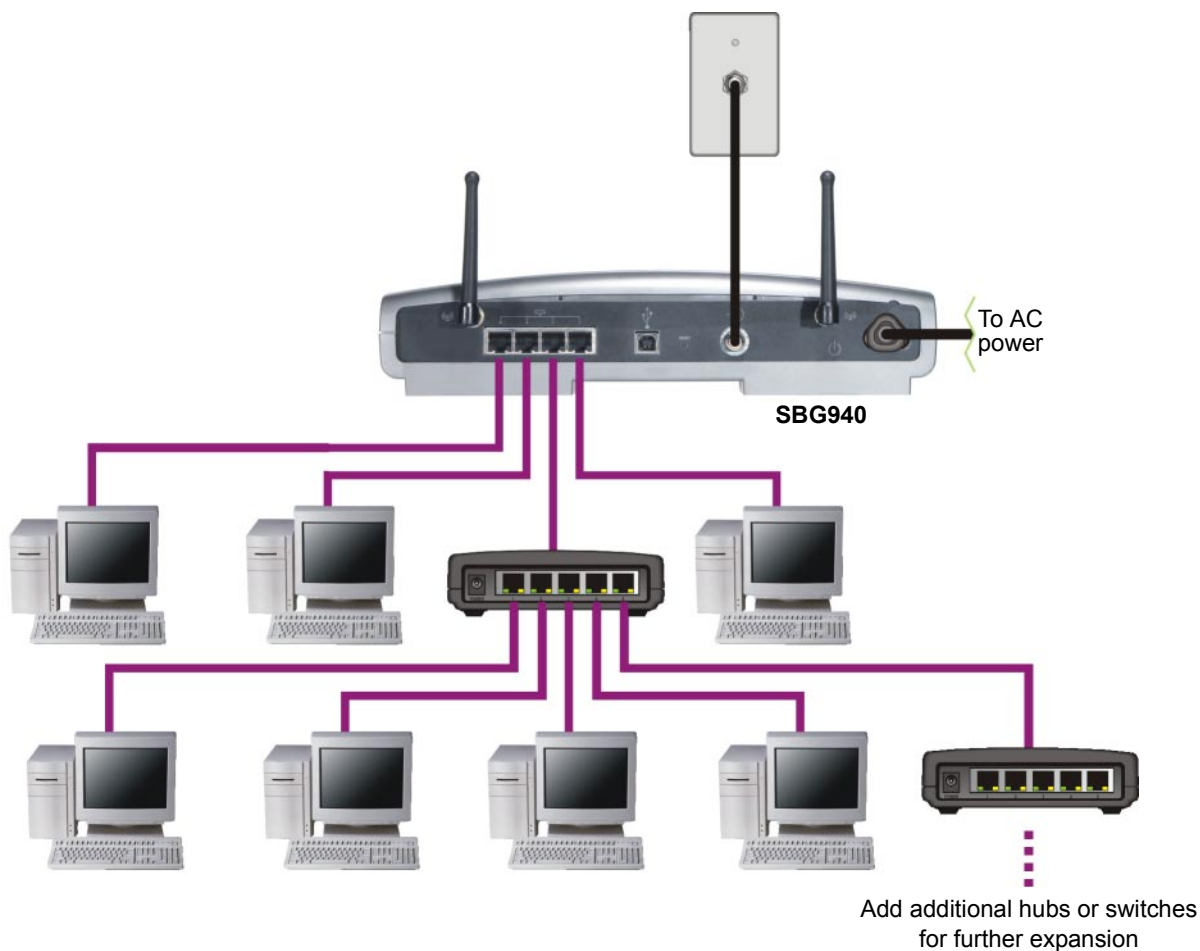


A wired Ethernet LAN with more than four computers requires one or more [hubs, switches, or routers](#). You can:

- Connect a hub or switch to any Ethernet port on the SBG940
- Use Ethernet hubs, switches, or routers to connect up to 253 computers to the SBG940

The following illustration is an example of an Ethernet LAN you can set up using the SBG940. Cable the LAN in an appropriate manner for the site. A complete discussion of Ethernet cabling is beyond the scope of this document.

Sample Ethernet connection to hubs or switches



USB Connection

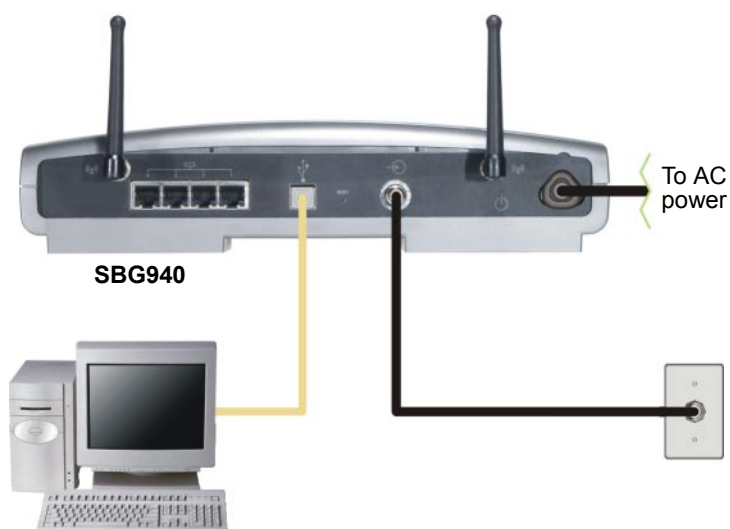
You can connect a single PC running Windows® 98, Windows XP™, Windows Me®, or Windows® 2000 to the SBG940 USB V1.1 port. For cabling instructions, see “[Connecting a PC to the USB Port](#)”.

Caution!



Before plugging in the USB cable, be sure the SBG940 Installation CD-ROM is inserted in the PC CD-ROM drive.

Sample USB connection





Security

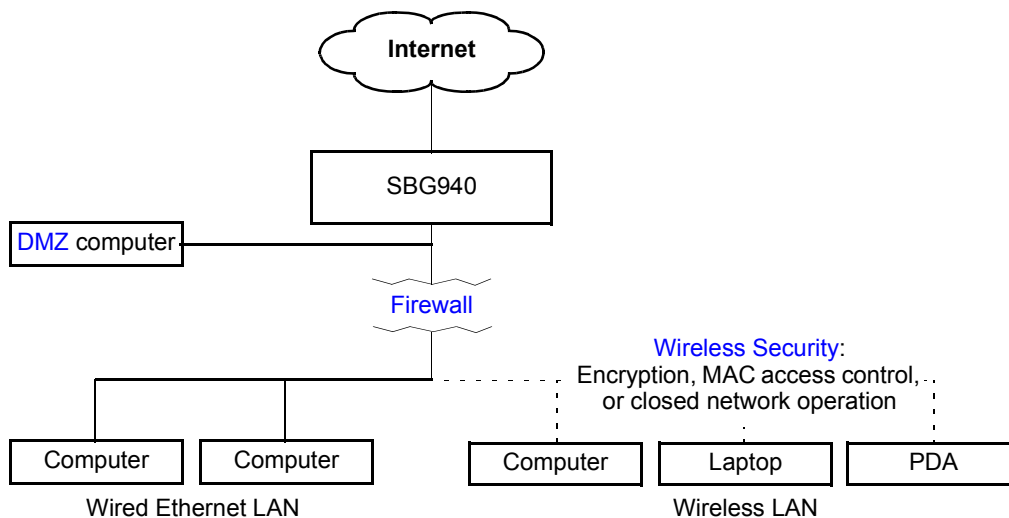
The SBG940 provides:

- A [firewall](#) to protect the SBG940 LAN from undesired attacks over the Internet
- For wireless transmissions, data encryption and network access control

Network Address Translation ([NAT](#)) provides some security because the IP addresses of SBG940 LAN computers are not visible on the Internet.

This diagram does not necessarily correspond to the network cabling. A full discussion of network security is beyond the scope of this document.

SBG940 security measures shown in a logical network diagram



Firewall

The SBG940 firewall protects the SBG940 LAN from undesired attacks and other intrusions from the Internet. It provides an advanced integrated [stateful-inspection](#) firewall supporting intrusion detection, session tracking, and denial-of-service attack prevention. The firewall:

- Maintains state data for every [TCP/IP](#) session on the [OSI](#) network and transport layers
- Monitors all incoming and outgoing [packets](#), applies the firewall policy to each one, and screens for improper packets and intrusion attempts
- Provides comprehensive logging for all:
 - User authentications
 - Rejected internal and external connection requests
 - Session creation and termination
 - Outside attacks (intrusion detection)

You can configure the firewall filters to set rules for port usage. For information about choosing a predefined firewall policy template, see "[Setting the Firewall Policy](#)".



DMZ

A de-militarized zone ([DMZ](#)) is one or more computers logically located outside the firewall between an SBG940 LAN and the Internet. A DMZ prevents direct access by outside users to private data.

For example, you can set up a web server on a DMZ computer to enable outside users to access your website without exposing confidential data on your network.

A DMZ can also be useful to play interactive games that may have a problem running through a firewall. You can leave a computer used for gaming *only* exposed to the Internet while protecting the rest of your network. For more information, see “[Gaming Configuration Guidelines](#)”.

Port Triggering

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

- The SBG940 has preconfigured port triggers for common applications.
- If needed, you can configure additional port triggers on the [Gateway > PORT TRIGGERS — custom Page](#).

Wireless Security

Because WLAN data is transmitted using radio signals, it may be possible an unauthorized person to access your WLAN unless you prevent them from doing so. *To prevent unauthorized eavesdropping of data transmitted over your LAN, you must enable wireless security. The default SBG940 settings neither provide security for transmitted data nor protect network data from unauthorized intrusions.*

The SBG940 provides the following wireless security measures, which are described in “[Setting Up Your Wireless LAN](#)”:

- To prevent unauthorized eavesdropping, you must encrypt data transmitted over the wireless interface using one of:
 - If all of your wireless clients support Wi-Fi® Protected Access (WPA) encryption, we recommend using WPA (see “[Configuring WPA on the SBG940](#)” and “[Configuring a Wireless Client for WPA](#)”).
 - Otherwise, configure a Wired Equivalency Privacy (WEP) key on the SBG940 and each WLAN client (see “[Configuring WEP on the SBG940](#)” and “[Configuring a Wireless Client for WEP](#)”).
- To protect LAN data from unauthorized intrusions, you can restrict WLAN access to computers having one or both of:
 - Known MAC addresses (see “[Configuring a MAC Access Control List on the SBG940](#)”)
 - The same unique network name (ESSID) as the SBG940 (see “[Configuring the Wireless Network Name on the SBG940](#)” and “[Configuring a Wireless Client with the Network Name \(ESSID\)](#)”)

Restricting access to computers having the same network name is also called “disabling ESSID broadcasting” or “enabling closed network operation.”

Port Forwarding

The SBG940 opens logical data ports when a computer on its LAN sends data, such as e-mail messages or web data, to the Internet. A logical data port is different from a physical port, such as an Ethernet port. Data from a protocol must go through certain data ports.

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

To configure port forwarding, you must specify an inbound (source) port or range of ports. The inbound port opens only when data is sent to the inbound port and closes again after a specified time elapses with no data sent to it. You can configure up to 32 port forwarding entries using the [Gateway > PORT FORWARDING — config Page](#).

Virtual Private Networks

The SBG940 supports multiple [tunnel](#) VPN [pass-through](#) operation to securely connect remote computers over the Internet. The SBG940:

- Is compatible with Point to Point Tunneling Protocol ([PPTP](#)) and Layer 2 Tunneling Protocol ([L2TP](#))
- Is fully interoperable with any [IPSec](#) client or gateway and [ANX](#) certified IPSec stacks

Related Documentation

The *SBG940 Quick Installation Guide* also provides information about using the SBG940.

For information about and documentation for Motorola home-networking products, visit the Motorola Home Networking page http://broadband.motorola.com/consumers/home_networking.asp.



Installation





The following subsections provide information about installing the SBG940 hardware:

- [Before You Begin](#)
- [Precautions](#)
- [Signing Up for Service](#)
- [Computer System Requirements](#)
- [Connecting the SBG940 to the Cable System](#)
- [Cabling the LAN](#)
- [Obtaining an IP Address for Ethernet](#)
- [Connecting a PC to the USB Port](#)
- [Wall Mounting](#)

For information about WLAN setup, see “[Setting Up Your Wireless LAN](#)”.

Before You Begin

Before you begin the installation, check that you received the following items with your SBG940:

Item		Description
Power cord		Connects the SBG940 to the AC electrical outlet
10/100Base-T Ethernet cable		Connects to the Ethernet port
USB cable		Connects to the USB port
SBG940 Installation CD-ROM		Contains this <i>User Guide</i> and USB drivers

You will need 75-ohm [coaxial cable](#) with F-type connectors to connect the SBG940 to the nearest cable outlet. If a TV is connected to the cable outlet, you may need a 5 to 900 MHz RF [splitter](#) and two additional coaxial cables to use both the TV and the SBG940.

Determine the connection types you will make to the SBG940. Check that you have the required cables, adapters, and adapter software. You may need:

Wireless LAN	Wireless adapter and driver software for each computer having a wireless connection (see “ Optional Accessories ”)
Wired Ethernet LAN	Ethernet cables and network interface cards (NICs) with accompanying installation software To connect more than four computers to the SBG940, one or more Ethernet hubs or switches
USB	A USB cable and the <i>SBG940 Installation</i> CD-ROM containing the software for USB installation

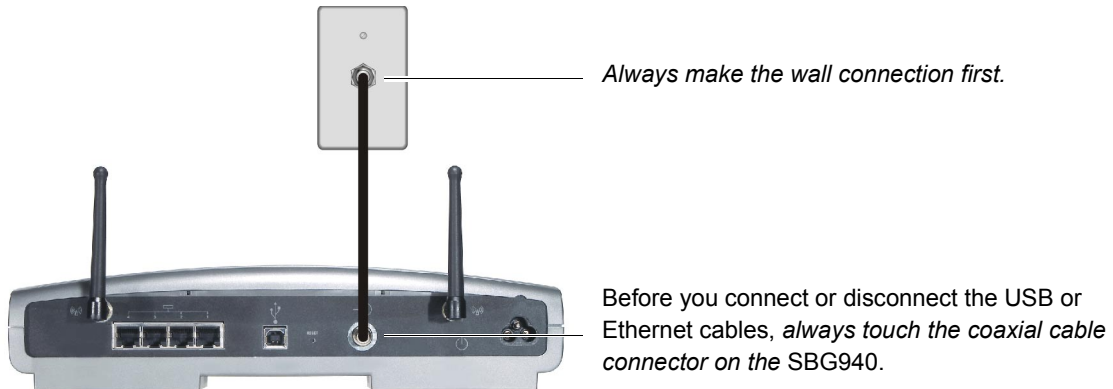
Coaxial cable, RF splitters, hubs, and switches are available at consumer electronic stores.



Precautions

Postpone SBG940 installation until there is no risk of thunderstorm or lightning activity in the area.

To avoid damaging the SBG940 or computers with static electricity:



To avoid potential shock, always unplug the power cord from the wall outlet or other power source before disconnecting it from the SBG940 rear panel.

To prevent overheating the SBG940, do not block the ventilation holes on the sides of the unit.

Do not open the unit. Refer all service to your cable provider.

Wipe the unit with a clean, dry cloth. Never use cleaning fluid or similar chemicals. Do not spray cleaners directly on the unit or use forced air to remove dust.

Signing Up for Service

You must sign up with a cable provider to access the Internet and other online services.

To activate your service, call your local cable provider.

You need to provide the MAC address marked **HFC MAC ID** printed on the [Label on the Bottom of the SBG940](#). You can record it in the SBG940 *Quick Installation Guide*.

You should ask your cable provider the following questions:

- Do you have any special system requirements?
- When can I begin to use my SBG940?
- Are there any files I need to download after I am connected?
- Do I need a user name or password to access the Internet or use e-mail?



Computer System Requirements

You can connect Microsoft Windows, Macintosh, UNIX[®], or Linux[®] computers equipped as follows to the SBG940 LAN:

- One of the following:

Ethernet	10Base-T or 10/100Base-T Ethernet adapter with proper NIC driver software installed.
Wireless	Any IEEE 802.11g or IEEE 802.11b device. For information about the Motorola WN825G Wireless Card (PCMCIA type II 3.3 V slot) or WPCI810G Wireless Adapter, see " Optional Accessories ".

- PC with Pentium class or better processor
- Windows[®] 98, Windows[®] 98 SE, Windows Me[®], Windows[®] 2000, Windows XP[™], Windows NT[®], Macintosh, or Linux operating system with operating system CD-ROM available
- Minimum 16 MB RAM recommended
- 10 MB available hard disk space

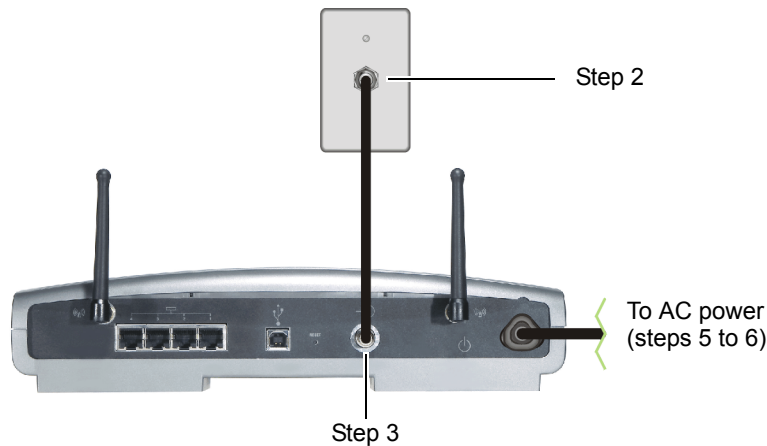
You can use any web browser such as Microsoft[®] Internet Explorer or Netscape Navigator[®] with the SBG940.



You can use the USB connection with any PC running Windows 98, Windows 2000, Windows Me, or Windows XP that has a USB interface. The USB connection requires special USB driver software that is supplied on the *SBG940 Installation* CD-ROM. You can upgrade your USB drivers from the Motorola [Downloads](#) page http://broadband.motorola.com/noflash/usb_drivers.asp.



Connecting the SBG940 to the Cable System

- 1 Be sure the computer is on and the SBG940 is unplugged.
- 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 SBG940.
Hand-tighten the connectors to avoid damaging them.
- 4 Insert the *SBG940 Installation* CD-ROM into the CD-ROM drive.
- 5 Plug the power cord into the power connector on the SBG940.
- 6 Plug the power cord into the electrical outlet. *This turns the SBG940 on. You do not need to unplug it when not in use. The first time you plug in the SBG940, allow 5 to 30 minutes to find and lock on the appropriate communications channels.*



- 7 Check that the lights on the front panel cycle through this sequence:
 -  Turns on when AC power is connected to the SBG940. Indicates that the power is connected properly.
 - DS** Flashes while scanning for the downstream receive channel. Changes to solid green when the receive channel is locked.
 - US** Flashes while scanning for the upstream send channel. Changes to solid green when the send channel is locked.
 - ONLINE** Flashes during SBG940 registration and configuration. Changes to solid green when the SBG940 is registered.
 -  Flashes when the SBG940 is transmitting or receiving data over the Internet.

Cabling the LAN

After connecting to the cable system, you can connect your wired Ethernet LAN. Some samples are shown in “[Wired Ethernet LAN](#)”. On each networked computer, you must install proper drivers for the Ethernet NIC. Detailed information about network cabling is beyond the scope of this document.

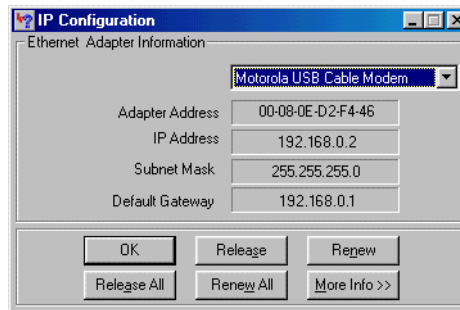


Obtaining an IP Address for Ethernet

Obtaining an IP Address in Windows 98, Windows 98 SE, or Windows Me

You must do the following on each Ethernet client PC running Windows 98, Windows 98 SE, or Windows Me:

- 1 On the Windows Desktop, click **Start**.
- 2 Select **Run**. The Run window is displayed.
- 3 Type **winipcfg.exe** and click **OK**. The IP Configuration window is displayed:



- 4 Click the **Renew** button to obtain an IP address for the PC from the DHCP server on the SBG940.

Obtaining an IP Address in Windows 2000 or Windows XP

You must do the following on each Ethernet client PC running Windows 2000 or Windows XP:

- 1 On the Windows Desktop, click **Start**.
- 2 Select **Run**. The Run window is displayed.
- 3 Type **cmd** and click **OK** to display a command prompt window.
- 4 Type **ipconfig /renew** and press **ENTER** to obtain an IP address for the PC from the DHCP server on the SBG940.
- 5 Type **exit** and press **ENTER** to return to Windows.

Obtaining an IP Address on Macintosh or UNIX Systems

Follow the instructions in your user manual.



Connecting a PC to the USB Port

You can connect a single PC running Windows 98, Windows XP, Windows Me, or Windows 2000 to the SBG940 USB port.

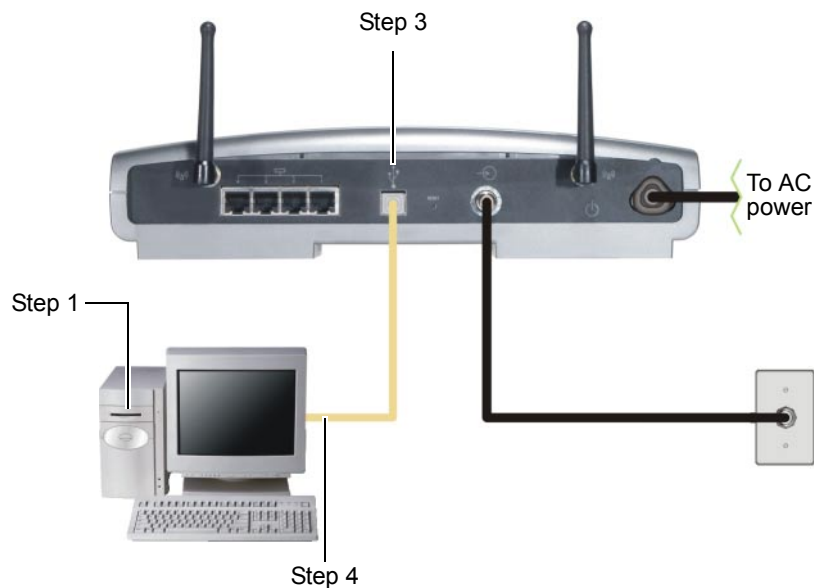
Caution!



Before plugging in the USB cable, be sure the SBG940 Installation CD-ROM is inserted in the PC CD-ROM drive.

To connect a PC to the USB port:

- 1 Insert the *SBG940 Installation* CD-ROM in the CD-ROM drive.
- 2 Install the USB driver following the appropriate procedure for "[Setting Up a USB Driver](#)".
- 3 Connect the USB cable to the USB port on the SBG940 [Rear Panel](#).
- 4 Connect the other end to the USB port on the computer.





Wall Mounting

If you mount the unit on the wall, you must:

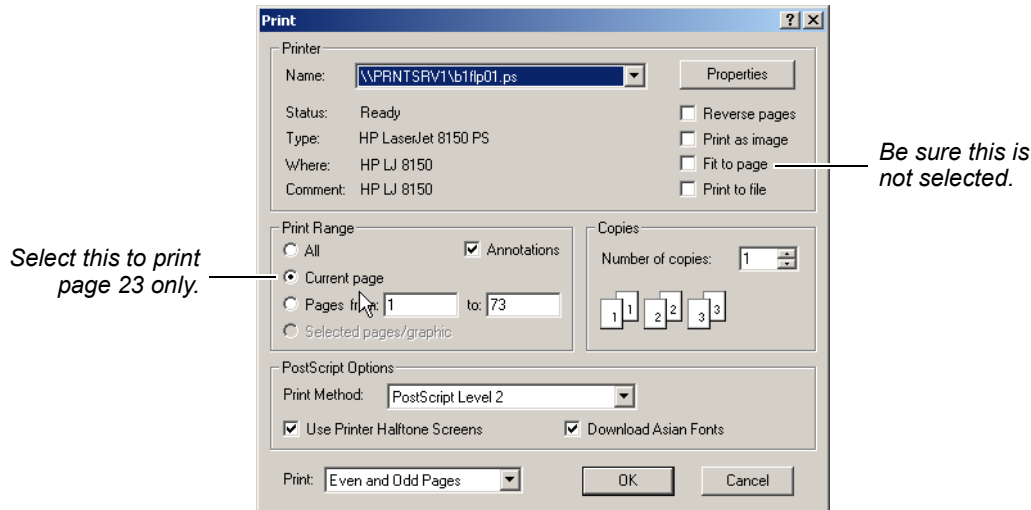
- Locate the unit as specified by the local or national codes governing residential or business cable TV and communications services.
- Follow all local standards for installing a network interface unit/network interface device (NIU/NID).

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

To mount your SBG940 on the wall:

- 1 Print the [Wall Mounting Template](#) on page 23.

Go to page 23 and click the **Print** icon or choose **Print** from the **File** menu to display the Print dialog box. (The following image is from Adobe Acrobat Reader® version 4.0 running on Windows 2000; there may be slight differences in your version.)



*Be sure you print the template at 100% scale. Be sure **Fit to page** is not selected.*

To print the template **only**, select **Current page** as the Print Range.

Click the **OK** button to print the 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.

Caution!



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

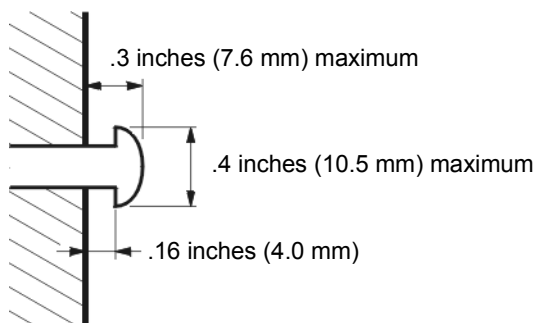
- 5 Drill the holes to a depth of at least 1½ inches (3.8 cm).

- 6 If necessary, seat an anchor in each hole.

Use M5 x 38 mm (#10-16 x 1¹/₂ inch) screws with a flat underside and maximum screw head diameter of 10.5 mm to mount the SBG940.

- 7 Using a screwdriver, turn each screw until part of it protrudes from the wall, as shown:

- There must be .16 inches (4.0 mm) between the wall and the underside of the screw head.
- The maximum distance from the wall to the top of the screw head is 7.6 mm (.3 in).



- 8 Place the SBG940 so the keyholes on the back of the unit are aligned above the mounting screws.

Be sure you do not damage the antennas.

- 9 Slide the SBG940 down until it stops against the top of the keyhole opening.

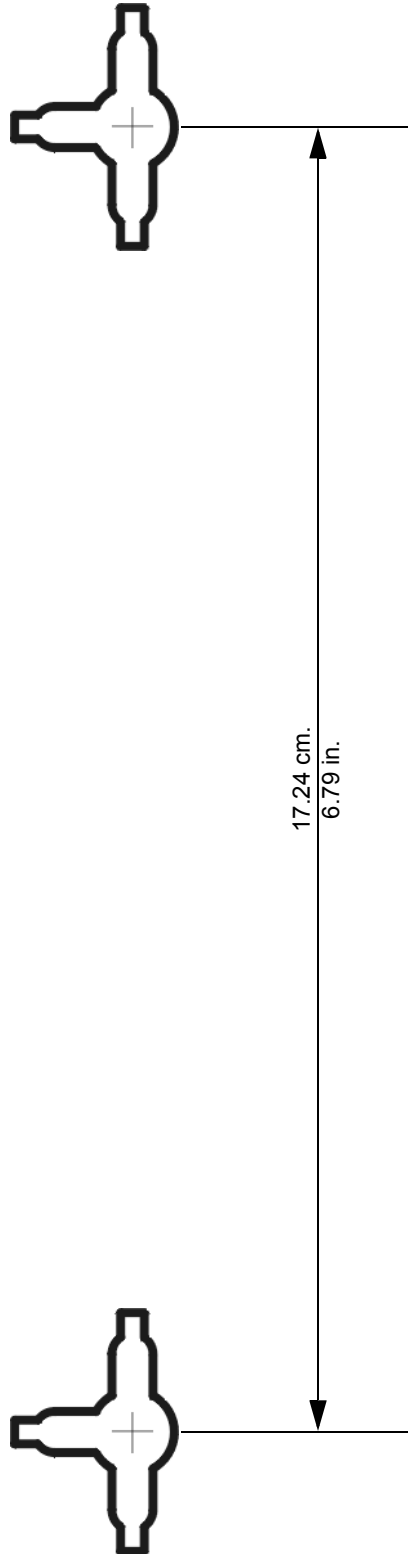


Wall Mounting Template

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

Be sure you print it at 100% scale. In Acrobat Reader, be sure that Fit To Page is not selected in the Print dialog box.

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





❖ Basic Configuration

The following sections provide information about basic SBG940 configuration:

- [Starting the SBG940 Setup Program](#)
- [Changing the Default Password](#)
- [Getting Help](#)
- [Setting the Firewall Policy](#)
- [Gaming Configuration Guidelines](#)

For more advanced configuration information, see “[Configuring TCP/IP](#)”, “[Setting Up Your Wireless LAN](#)”, or “[Setting Up a USB Driver](#)”.

For normal operation, you do not need to change most default settings. The following caution statements summarize the issues you must be aware of:

Caution!



To prevent unauthorized configuration, change the default password *immediately* when you first configure the SBG940. See “[Changing the Default Password](#)”.

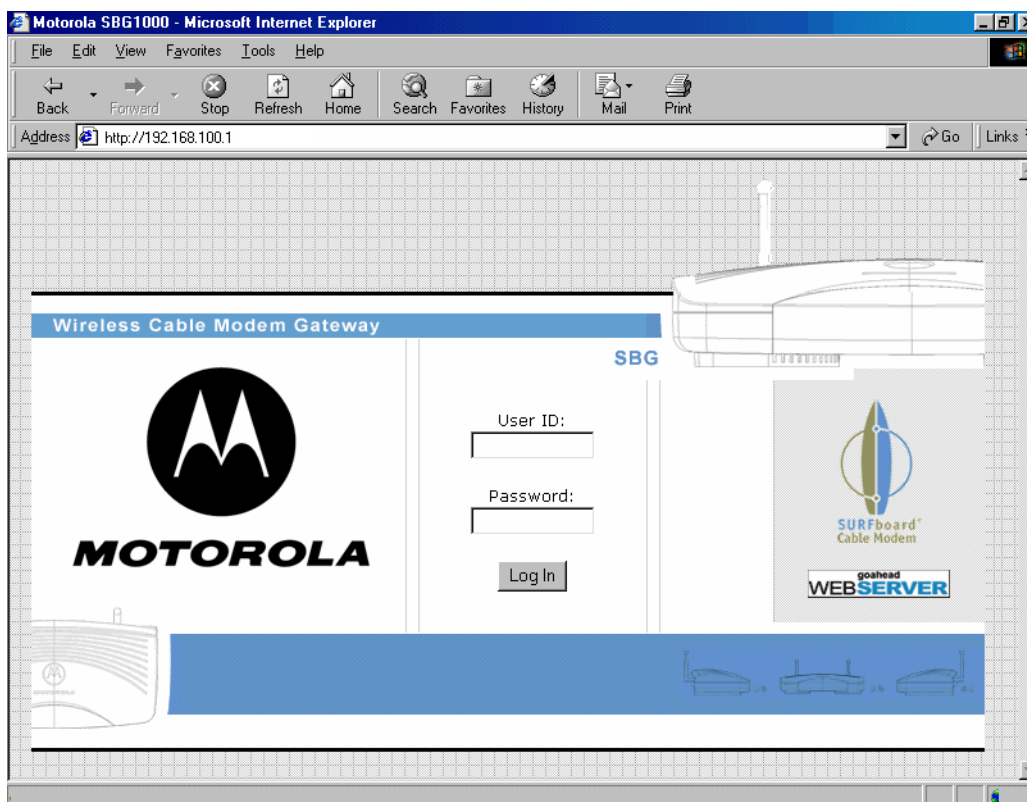
Firewalls are not foolproof. Choose the most secure firewall policy you can. See “[Setting the Firewall Policy](#)”.

If you are using a wired LAN only and have no wireless clients, be sure you disable the wireless interface by turning off Enable Wireless Interface on the [Wireless > NETWORK Page](#).

For a wireless LAN only, be sure you follow the instructions in “[Setting Up Your Wireless LAN](#)”.

Starting the SBG940 Setup Program

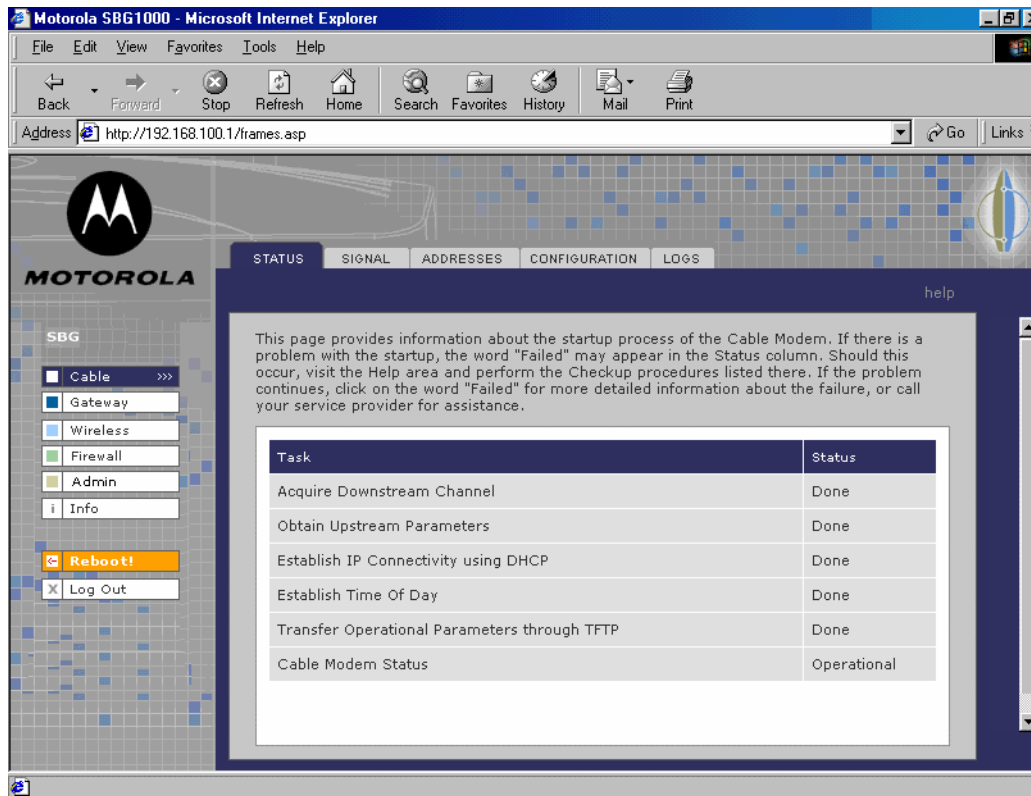
- 1 On a computer wired to the SBG940 over Ethernet or USB, open a web browser. *Do not attempt to configure the SBG940 over a wireless connection.*
- 2 In the Address or Location field, type **http://192.168.100.1** or **http://192.168.0.1** and press **ENTER** to display the Log In window:



- 3 In the **User ID** field, type the **User Name**; the default is "admin" (this field is case sensitive).
- 4 In the **Password** field, type the **Password**; the default is "motorola" (this field is case sensitive).



- 5 Click **Log In** to display the SBG940 user configuration and status windows:



Click To Perform

- Cable** Configure and monitor the cable system connection.
- Gateway** Configure and monitor the gateway preferences (see [“Configuring the Gateway”](#)).
- Wireless** Configure and monitor the wireless interface (see [“Setting Up Your Wireless LAN”](#)).
- Firewall** Configure and monitor the firewall (see [“Setting the Firewall Policy”](#)).
- Admin** [Changing the Default Password](#).
- Info** Display information about the SBG940 Setup Program.
- Reboot** Restart the SBG940. It is the same as pressing the reset button on the [Rear Panel](#) for less than five seconds.
- Log Out** Log out of the SBG940.

If you have difficulty starting the SBG940 Setup Program, see [“Troubleshooting”](#) for information.

Router is a configuration option that may appear on your window but may not be supported.

For some settings, after you edit the field and click Apply, you are warned that you must reboot for your change to take effect. Rebooting takes 10 to 15 seconds. After rebooting, you must log in again.



Changing the Default Password

Caution!



To prevent unauthorized configuration, change the default password *immediately* when you first configure the Motorola SURFboard Wireless Cable Modem Gateway.

To change the default password:

- 1 On the SBG940 Setup Program left panel, click **Admin** to display the ADMIN — basic page:

The screenshot shows the SBG940 Setup Program interface. On the left is a vertical menu with options: Cable, Gateway, Wireless, Firewall, Admin (highlighted with a double arrow), and Info. Below the menu are buttons for Reboot! and Log Out. The main area displays the ADMIN page with tabs for basic and advanced settings. The basic tab is active, showing a message: "This page allows basic user configuration of your admin settings." Below this is a "CHANGE PASSWORD" form with four input fields: User Id (containing "admin"), Old Password, New Password, and Verify Password. An "Apply" button is at the bottom of the form.

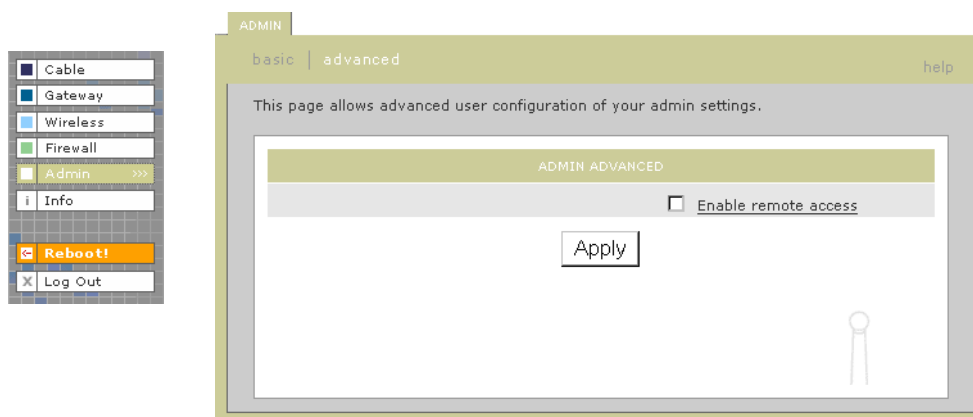
- 2 In the **Old Password** field, type the old **password**. The default password is “motorola” (this field is case sensitive).
- 3 In the **New Password** field, type the new **password**.
- 4 In the **Verify Password** field, type the new **password** again.
- 5 Click **Apply** to apply your changes.

Enabling Remote Access

You can enable remote access to the SBG940 over the Internet. You must know the **userid**, **password**, and **public IP address** assigned to your SBG940 to run the Setup Program over the Internet. Remote access is provided using a web browser on the remote client and connecting to the SBG940 web server.

To enable remote access to the SBG940:

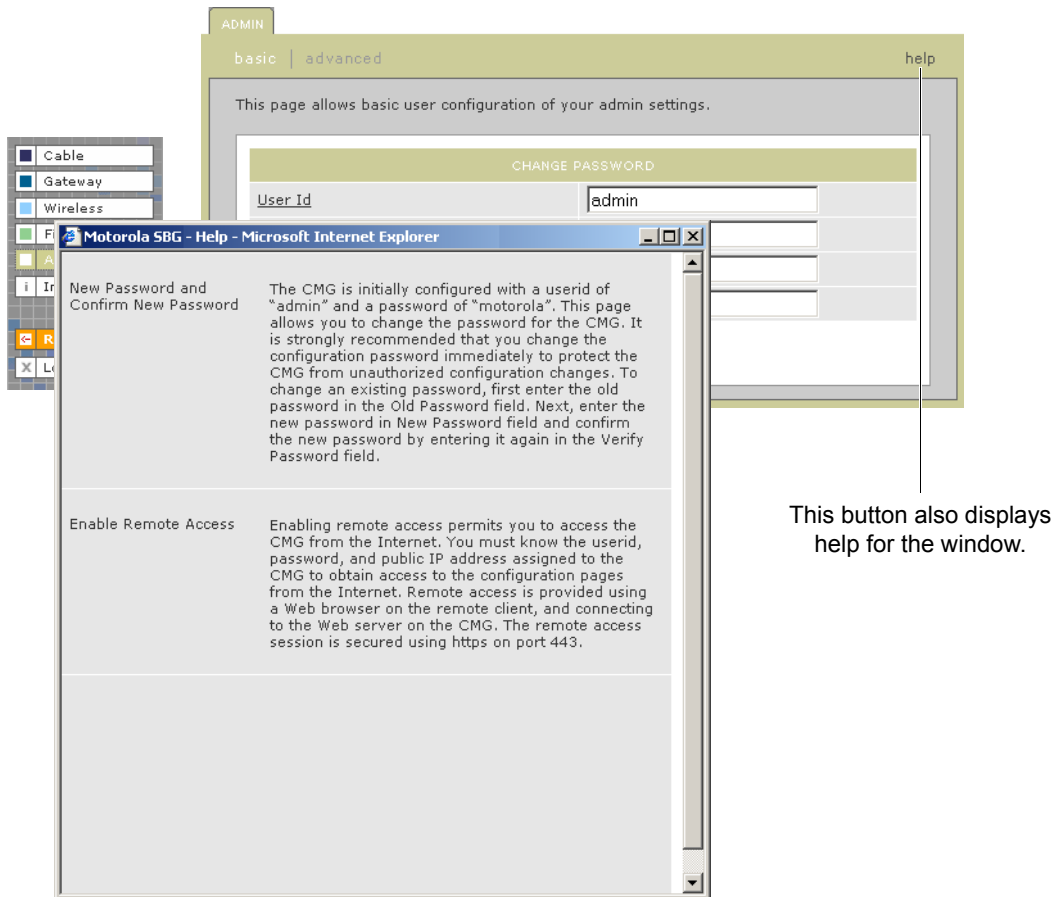
- 1 On the SBG940 Setup Program left panel, click **Admin** to display the ADMIN — basic page.
- 2 Click **advanced** to display the ADMIN — advanced page.



- 3 Click the box next to **Enable remote access** to enable it.
- 4 Click **Apply** to apply your change.

Getting Help

To get help on any underlined item or field, click the text. For example, if you click a field or the help button on the ADMIN — basic page, the following help is displayed:



You can scroll to browse the help or click another item to display help for that item.

Setting the Firewall Policy

The SBG940 firewall protects the SBG940 LAN from undesired attacks and other intrusions from the Internet. This section describes using the Firewall > POLICY — basic page to choose one of the predefined firewall policy templates provided with the SBG940.

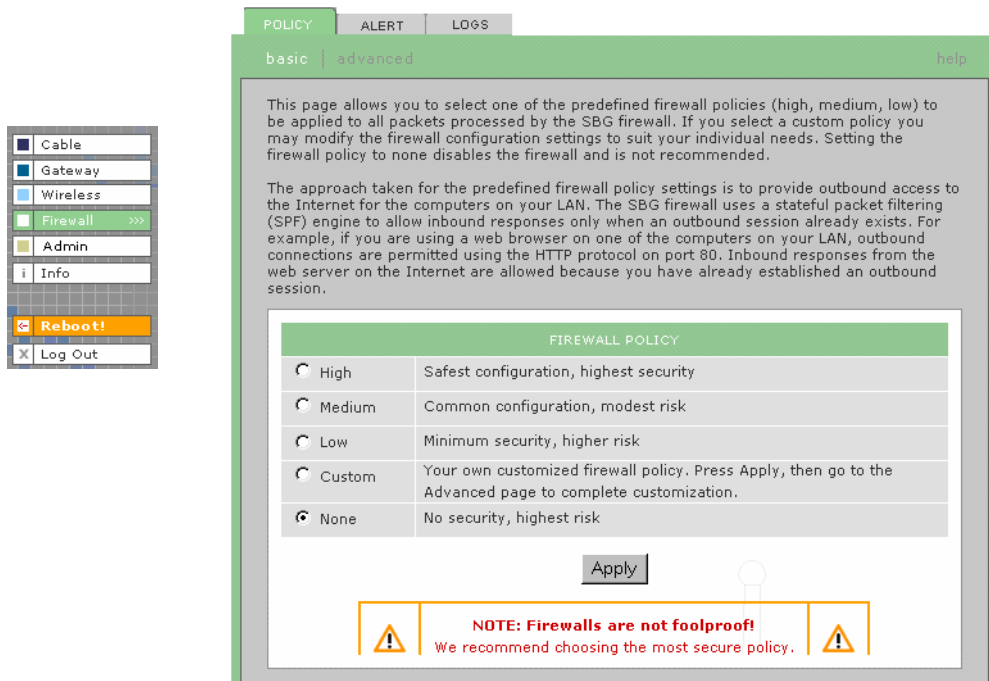
Caution!



Firewalls are not foolproof. Choose the most secure firewall policy you can. To enable easy network setup, the default firewall policy is None, which provides no security.

To select a predefined policy for all packets processed by the SBG940 firewall:

- 1 On the SBG940 Setup Program left panel, click **Firewall**.
- 2 Click **POLICY**.
- 3 Click **basic** to display the predefined firewall policy templates:



The screenshot shows the SBG940 Setup Program interface. On the left is a sidebar with navigation options: Cable, Gateway, Wireless, Firewall (highlighted with a green bar and '>>>'), Admin, Info, Reboot!, and Log Out. The main window has tabs for POLICY, ALERT, and LOGS. The POLICY tab is active, and the 'basic' sub-tab is selected. The page contains a text block explaining the firewall policy selection process, a table of predefined policies, an 'Apply' button, and a red warning box at the bottom.

FIREWALL POLICY	
<input type="radio"/> High	Safest configuration, highest security
<input type="radio"/> Medium	Common configuration, modest risk
<input type="radio"/> Low	Minimum security, higher risk
<input type="radio"/> Custom	Your own customized firewall policy. Press Apply, then go to the Advanced page to complete customization.
<input checked="" type="radio"/> None	No security, highest risk

NOTE: Firewalls are not foolproof!
We recommend choosing the most secure policy.

- 4 Select the most secure firewall policy you can:

- High** The safest predefined firewall policy template, providing the highest security. *We recommend this setting.*
- Medium** A predefined firewall policy template providing a common configuration having modest risk.
- Low** A predefined firewall policy template providing minimum security, with a higher risk of intrusions.
- Custom** You may need to create a custom firewall policy on the [Firewall > POLICY — advanced Page](#). *Do not create a custom policy unless you have the necessary expertise and the need to do so.*
- None** Disables the firewall. To enable easy network setup, it is the default. *After you set up your network, use High, Medium, or Low to improve your security.*



5 Click **Apply** to apply your changes.

After you edit some fields and click Apply, you are warned that you must reboot for your change to take effect. Rebooting takes 10 to 15 seconds. After rebooting, you must log in again.

If you have the need, you can:

- View the rules for the High, Medium, or Low predefined policy templates or create a custom policy on the [Firewall > POLICY — advanced Page](#)
- Configure a firewall alert on [Firewall > ALERT — basic Page](#) and [Firewall > ALERT — email Page](#)
- View the firewall logs on the [Firewall > LOGS Page](#)

For information about how the firewall can affect gaming, see “[Gaming Configuration Guidelines](#)”.

The predefined policies provide outbound Internet access for computers on the SBG940 LAN. The SBG940 firewall uses [stateful inspection](#) to allow inbound responses when there already is an outbound session running corresponding to the data flow. For example, if you use a web browser, outbound HTTP connections are permitted on port 80. Inbound responses from the Internet are allowed because an outbound session is established.

When required, you can configure the SBG940 firewall to allow inbound packets without first establishing an outbound session. You also need to configure a port forwarding entry on the [Gateway > PORT FORWARDING — config Page](#) or a DMZ client on the [Gateway > LAN — nat config Page](#).

Firewall > POLICY — advanced Page

Do not create a custom firewall policy unless you have the necessary expertise and the need to do so. Instead, select one of the predefined policy templates as described in “[Setting the Firewall Policy](#)”.

To create a custom firewall policy, first select **Custom** and click **Apply** on the Firewall > POLICY — basic Page. Then use this page to configure a custom firewall policy:

- ☐ Cable
- ☐ Gateway
- ☐ Wireless
- ☒ Firewall >>>
- ☐ Admin
- ☐ Info
-
-

POLICY
ALERT
LOGS

basic | advanced
help

This page allows you to construct a custom firewall policy by setting all necessary configuration parameters.

NEW FILTER ENTRY

Port ID	<input style="width: 100%;" type="text"/>
Enable	<input type="checkbox"/>
Allowed Protocol	<input type="text" value="IP"/> ▼
Port Range	<input style="width: 40%;" type="text" value="0"/> : <input style="width: 40%;" type="text" value="0"/>
Protocol Number	<input style="width: 100%;" type="text"/>
Allow Inbound	<input type="checkbox"/>
Allow Outbound	<input type="checkbox"/>

FIREWALL POLICY

Port ID	Enable	Port Range	Allowed Protocol	Allow IB	Allow OB	Protocol #	Delete
DNS	<input type="checkbox"/>	12:12	UDP	Yes	Yes	0	<input type="checkbox"/>
FTP	<input checked="" type="checkbox"/>	90:90	TCP	Yes	Yes	0	<input type="checkbox"/>
Telnet	<input checked="" type="checkbox"/>	700:700	UDP/TCP	No	Yes	0	<input type="checkbox"/>
ICMP	<input checked="" type="checkbox"/>	1010:1010	UDP/TCP	Yes	No	0	<input type="checkbox"/>
HTTPS	<input checked="" type="checkbox"/>	80:80	IP	Yes	Yes	5	<input type="checkbox"/>

FIREWALL POLICY TEMPLATE

Applying a Policy Template will erase previously defined customizations.

Policy Template ▼

To base the custom policy on a predefined firewall policy template, choose High, Medium, or Low in the **Policy Template** field and click **Apply Policy Template**.

**Firewall > POLICY — advanced page fields**

Field	Description
NEW FILTER ENTRY	Use these fields to set up one or more custom firewall filters, <i>if you have the necessary expertise</i> .
Port ID	Type the protocol being filtered.
Enable	Select this box to enable firewall policy filtering for the port.
Allowed Protocol	Select the allowed protocols from the drop-down list.
Port Range (From:To)	Sets the port range, which must contain all ports required by the protocol.
Protocol Number	Sets the protocol number of the IP packets to allow.
Allow Inbound	Enables you to specify the port(s) on which inbound packets can pass through the firewall from the Internet to your LAN.
Allow Outbound	Enables you to specify the port(s) on which outbound packets can pass through the firewall from your LAN to the Internet. Stateful inspection ensures appropriate responses for outbound sessions.
Add	Click to add the new filter. It is displayed on the FIREWALL POLICY table.
FIREWALL POLICY Table	Lists your custom firewall filters.
Enable	Select this box to enable firewall policy filtering for the port.
Delete	Select the Delete box to delete the filter.
Apply	Click to apply your changes.
FIREWALL POLICY TEMPLATE	
Policy Template	You can use this drop-down list to select a predefined policy template on which to base your custom template — High, Medium, or Low. These templates are described in “Setting the Firewall Policy”
Apply Policy Template	Click to apply the selected Policy Template and cancel any customizations.



Firewall > ALERT — basic Page

You can use this page to set the alert mechanism for firewall intrusion detection events.

POLICY ALERT LOGS

basic | email help

FirewallAlertEmail

This page allows you to select the alert mechanism to use when firewall Intrusion Detection events are detected. Select the Email check box to be alerted via an SMTP email. Note: Email alerting assumes that an SMTP server is present to receive the email and that the SMTP server does not require any authentication (e.g., user-id/password).

ALERT BASIC

Intrusion Detection ☒ Email

Apply

Firewall > ALERT — basic page fields

Field or Button

Description

Intrusion Detection

Select Email to be alerted through SMTP e-mail. An SMTP server that does not require any authentication such as a user name or password must be present to receive the e-mail.

Apply

Click to apply your changes.



Firewall > ALERT — email Page

You can use this page to configure the e-mail alert parameters:

POLICY ALERT LOGS

basic | email help

This page allows you to configure the Email parameters. Enter the IP address of the email SMTP server in the Email Server IP Address. Enter the port number the SMTP email server is listening on in the Email Server Port field. Enter the sender's email address in the Email Sender field. Enter the list of recipient's email addresses in the Email Recipient List field.

ALERT EMAIL	
Email Server IP Address	10.10.10.100
Email Server Port	25
Email Sender	125@125.com
Email Recipient List	<div> m3@125.com </div>

Apply

Firewall > ALERT — email page fields

Field or Button	Description
E-mail Server IP Address	Sets the e-mail server IP address in dotted-decimal format .
E-mail Server Port	Sets the e-mail server port number.
E-mail Sender	Sets the sender e-mail address.
E-mail Recipient List	Sets the list of e-mail addresses that receive alerts from the SBG940 firewall.
Apply	Click to apply your changes.



Firewall > LOGS Page

You can use this page to set which firewall events are logged.

Firewall > LOGS page fields

Field or Button

Description

Enable Session Log

Select this box to log every data session from the private LAN that was authorized by the SBG940 firewall. Usually, the session log displays a history of normal data traffic. It also lists the start of sessions the firewall terminated because:

- The policy was changed
- They were eventually determined to be an intrusion or attack

To display the session log, click **session**.

Enable Blocking Log

Select this box to log inbound and outbound packets that the SBG940 firewall:

- Does not allow to pass because they use protocols and/or ports not explicitly allowed by the active policy
- Determines to be invalid because of a session or reassembly timeout

To display the blocking log, click **blocking**.

Enable Intrusion Log

Select this box to log attacks using common network intrusion tactics that the SBG940 firewall detects and stops.

To display the intrusion log, click **intrusion**.

Apply

Click to apply your changes.

If you enable the firewall, the blacklist log is always generated. Any IP address the firewall determines to have breached the active policy is added to the blacklist log. To view the blacklist log, click **blacklist**. The firewall blocks all traffic to and from a blacklisted IP address for 24 hours or until you reboot the SBG940 or manually clear the blacklist by clicking **Clear** on the Firewall > LOGS — blacklist page.



Gaming Configuration Guidelines

The following subsections provide information about configuring the SBG940 firewall and DMZ for gaming.

Configuring the Firewall for Gaming

By default, the SBG940 firewall is disabled. If, as recommended, you enable the firewall, refer to the game's documentation to ensure that the necessary ports are open for use by that game.

The pre-defined SBG940 firewall policies affect Xbox Live™ as follows:

- Low** Xbox Live data can pass through the firewall. No user action is required.
- Medium or high** To enable Xbox Live traffic to pass, you must configure:
- Choose Custom on the Firewall > POLICY — basic Page
 - UDP 88:88 and UDP/TCP 3074:3074 on the [Firewall > POLICY — advanced Page](#)

Configuring Port Triggers

Because the SBG940 has pre-defined port triggers for games using any of the following applications, no user action is required to enable them:

- DirectX 7 and DirectX 8
- MSN Games by Zone.com
- Battle.net®

For a list of games supported by Battle.net, visit <http://www.battle.net>.

You may need to create custom port triggers to enable other games to operate properly. If you set custom port triggers and enable the firewall, you must customize the firewall to allow traffic through those ports. To create custom port triggers, use the [Gateway > PORT TRIGGERS — custom Page](#).



Configuring a Gaming DMZ Host

Caution!



The gaming DMZ host is not protected by the firewall. It is open to communication or hacking from any computer on the Internet. Consider carefully before configuring a device to be in the DMZ.

Some games and game devices require *one* of:

- The use of random ports
- The forwarding of unsolicited traffic

For example, to connect a PlayStation® 2 for PS2® online gaming, designate it as the gaming DMZ host because the ports required vary from game to game. For these games, we recommend configuring the gaming computer or device as a gaming DMZ device.

To configure a gaming DMZ device, on the [Gateway > LAN — dhcp leases Page](#):

- 1 Reserve a private IP address for the computer or game device MAC address.
- 2 Designate the device as a DMZ device.

You can reserve IP addresses for multiple devices, but only one can be designated as the gaming DMZ at once.



Configuring the Gateway

This section describes the Gateway configuration pages in the SBG940 Setup Program:

- [Gateway > STATUS Page](#)
- [Gateway > WAN Page](#)
- [Gateway > LAN — nat config Page](#)
- [Gateway > LAN — dhcp server config Page](#)
- [Gateway > LAN — dhcp leases Page](#)
- [Gateway > PORT FORWARDING — status Page](#)
- [Gateway > PORT FORWARDING — config Page](#)
- [Gateway > PORT TRIGGERS — predefined Page](#)
- [Gateway > PORT TRIGGERS — custom Page](#)
- [Gateway > LOG Page](#)

After you edit some fields and click Apply, you are warned that you must reboot for your change to take effect. Rebooting takes 10 to 15 seconds. After rebooting, you must log in again.



Gateway > STATUS Page

This page displays the gateway status information:

Cable

Gateway >>>

Wireless

Firewall

Admin

Info

Reboot!

Log Out

STATUS

WAN

LAN

PORT TRIGGERS

LOG

help

This page lists the status information for several gateway configuration parameters.

WAN Status	Data
DNS Address 1	206.19.80.10
DNS Address 2	206.19.86.10
DNS Address 3	0.0.0.0
WAN IP Address	206.19.86.131
TCP Session Wait Timeout	300 seconds
UDP Session Wait Timeout	300 seconds
ICMP Session Wait Timeout	300 seconds

LAN Status	Data
LAN IP Address	192.168.0.1
LAN Subnet Mask	255.255.255.0
MAC Address	00:08:0E:D2:F4:71
DHCP Server Enabled	Yes

DHCP LEASE TABLE					
IP Address	MAC Address	Hostname	Method	Lease Create Time	Lease Expire Time
192.168.0.2	00:C0:F0:3B:3E:9C	Micron-95	Dynamic	2003-01-14 12:54:49	2003-01-14 13:54:49

TRANSLATED ADDRESS					
WAN IP Address	WAN Port	LAN IP Address	LAN Port	Mapping Mode	Mapping Protocol
206.19.86.131	2233	192.168.0.2	2233	0	3
206.19.86.131	2228	192.168.0.2	2228	0	3

PASSTHROUGH HOST

These fields display settings that are set on the other Gateway pages. For field descriptions, see the following subsections that describe the fields on each tab.

Home

Print

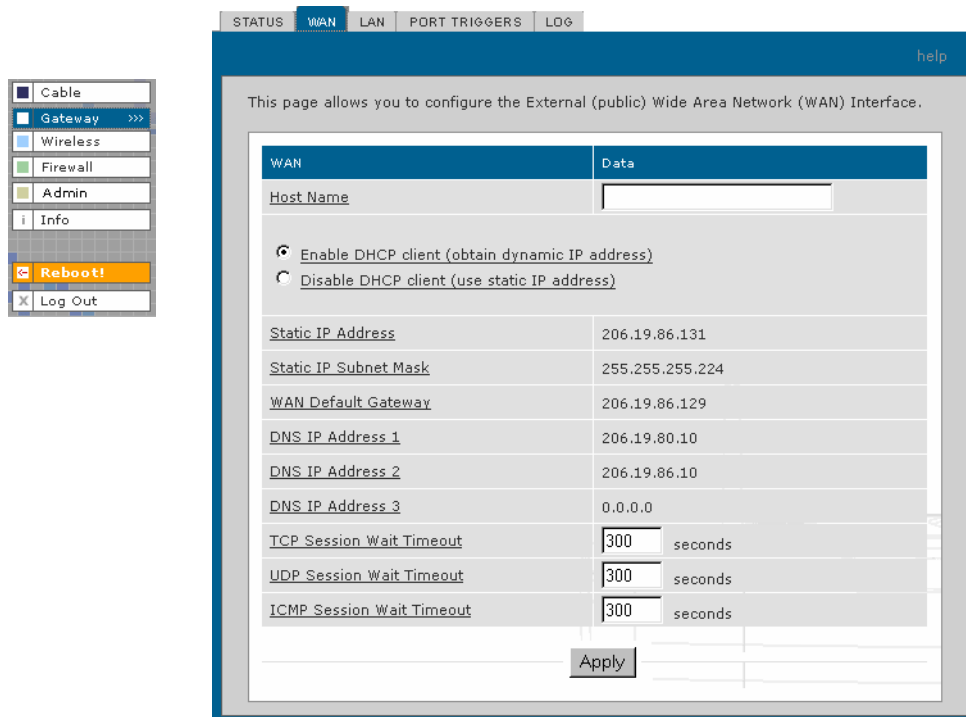
Exit

◀ 40 ▶

SBG940 User Guide

Gateway > WAN Page

Use this page to configure the external (public) wide area network (WAN) interface:



Gateway > WAN page fields

Field	Description
Host Name	If the cable provider requires a hostname to access to their network, type the <i>hostname</i> they provided in this field. The default is None.
Enable DHCP Client (obtain dynamic IP address)	Enabling the DHCP client causes the wireless gateway to automatically obtain the public IP address , subnet mask , domain name , and DNS server(s). Most commonly, the DHCP client is enabled if the cable provider automatically assigns a public IP address from their DHCP server. Enable DHCP Client is selected by default.
Disable DHCP Client (use static IP address)	If the cable provider does not automatically assign a public IP address using DHCP, they must provide a static IP address . Select Disable DHCP Client. When you disable the DHCP client, you must type the static IP address, subnet mask, DNS server(s), and domain name (if necessary) in the fields provided. Disable DHCP Client is not selected by default.
Static IP Address	If Disable DHCP Client is selected, type the static <i>IP address</i> provided by the cable provider in dotted-decimal format . The default is None.
Static IP Subnet Mask	If Disable DHCP Client is selected, type the <i>subnet mask</i> associated with the static IP address in dotted-decimal format. The default is None.
WAN Default Gateway	When using a Static IP Address from the cable provider, type the default gateway <i>IP address</i> on the WAN for the SBG940 in dotted-decimal format.



Gateway > WAN page fields (continued)

Field

Description

DNS IP Address 1

DNS IP Address 2

DNS IP Address 3

The cable provider DNS server provides name-to-IP address resolution. If the cable provider does not automatically assign DNS addresses from their DHCP server, they must provide at least one DNS server IP address to enter in these fields in dotted-decimal format. The default is None.

**TCP Session Wait
Timeout**

Sets the maximum time in seconds to wait before assuming a TCP session has timed out. The default is 24 hours.

**UDP Session Wait
Timeout**

Sets the maximum time in seconds to wait before assuming a UDP session has timed out. The default is 300 seconds (5 minutes).

**ICMP Session Wait
Timeout**

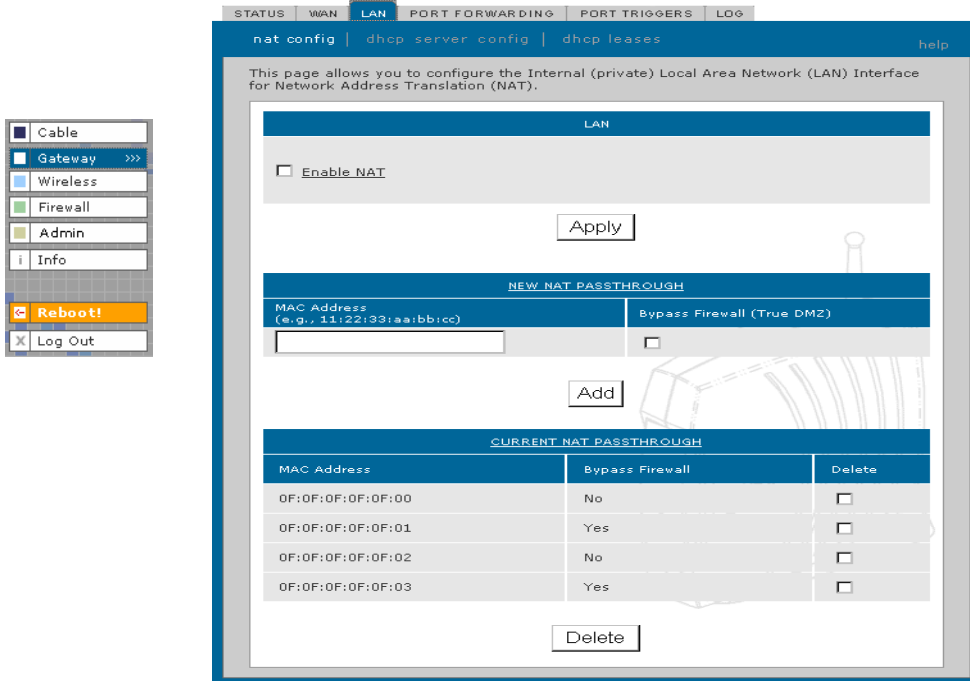
Sets the maximum time in seconds to wait before assuming an ICMP session has timed out. The default is 300 seconds (5 minutes).

Apply

Click to apply your changes.

Gateway > LAN — nat config Page

Use this page to enable **NAT** and add clients to the CURRENT NAT PASSTHROUGH list:



Gateway > LAN — nat config page fields

Field or Button

Description

LAN

Enable NAT

If enabled, the single HFC IP Address (public IP address) assigned by the cable provider is mapped to many private IP addresses on the SBG940 LAN.

Apply

Click to apply your changes. You must reboot the SBG940.

NEW NAT PASSTHROUGH

Specifies up to 32 computers as passthrough clients not subject to NAT, using their MAC addresses.

MAC Address

Type the passthrough client MAC address. The format is 16 hexadecimal numerals.

Bypass Firewall (True DMZ)

Select this box to set the NAT passthrough computer as a DMZ client. *Use this setting with extreme caution because a DMZ client is completely open to Internet hackers.*

Add

Click to add the MAC address to the CURRENT NAT PASSTHROUGH list.

CURRENT NAT PASSTHROUGH

Lists the computers on the LAN that are configured for NAT passthrough.

Delete

Click to delete the selected MAC address from the NAT passthrough list.



Gateway > LAN — dhcp server config Page

Only experienced network administrators should use this page to perform advanced DHCP server configuration:

CAUTION!



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

Gateway > LAN — dhcp server config page fields

Field

Description

LAN IP Address	You can type the <i>IP address</i> of the SBG940 for your private LAN. The default is 192.168.0.1.
LAN IP Subnet Mask	Displays the subnet mask in dotted-decimal format. The default is 255.255.255.0.
Starting IP Address	Enter the starting <i>IP address</i> to be assigned by the SBG940 DHCP server to clients in dotted-decimal format. The default is 192.168.0.2.
# of DHCP Users	Sets the <i>number</i> of clients for the SBG940 DHCP server to assign a private IP address. There are 253 possible client addresses. The default is 253.
DHCP Server Lease Time	Sets the <i>time</i> in seconds that the SBG940 DHCP server leases an IP address to a client. The default is 3600 seconds (60 minutes).
Domain Name	Sets the <i>domain name</i> for the SBG940 LAN. The default is None.
Time To Live	Sets the <i>TTL</i> (hop limit) for outbound packets. The default is 64.
Interface Maximum Transmission Unit	Sets the SBG940 LAN MTU in bytes. The minimum is 68 bytes. The default is 1500 bytes.
Apply	Click to apply your changes. You must reboot the SBG940.

Gateway > LAN — dhcp leases Page

Use this page to configure DHCP leases:

Cable

Gateway >>>

Wireless

Firewall

Admin

Info

Reboot!

Log Out

STATUS WAN LAN PORT FORWARDING PORT TRIGGERS LOG

nat config dhcp server config dhcp leases help

This page allows you to view and configure the DHCP leases.

DMZ stands for de-militarized zone. The computer configured to be in the DMZ is not protected by the firewall and is open to communication from any computer on the Internet. Thus, careful consideration should be given before configuring your computer to be in the DMZ. This feature is useful if you are having difficulties running certain applications - typically gaming applications.

GAMING DMZ

DMZ Host

RESERVE NEW IP ADDRESS

MAC Address <small>(e.g., 11:22:33:aa:bb:cc)</small>	IP Address	Bypass Firewall	Host Name
	9.9.9.	<input type="checkbox"/>	

CURRENT DHCP LEASES

MAC Address	IP Address	Bypass Firewall	Host Name	Method	Delete
02:03:04:05:06:09	9.9.9.9	No	host9	Dynamic Inactive	<input type="checkbox"/>
02:03:04:05:06:0A	9.9.9.10	No	host10	Dynamic Inactive	<input type="checkbox"/>
02:03:04:05:06:0B	9.9.9.11	Yes	host11	Dynamic Inactive	<input type="checkbox"/>
02:03:04:05:06:0B	9.9.9.11	Yes	host12	Dynamic Active	<input type="checkbox"/>

Gateway > LAN — dhcp leases page fields

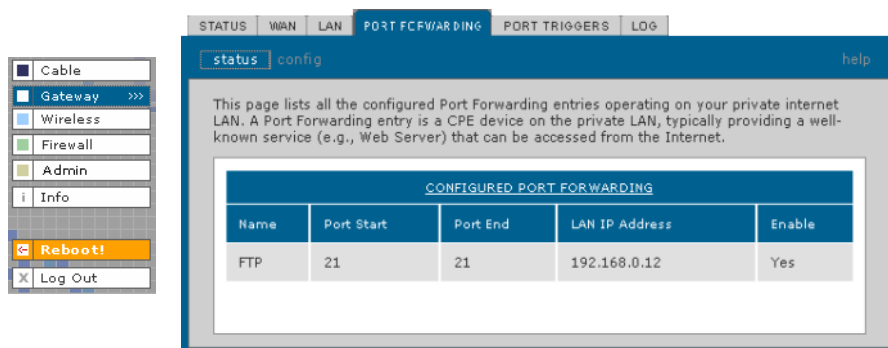
Field	Description
GAMING DMZ	
Enable Gaming DMZ	Select this box to designate the selected computer or gaming device as the gaming DMZ host. For more information, see " Configuring a Gaming DMZ Host ". This can be useful if you have difficulties running certain applications; typically gaming applications.
(Gaming) DMZ Host	<p>The gaming DMZ host is a computer with a reserved IP address designated as the default DMZ host. Only one gaming DMZ host can be active at once.</p> <p><i>The gaming DMZ host is not protected by the firewall. It is open to communication or hacking from any computer on the Internet. Consider carefully before configuring a computer to be in the DMZ.</i></p> <p>The benefit of using a gaming DMZ host instead of a NAT passthrough host is that a gaming DMZ host does not require a public IP address as does a NAT passthrough host. If the application requires a public IP address, configure the computer for NAT passthrough on the Gateway > LAN — nat config Page.</p>

Gateway > LAN — dhcp leases page fields (continued)

Field	Description
RESERVE NEW IP ADDRESS	You can reserve up to 32 IP addresses assigned by the SBG940 DHCP server for specific LAN clients. For example, to ensure that they always receive the same private IP address, you can reserve IP addresses for a private FTP server or gaming DMZ device.
MAC Address	Type the MAC address of the DHCP client for which a reserved IP address is required. The format is 16 hexadecimal numerals.
IP Address	Sets the host portion of the reserved IP address for the LAN client having the specified MAC address. When the LAN client requests an IP address, the SBG940 DHCP server assigns the client this IP address.
Host Name	If your ISP requires a hostname to access their network, enter the hostname provided to you in the Host Name field.
Add	Click Add to reserve a new IP address.
CURRENTLY RESERVED IP ADDRESSES	Displays all DHCP clients having reserved IP addresses.
MAC Address	Displays the client MAC address.
IP Address	Displays its reserved IP address
Host Name	Displays its host name.
Method	Displays dynamic and static lease status. Add or delete dynamic or static lease status in this field.
Delete	Click this box to remove the reserved IP address for the client.
Delete	Click this button to remove the reserved IP addresses for clients designated by the Delete box.

Gateway > PORT FORWARDING — status Page

Use this page to display the configured port forwarding entries on the SBG940 LAN. The fields are the same as on the [Gateway > PORT FORWARDING — config Page](#):



STATUS WAN LAN **PORT FORWARDING** PORT TRIGGERS LOG

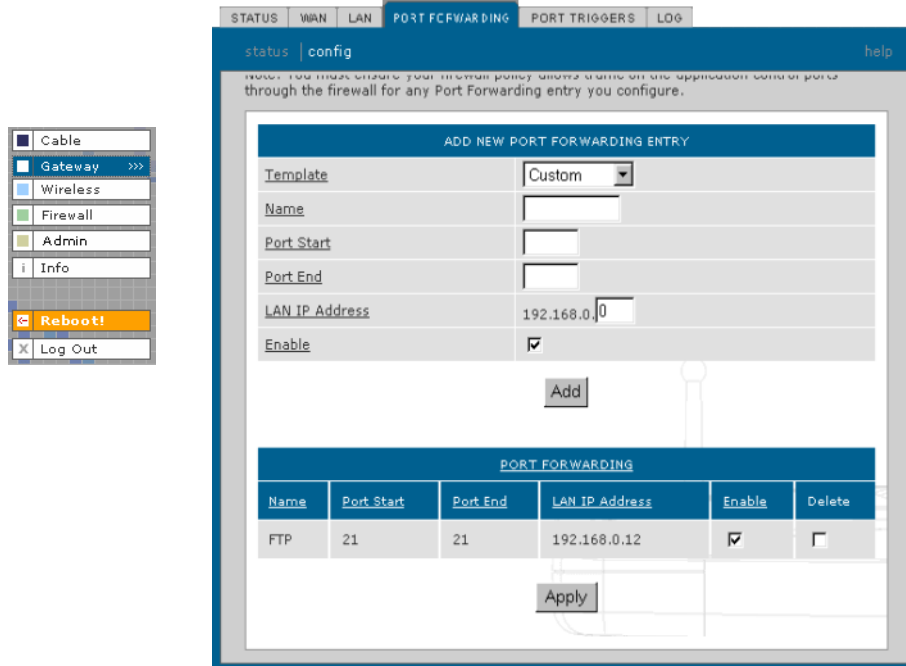
status config help

This page lists all the configured Port Forwarding entries operating on your private internet LAN. A Port Forwarding entry is a CPE device on the private LAN, typically providing a well-known service (e.g., Web Server) that can be accessed from the Internet.

CONFIGURED PORT FORWARDING				
Name	Port Start	Port End	LAN IP Address	Enable
FTP	21	21	192.168.0.12	Yes

Gateway > PORT FORWARDING — config Page

Use this page to configure up to 32 virtual servers:



Gateway > PORT FORWARDING — config page fields

Field	Description
ADD NEW PORT FORWARDING ENTRY	You can configure up to 32 virtual servers. If you select Custom, you must set the Name, Port Start, Port End, and LAN IP Address.
Template	If you select a predefined template such as HTTP or FTP, the Name, Port Start, Port End values are provided. You only need to enter LAN IP Address and change default values only if necessary.
Name	Type a unique identifier for the custom virtual server. The typical practice is to use the protocol as a unique identifier (for example "ftp").
Port Start	Sets the LAN internal interface port or the start of a port range. Inbound Internet connection requests are statically mapped to this port. The ports used by some common applications are: <ul style="list-style-type: none"> FTP 20, 21 HTTP 80 NTP 123 Secure Shell 22 SMTP e-mail 25 Telnet 23
Port End	If a range of ports is required, sets the end of the port range.



Gateway > PORT FORWARDING — config page fields (continued)

Field	Description
LAN IP Address	Sets the private LAN IP address for the port forwarding page. An Internet user must know the public IP address to access any port forwarding entry you define on the private LAN.
Enable	Select this box to enable the port forwarding entries to be accessed through NAT.
Add	Click to add the virtual server to the PORT FORWARDING list.
PORT FORWARDING	Displays the configured custom virtual servers.

Gateway > PORT TRIGGERS — predefined Page

When you run a PC application that accesses the Internet, it communicates with a computer on the Internet. In some applications, especially gaming, the computer on the Internet also communicates with your PC. Because NAT does not normally allow these incoming connections, the SBG940 supports port triggering.

The SBG940 is preconfigured with port triggering for common applications. You can also configure additional port triggers if needed. Configuring port triggers for an application requires:

- The application transport protocol — TCP or UDP
- The application port number

You can use the default values for the remaining parameters.

Only one computer at a time connected to the SBG940 can use an application requiring port triggering. Use this page to view predefined port triggers:

STATUS
WAN
LAN
PORT TRIGGERS
LOG

Cable

Gateway >>>

Wireless

Firewall

Admin

Info

Reboot!

Log Out

predefined | custom
help

This page allows you to enable or disable the predefined Application Level Gateway (Port Triggers) triggers. A Port Trigger is needed for certain applications that need one or more ports opened to operate properly. The typical applications that need Port Triggers to operate properly are games, video conferencing, and file transfer (e.g., FTP). Note: You must ensure your firewall policy allows traffic on the application control ports through the firewall for any Port Triggers you configure.

Name	Enable	Protocol	Port Range	Session Chaining	Session Interval	Address Replace	Multi Host
DirectX7 (TCP)	<input checked="" type="checkbox"/>	TCP	47624:47624	TCP/UDP	600	Disable	Yes
DirectX7 (UDP)	<input checked="" type="checkbox"/>	UDP	47624:47624	TCP/UDP	600	Disable	Yes
DirectX8 (UDP)	<input checked="" type="checkbox"/>	UDP	6073:6073	TCP/UDP	600	Disable	Yes
DirectX8 (TCP)	<input checked="" type="checkbox"/>	TCP	6073:6073	TCP/UDP	600	Disable	Yes
MS zone.com (TCP)	<input checked="" type="checkbox"/>	TCP	6667:6667	TCP/UDP	600	Disable	Yes
MS zone.com (UDP)	<input checked="" type="checkbox"/>	UDP	6667:6667	TCP/UDP	600	Disable	Yes
Battle.n et1 (TCP)	<input checked="" type="checkbox"/>	TCP	6112:6112	TCP/UDP	600	Disable	Yes
Battle.n et2 (UDP)	<input checked="" type="checkbox"/>	UDP	6112:6112	TCP/UDP	600	Disable	Yes
Battle.n et3 (TCP)	<input checked="" type="checkbox"/>	TCP	4000:4000	TCP/UDP	600	Disable	Yes
Battle.n et4 (UDP)	<input checked="" type="checkbox"/>	UDP	4000:4000	TCP/UDP	600	Disable	Yes
Quicktim e RTSP TCP	<input checked="" type="checkbox"/>	TCP	554:554	TCP/UDP	600	Disable	Yes
Netmeeti ng H-323	<input checked="" type="checkbox"/>	TCP	1720:1720	TCP/UDP	600	TCP	Yes
Net2Phon e	<input checked="" type="checkbox"/>	UDP	6801:6801	TCP/UDP	600	Disable	Yes
MSN Msg	<input checked="" type="checkbox"/>	TCP	1863:1863	TCP/UDP	600	Disable	No
AOL IM	<input checked="" type="checkbox"/>	TCP	5190:5190	TCP/UDP	600	Disable	No

Apply

Gateway > PORT TRIGGERS — predefined page fields

Field	Description
Name	Displays the unique name for the port triggers. This is typically the protocol name.
Enable	Select this box to activate the port triggers for the predefined application.
Protocol	Displays the transport protocol for the port trigger — TCP or UDP.
Port Range	Displays the port range (From/To) for the port trigger.
Session Chaining	Displays the session chaining selection for the port trigger — Disable, TCP, or TCP/UDP.
Session Interval	Displays the session interval set for the port trigger.
Address Replace	Displays the address replacement method for the port trigger.
Multi Host	Displays the multi host selection for the port trigger.



Gateway > PORT TRIGGERS — custom Page

Use this page to create a custom port trigger:

predefined custom help

This page allows you to configure custom Application Level Gateway and Smart Tracking Trigger parameters. Up to 32 custom Port Triggers can be configured. Note: You must ensure your firewall policy allows traffic on the application control ports through the firewall for any Port Triggers you configure.

ADD NEW SPECIAL APPLICATION

Name:

Enable: ☐

Protocol:

Port Range: :

Session Chaining:

Session Interval: seconds

Address Replace:

Multi Host: ☐

Add

PORT TRIGGERS TABLE

Name	Enable	Protocol	Port Range	Session Chaining	Session Interval	Address Replace	Multi Host	Delete
------	--------	----------	------------	------------------	------------------	-----------------	------------	--------

Gateway > PORT TRIGGERS — custom page fields

Field

Description

ADD NEW SPECIAL APPLICATION

Name	Enter the unique name for the port trigger. This is typically the protocol.
Enable	Select this box to enable the custom port trigger.
Protocol	Sets the transport protocol for the port trigger — TCP or UDP.
Port Range (From:To)	Sets the port range for the port trigger. Type the start of the range in the left field and the end in the right field.
Session Chaining	Enable session chaining if the application needs to open one or more ports in different ranges to operate properly. The options are Disable, TCP, or TCP/UDP.
Session Interval	Sets the session interval for the application: <ul style="list-style-type: none">If the port triggers detect traffic on the Port Range within the Session Interval, it is considered to be related to the initial session.If the port triggers detect traffic on the Port Range after the Session Interval expires, it is considered to be a new and unique session.
Address Replace	Sets the address replacement method for the application.
Multi Host	Select if appropriate for the application.
Add	Click to add the port trigger to the PORT TRIGGERS TABLE.



Gateway > PORT TRIGGERS — custom page fields (continued)

Field

Description

PORT TRIGGERS TABLE Lists all port triggers you defined and their parameters.

Priority Port Select the port to have a priority status.

Gateway > LOG Page

Use this page to view detailed information about the gateway:

Time	Priority	Code	Message
2003-01-14 12:55:12	6-Notice	0x04C515A8	CAP unable to make C-NAPT mapping. No WAN IP address available
2003-01-14 12:55:14	4-Error	0x040DC1A0	DHCP REBIND sent - Invalid DHCP option

Gateway > LOG page fields

Field

Description

Time The date and time in the format yyyy-mm-dd hh:mm:ss

Priority Indicates the importance of the message.

Code Displays a code associated with the message.

Message Describes the event.

❖ Configuring TCP/IP

You must be sure all client computers are configured for [TCP/IP](#) (a protocol for communication between computers). Perform *one* of:

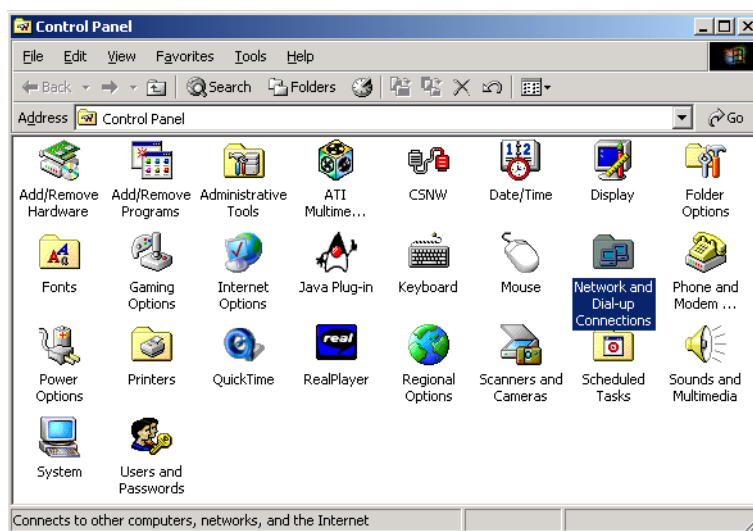
- [Configuring TCP/IP in Windows 95, Windows 98, or Windows Me](#)
- [Configuring TCP/IP in Windows 2000](#)
- [Configuring TCP/IP in Windows XP](#)
- Follow the instructions in your Macintosh or UNIX user manual

After configuring TCP/IP, perform *one* of the following to verify the [IP address](#):

- [Verifying the IP Address in Windows 95, Windows 98, or Windows Me](#)
- [Verifying the IP Address in Windows 2000 or Windows XP](#)
- Follow the instructions in your Macintosh or UNIX user manual

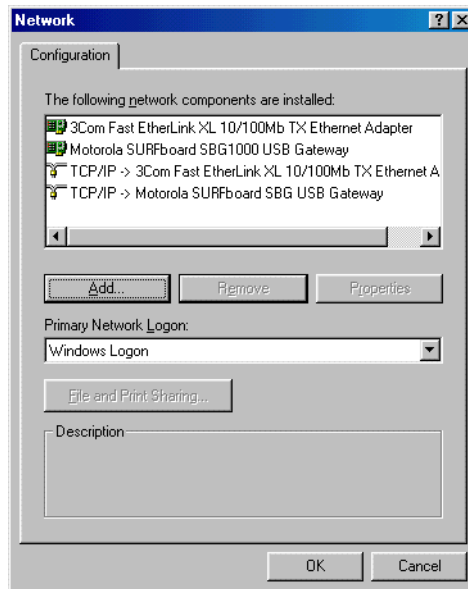
Configuring TCP/IP in Windows 95, Windows 98, or Windows Me

- 1 On the Windows Desktop, click **Start**.
- 2 Select **Settings** and then **Control Panel** from the pop-up menus to display the Control Panel window:



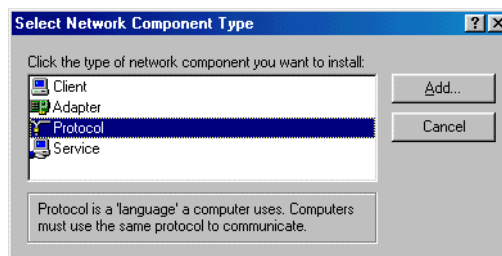


- 3 Double-click the **Network** icon to display the Network window:

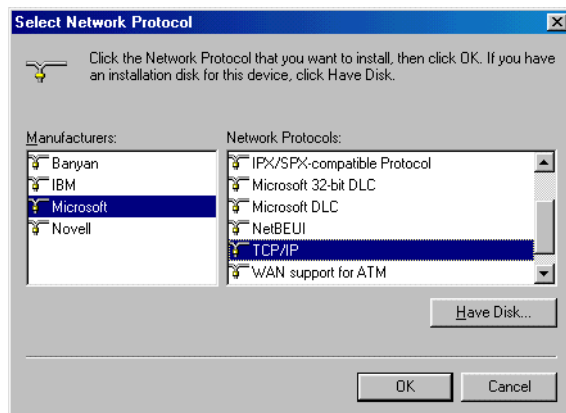


Although your SBG model number may be different than in the images in this guide, the procedure is the same.

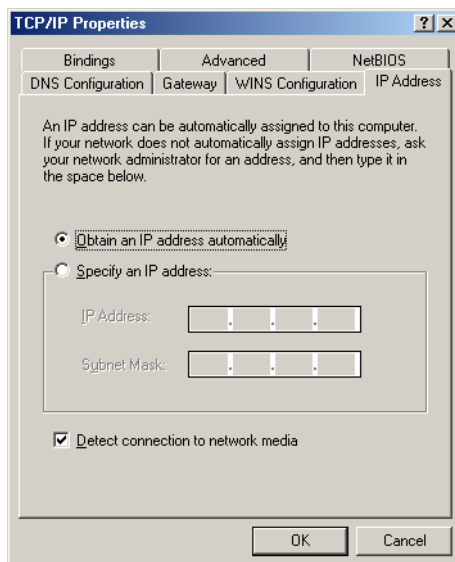
- 4 Select the **Configuration** tab.
- 5 Verify that TCP/IP is installed for the adapter used to connect to the SBG940. If TCP/IP is installed, skip to step 10. If TCP/IP is not installed for the adapter, continue with step 6.
- 6 Select the adapter to use for the SBG940 connection and click **Add**. The Select Network Component Type window is displayed:



- 7 Click **Protocol** and click **Add**. The Select Network Protocol window is displayed:



- 8 Click **Microsoft** in the Manufacturers section and click **TCP/IP** in the Network Protocols section.
- 9 Click **OK**.
- 10 Click **TCP/IP** on the Network window. If there is more than one TCP/IP entry, choose the one for the Ethernet card or USB port connected to the SBG940.
- 11 Click **Properties**. The TCP/IP Properties window is displayed:

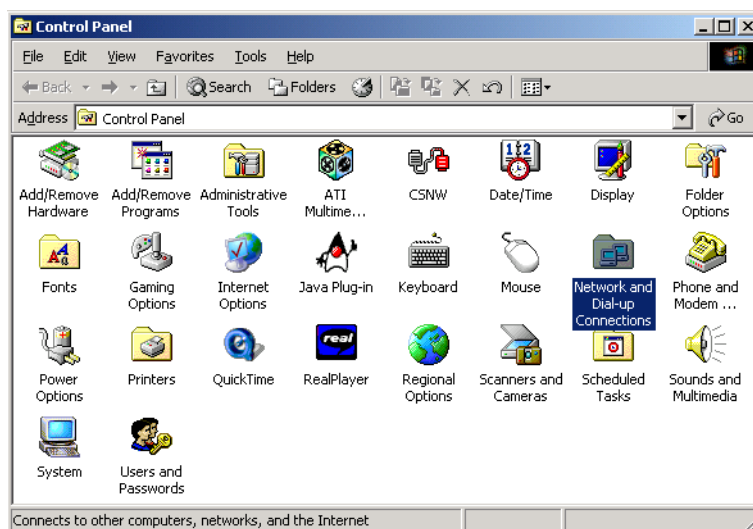


- 12 Click the **IP Address** tab.
- 13 Click **Obtain an IP address automatically**.
- 14 Click **OK** to accept the TCP/IP settings.
- 15 Click **OK** to close the Network window.
- 16 Click **OK** when prompted to restart the computer and click **OK** again.

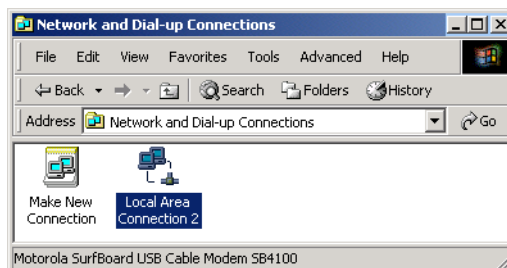
When you complete TCP/IP configuration, go to [“Verifying the IP Address in Windows 95, Windows 98, or Windows Me”](#).

Configuring TCP/IP in Windows 2000

- 1 On the Windows Desktop, click **Start**.
- 2 Select **Settings** and then **Control Panel** from the pop-up menus to display the Control Panel window:

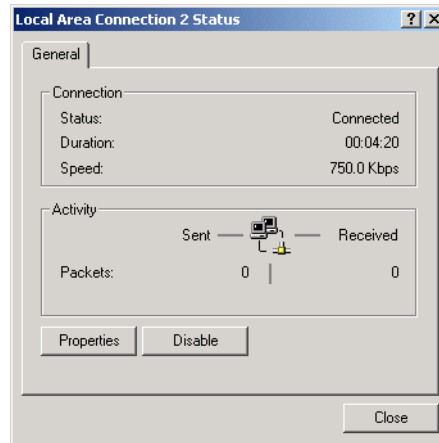


- 3 Double-click the **Network and Dial-up Connections** icon to display the Network and Dial-up Connections window:

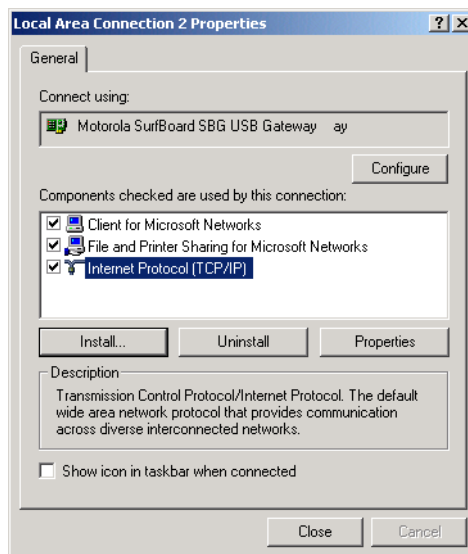




- 4 Click **Local Area Connection number**. The value of *number* varies from system to system. The Local Area Connection *number* Status window is displayed:

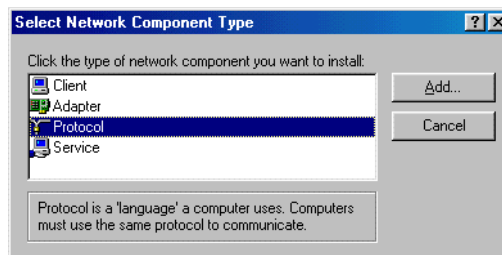


- 5 Click **Properties**. Information similar to the following window is displayed:

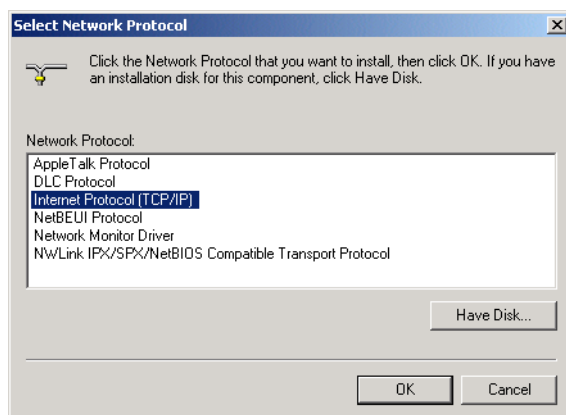


- 6 If Internet Protocol (TCP/IP) is in the list of components, TCP/IP is installed. You can skip to step 10.

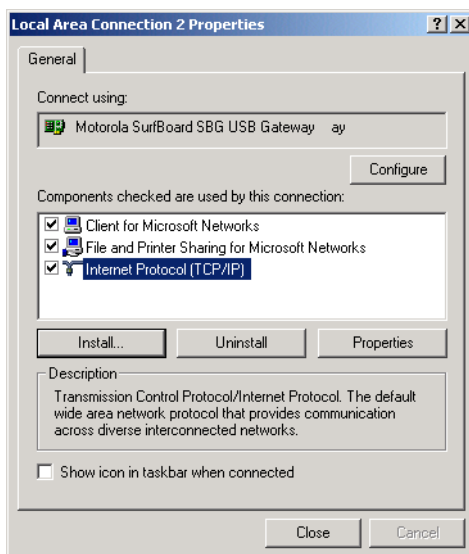
If Internet Protocol (TCP/IP) is not in the list, click **Install**. The Select Network Component Type window is displayed:



- 7 Click **Protocol** on the Select Network Component Type window and click **Add**. The Select Network Protocol window is displayed:

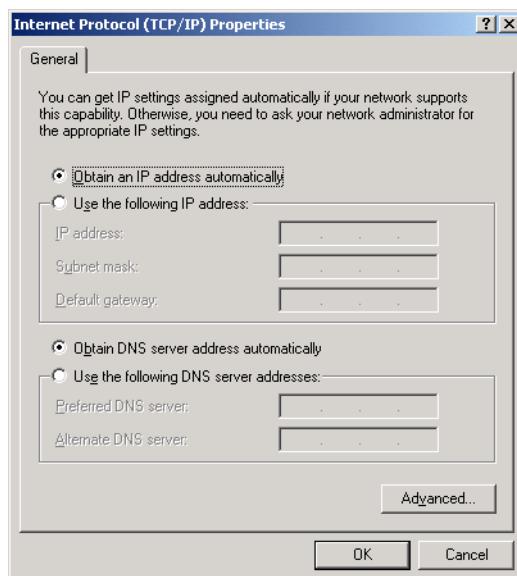


- 8 Click **Internet Protocol (TCP/IP)**.
- 9 Click **OK**. The Local Area Connection *number* Properties window is re-displayed.



- 10 Be sure the box next to Internet Protocol (TCP/IP) is selected.

- 11** Click **Properties**. The Internet Protocol (TCP/IP) Properties window is displayed:



- 12** Be sure **Obtain IP address automatically** and **Obtain DNS server address automatically** are selected.

- 13** Click **OK** to accept the TCP/IP settings.

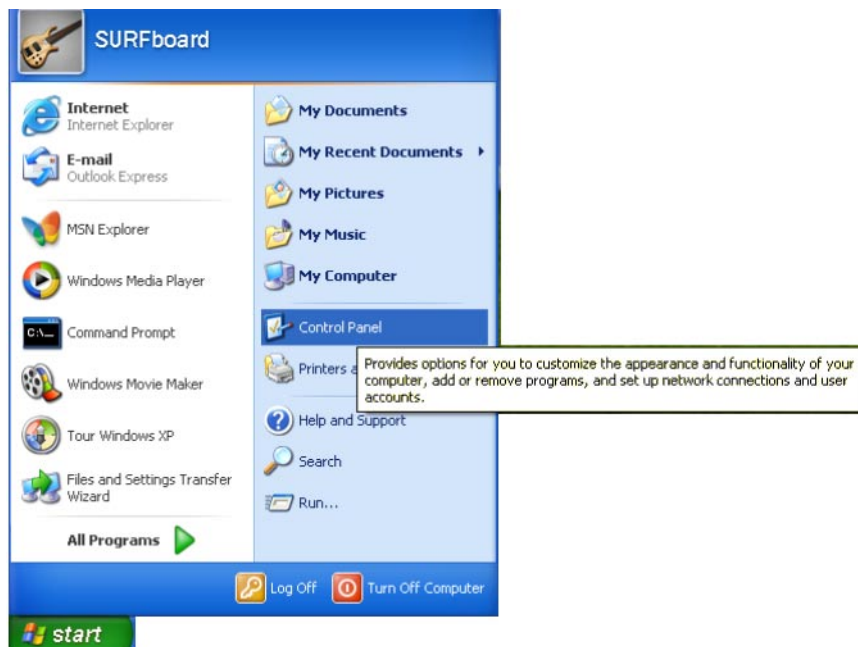
- 14** Click **Close** to close the Local Area Connection *number* Properties window.

- 15** Click **OK** when prompted to restart the computer and click **OK** again.

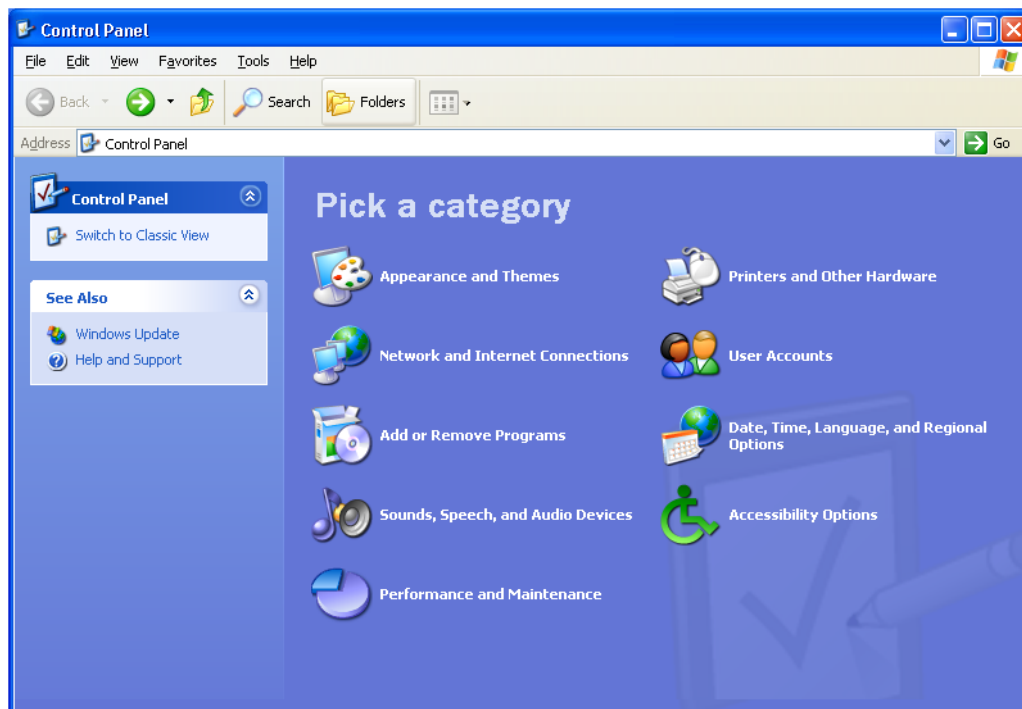
When you complete the TCP/IP configuration, go to ["Verifying the IP Address in Windows 2000 or Windows XP"](#).

Configuring TCP/IP in Windows XP

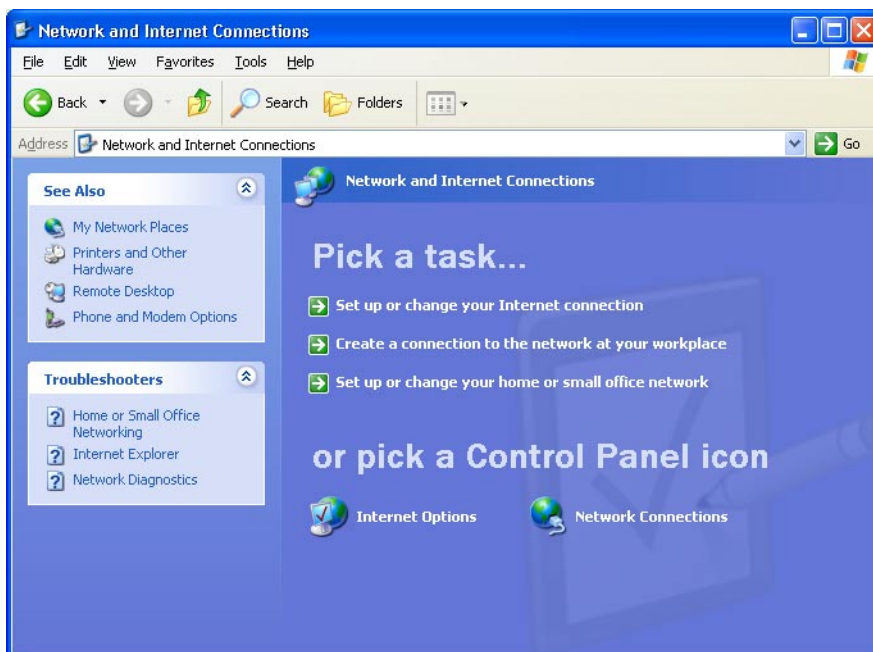
- 1 On the Windows desktop, click **Start** to display the Start window:



- 2 Click **Control Panel** to display the Control Panel window. The display varies, depending on the Windows XP view options. If the display is a Category view as shown below, continue with step 3. Otherwise, skip to step 5.

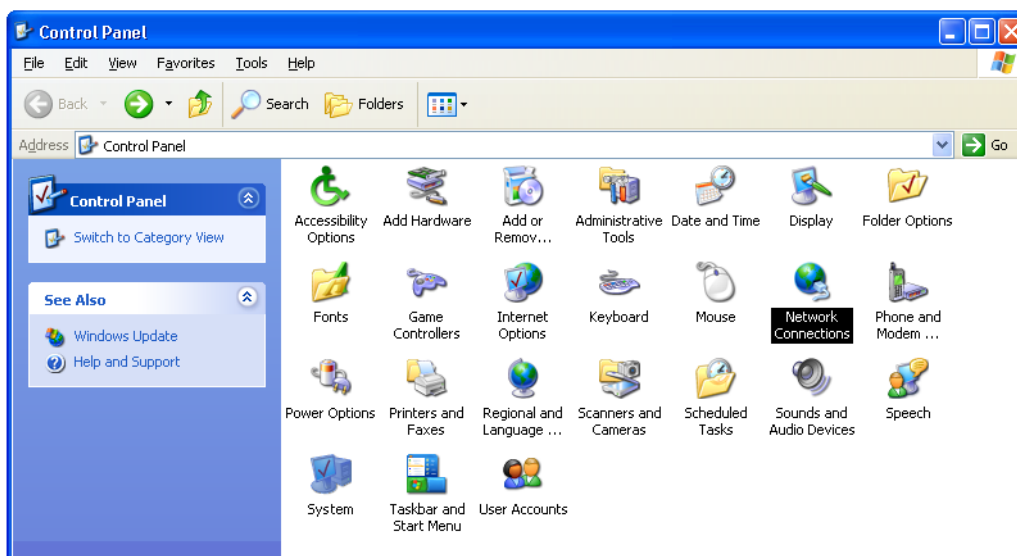


- 3 Click **Network and Internet Connections** to display the Network and Internet Connections window:



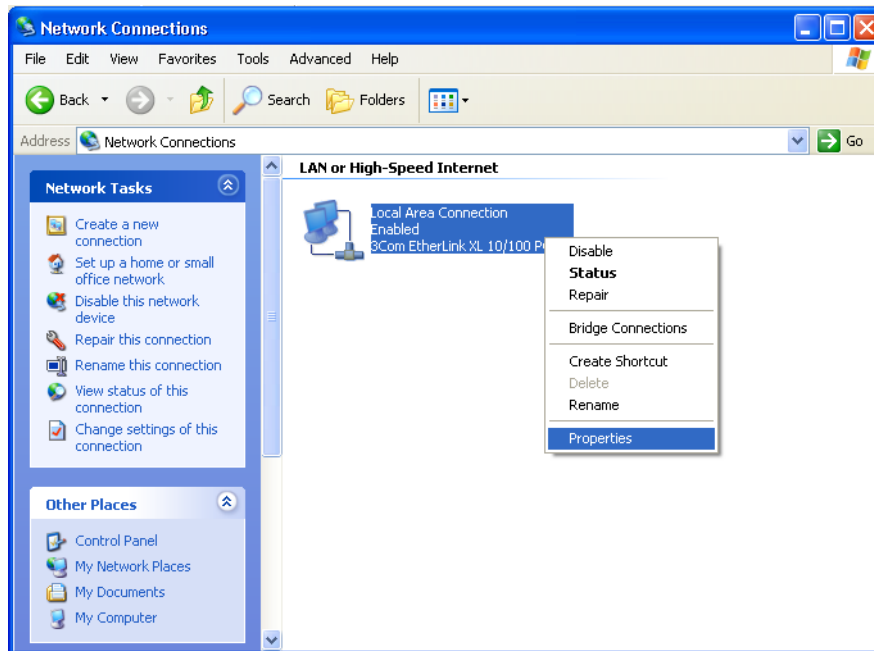
- 4 Click **Network Connections** to display the LAN or High-speed Internet connections. Skip to step 7.

- 5 If a classic view similar to below is displayed:

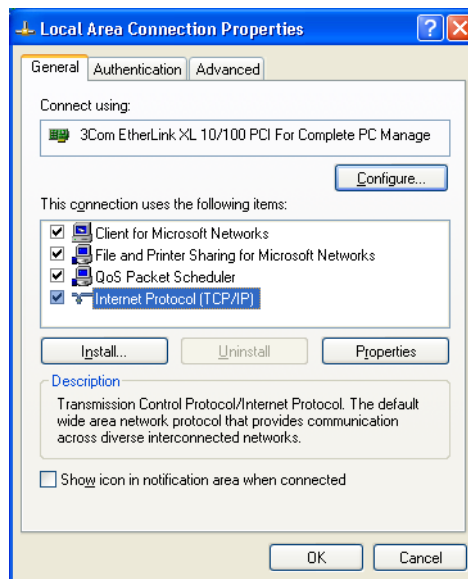


- 6 Double-click **Network Connections** to display the LAN or High-speed Internet connections.

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



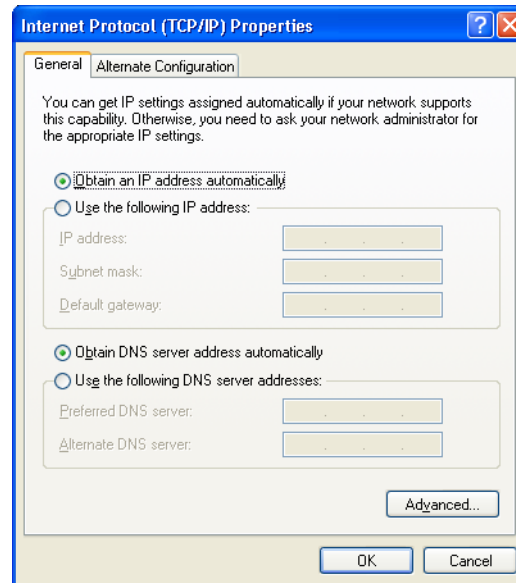
- 8 Select **Properties** from the pop-up menu to display the Local Area Connection Properties window:



- 9 On the Local Area Connection Properties window, be sure Internet Protocol (TCP/IP) is selected. If it is not selected, select it.



- 10 Select **Internet Protocol (TCP/IP)** and click **Properties** to display the Internet Protocol (TCP/IP) Properties window:



- 11 Verify that the settings are correct, as shown above.
- 12 Click **OK** to close the TCP/IP Properties window.
- 13 Click **OK** to close the Local Area Connection Properties window.

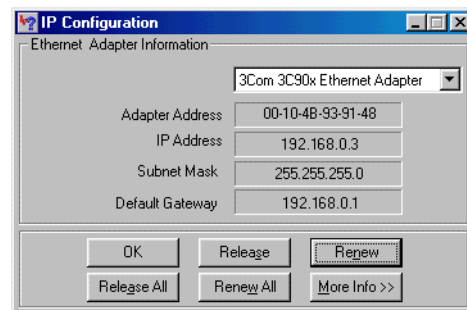
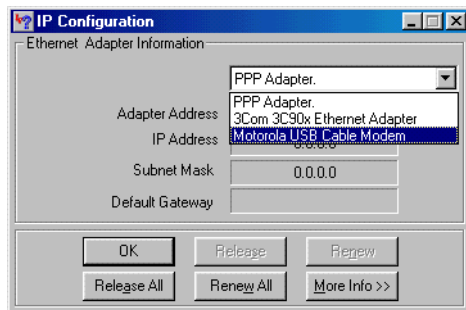
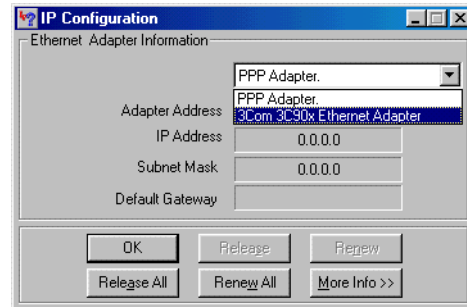
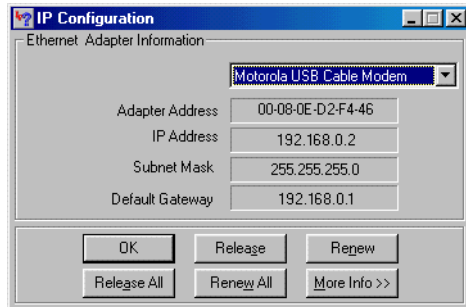
When you complete the TCP/IP configuration, go to [“Verifying the IP Address in Windows 2000 or Windows XP”](#).



Verifying the IP Address in Windows 95, Windows 98, or Windows Me

To check the IP address:

- 1 On the Windows Desktop, click **Start**.
- 2 Select **Run**. The Run window is displayed.
- 3 Type **winipcfg.exe** and click **OK**. The IP Configuration window is displayed. The Ethernet Adapter Information field will vary depending on the system, as shown in the following examples:



The values for Adapter Address, IP Address, Subnet Mask, and Default Gateway on the PC will be different than in the images.

In Windows 98, if “Autoconfiguration” is displayed before the IP Address as in the following image, call your service provider.

Adapter Address	00-80-C6-E7-59-E6
IP Autoconfiguration Address	169.254.191.251

- 4 Select the adapter name — the Ethernet card or USB device.
- 5 Click **Renew**.
- 6 Click **OK** after the system displays an IP address.

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



Verifying the IP Address in Windows 2000 or Windows XP

To check the IP address:

- 1 On the Windows Desktop, click **Start**.
- 2 Select **Run**. The Run window is displayed.
- 3 Type **cmd** and click **OK** to display a command prompt window.
- 4 Type **ipconfig** and press **ENTER** to display the IP configuration. A display similar to the following indicates a normal configuration:

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

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : surfboard.com
    IP Address. . . . .               : 192.168.0.4
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.0.1

Ethernet adapter Local Area Connection:

    Media State . . . . .             : Cable Disconnected

C:\>
```

If an Autoconfiguration IP Address is displayed as in the following window, there is an incorrect connection between the PC and the SBG940 or there are cable network problems. Check the cable connections and determine if you can view cable-TV channels on your television:

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

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

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

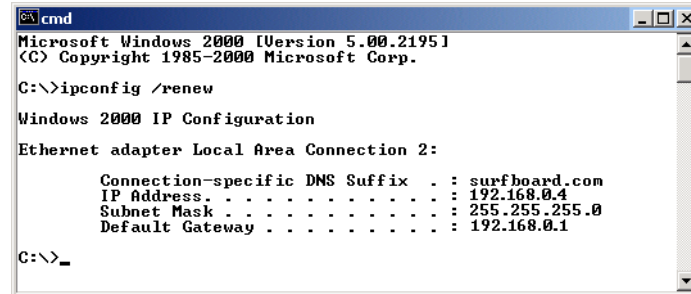
C:\>
```

After verifying the cable connections and proper cable-TV operation, renew the IP address.



To renew the IP address:

- 1 Type **ipconfig /renew** and press **ENTER**. If a valid IP address is displayed as shown, Internet access should be available.



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

C:\>ipconfig /renew

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : surfboard.com
    IP Address. . . . . : 192.168.0.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

C:\>
```

- 2 Type **exit** and press **ENTER** to return to Windows.

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



❖ Setting Up Your Wireless LAN

You can use the SBG940 as an access point for a wireless LAN (WLAN) without changing its default settings.

Caution!



To prevent unauthorized eavesdropping or access to WLAN data, you must enable wireless security. The default SBG940 settings provide no wireless security. After your WLAN is operational, be sure to enable wireless security.

To enable security for your WLAN, you can do the following on the SBG940:

To

Perform

Use in Setup Program

Encrypt wireless transmissions and restrict WLAN access

[Encrypting Wireless LAN Transmissions](#)

[Wireless > SECURITY — basic Page](#)

Further prevent unauthorized WLAN intrusions

[Restricting Wireless LAN Access](#)

[Wireless > SECURITY — advanced Page](#)

Connect at least one computer to the SBG940 Ethernet or USB port to perform configuration. Do not attempt to configure the SBG940 over a wireless connection.

You need to configure each wireless client (station) to access the SBG940 LAN as described in “[Configuring the Wireless Clients](#)”.

Caution!



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

For descriptions of all wireless configuration fields, see “[Configuring a Wireless Client with the Network Name \(ESSID\)](#)”.

Another step to improve wireless security is to place wireless components away from windows. This decreases the signal strength outside the intended area.



Encrypting Wireless LAN Transmissions

To prevent unauthorized viewing of data transmitted over your WLAN, you must encrypt your wireless transmissions.

Use the [Wireless > SECURITY — basic Page](#) to encrypt your transmitted data. Choose *one* of:

Configure on the SBG940

If all of your wireless clients support Wi-Fi Protected Access (WPA), we recommend [Configuring WPA on the SBG940](#)

Otherwise, perform [Configuring WEP on the SBG940](#)

Required On Each Wireless Client

If you use a local pre-shared key (WPA-PSK) passphrase, you must configure the identical passphrase to the SBG940 on each wireless client. Home and small-office settings typically use a local passphrase.

Configuring a RADIUS server requires specialized knowledge that is beyond the scope of this guide. For more information, contact your network administrator.

You must configure the identical WEP key to the SBG940 on each wireless client.

If all of your wireless clients support WPA encryption, we recommend using WPA instead of WEP because WPA:

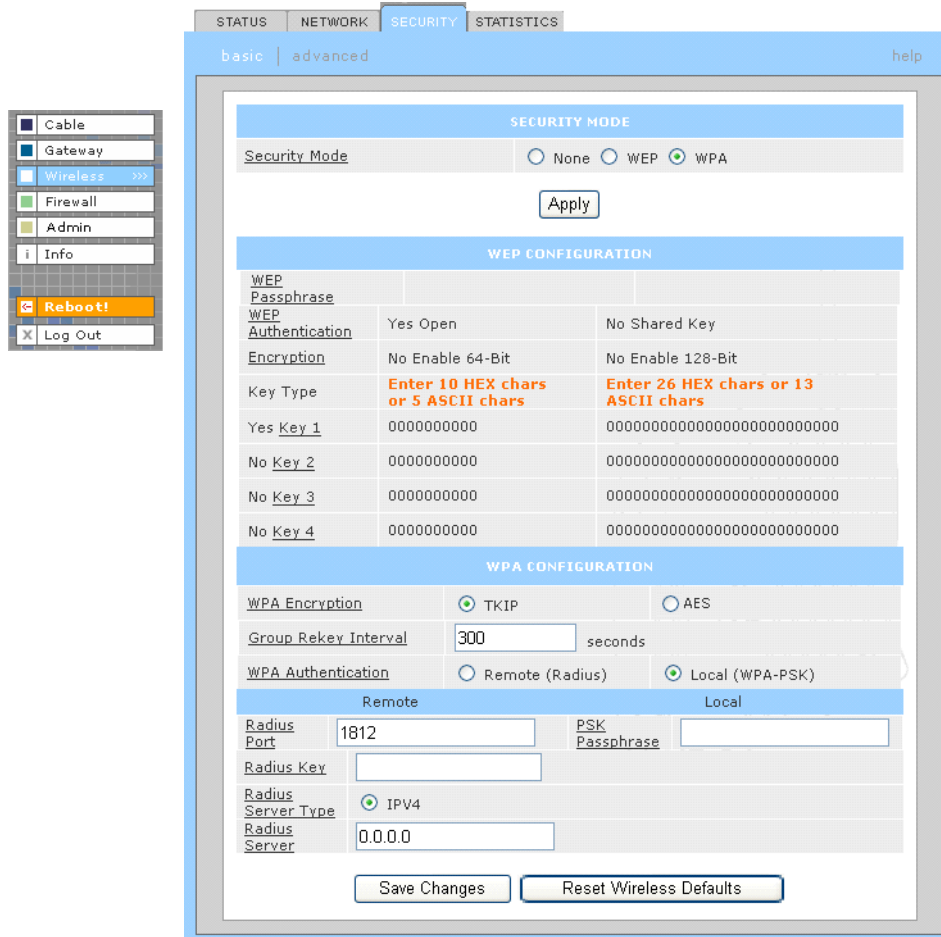
- Provides much stronger encryption and is more secure
- Provides authentication to ensure that authorized users *only* can log in to your WLAN
- Is much easier to configure
- Uses a standard algorithm on all compliant products to generate a key from a textual passphrase
- Will be incorporated into the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

For new wireless LANs, we recommend purchasing client adapters that support WPA, such as the [Motorola Wireless Notebook Adapter WN825G](#), [Wireless PCI Adapter WPCI810G](#), and [Wireless USB Adapter WU830G](#). For more information about the benefits of WPA, see the [Wi-Fi Protected Access](#) web page http://www.wifialliance.org/OpenSection/protected_access.asp.

Configuring WPA on the SBG940

To enable WPA and set the key on the SBG940:

- 1 On the SBG940 Setup Program left panel, click **Wireless**.
- 2 Click the **SECURITY** tab to display the Wireless > SECURITY — basic page:



The screenshot shows the SBG940 Setup Program interface. On the left is a sidebar with navigation options: Cable, Gateway, Wireless (selected), Firewall, Admin, Info, Reboot!, and Log Out. The main window has tabs for STATUS, NETWORK, SECURITY (selected), and STATISTICS. Below the tabs are 'basic' and 'advanced' sub-tabs, with 'basic' selected. The SECURITY tab displays the 'SECURITY MODE' section with radio buttons for None, WEP, and WPA (selected). An 'Apply' button is below. The 'WEP CONFIGURATION' section has fields for WEP Passphrase, WEP Authentication (Yes Open, No Shared Key), Encryption (No Enable 64-Bit, No Enable 128-Bit), and Key Type (Enter 10 HEX chars or 5 ASCII chars, Enter 26 HEX chars or 13 ASCII chars). Below are fields for Yes Key 1, No Key 2, No Key 3, and No Key 4. The 'WPA CONFIGURATION' section has WPA Encryption (TKIP selected, AES), Group Rekey Interval (300 seconds), and WPA Authentication (Remote (Radius), Local (WPA-PSK) selected). Below are fields for Radius Port (1812), Radius Key, Radius Server Type (IPv4 selected), and Radius Server (0.0.0.0). At the bottom are 'Save Changes' and 'Reset Wireless Defaults' buttons.

- 3 In the **Security Mode** field, select **WPA** and click **Apply**.
- 4 Under WPA CONFIGURATION, choose **one WPA Encryption** type. *Because performance may be slow with TKIP, we recommend choosing AES if your clients support AES:*

TKIP Temporal Key Integrity Protocol provides data encryption including a per-packet key mixing function, message integrity check (MIC), initialization vector (IV) and re-keying mechanism.

AES The Advanced Encryption Standard algorithm implements symmetric key cryptography as a block cipher using 128-bit keys. We recommend this setting if all of your wireless clients support AES. The Motorola client adapters shown in ["Optional Accessories"](#) support AES.



5 Choose the **WPA Authentication** type:

- Remote (Radius)** If a Remote Authentication Dial-In User Service ([RADIUS](#)) server is available, you can select this option and go to step 6. A RADIUS server is typically used in a large corporate location.
- Local (WPA-PSK)** If you choose Pre-Shared Key (PSK) local authentication, if the passphrase on any client supporting WPA matches the PSK Passphrase set on the SBG940, the client can access the SBG940 WLAN. To set the PSK Passphrase, go to step 7. A local key is typically used in a home or small office.

6 For **Remote (Radius)** authentication *only*, set:

- Radius Port** The port used for remote authentication through a RADIUS server. It can be from 0 to 65535.
- Radius Key** The key for remote authentication. It can be from 0 to 255 ASCII characters.
- Radius Server Type** Currently IPv4 *only*.
- Radius Server** The RADIUS server IP address in dotted-decimal format (xxx.xxx.xxx.xxx).

7 For **Local (WPA-PSK)** authentication *only*, set:

- PSK Passphrase** The PSK password containing from 8 to 63 ASCII characters. You must set the identical passphrase on each WLAN client (see "[Configuring a Wireless Client for WPA](#)").

8 Click **Save Changes**.

If you need to restore the wireless defaults, click **Reset Wireless Defaults**.

Configuring WEP on the SBG940

Use Wired Equivalent Privacy ([WEP](#)) only if you have wireless clients that do not support WPA.

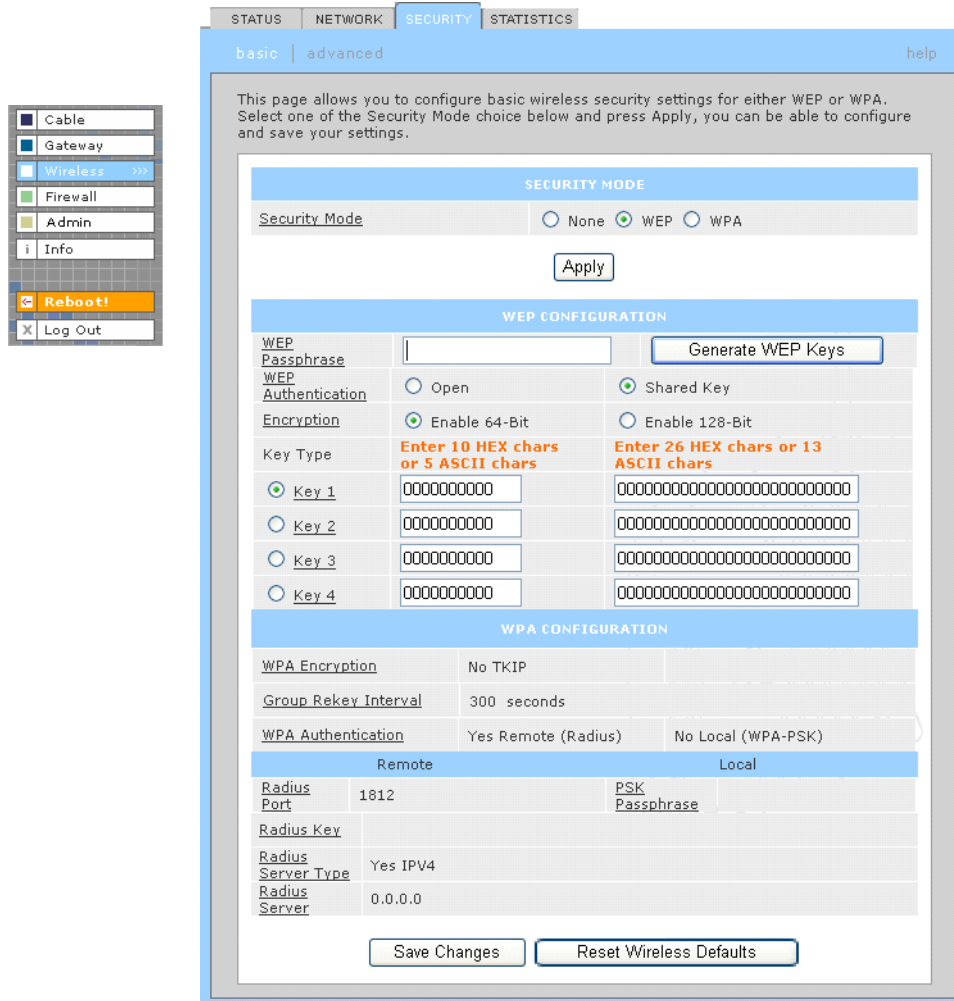
Caution!



If you use WEP encryption, you must configure the same WEP key on the SBG940 [access point](#) and all wireless clients (stations). *Never provide your WEP key or passphrase to anyone who is not authorized to use your WLAN.*

To enable WEP and set the key on the SBG940:

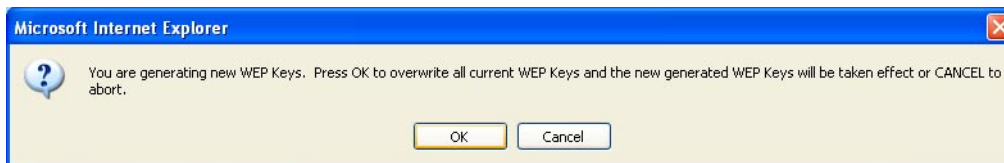
- 1 On the SBG940 Setup Program left panel, click **Wireless**.
- 2 Click the **SECURITY** tab to display the Wireless > SECURITY — basic page:



The screenshot shows the SBG940 Setup Program interface. On the left, a sidebar contains links: Cable, Gateway, **Wireless**, Firewall, Admin, Info, Reboot!, and Log Out. The main window has tabs for STATUS, NETWORK, **SECURITY**, and STATISTICS. The SECURITY tab is active, showing a 'basic' configuration page. The page title is 'SECURITY MODE'. Below the title, there's a 'Security Mode' section with radio buttons for 'None', 'WEP' (selected), and 'WPA'. An 'Apply' button is below. The 'WEP CONFIGURATION' section includes a 'WEP Passphrase' field, a 'Generate WEP Keys' button, 'WEP Authentication' (Open or Shared Key), 'Encryption' (Enable 64-Bit or 128-Bit), and a 'Key Type' section with instructions to enter 10 HEX chars or 5 ASCII chars. Below this are four key entries (Key 1 to Key 4) with text input fields. The 'WPA CONFIGURATION' section includes 'WPA Encryption' (No TKIP), 'Group Rekey Interval' (300 seconds), 'WPA Authentication' (Yes Remote (Radius) or No Local (WPA-PSK)), and a table for 'Remote' and 'Local' settings including Radius Port, Radius Key, Radius Server Type, and Radius Server. At the bottom are 'Save Changes' and 'Reset Wireless Defaults' buttons.

- 3 In the **Security Mode** field, select **WEP** and click **Apply**.
- 4 In the **WEP Passphrase** field, type a *passphrase* containing from 8 to 31 ASCII characters. For privacy, your passphrase displays as dots.

- 5 Click **Generate WEP Keys**. The following window is displayed:



- 6 Click **OK**. The WEP CONFIGURATION fields now appear something like:

WEP CONFIGURATION		
WEP Passphrase	••••••••	Generate WEP Keys
WEP Authentication	<input type="radio"/> Open	<input checked="" type="radio"/> Shared Key
Encryption	<input checked="" type="radio"/> Enable 64-Bit	<input type="radio"/> Enable 128-Bit
Key Type	Enter 10 HEX chars or 5 ASCII chars	Enter 26 HEX chars or 13 ASCII chars
<input checked="" type="radio"/> Key 1	e704d8bce7	e704d8bce78be042718adca8b2
<input type="radio"/> Key 2	718adca8b2	8f4c696d44d10d6b8222d1f978
<input type="radio"/> Key 3	8f4c696d44	ffb5918a1b024e93bd2475dc7
<input type="radio"/> Key 4	8222d1f978	cc1ad6dbfc137c898233206332

Before performing step 7, consider the following:

- If all of your wireless adapters support 128-bit encryption, you can select **Enable 128 Bit**. Otherwise, you must select **Enable 64 Bit**.
- For a WLAN client equipped with a Motorola wireless adapter, you can enter the WEP Passphrase when you perform [Configuring a Wireless Client for WEP](#). For all other wireless adapters, you will probably need to enter the generated WEP key that you designate in step 7.

- 7 Under WEP CONFIGURATION, set:

- WEP Authentication** Sets whether shared key authentication is enabled to provide data privacy on the WLAN:
- Open System — Any WLAN client can transmit data to any other client without authentication. It is the default, if the Security Mode is set to WEP.
 - Shared Key — The SBG940 authenticates and transfers data to and from all clients having shared key authentication enabled. *We recommend this setting.*
- Encryption** Use a WEP key length that is compatible with your wireless client adapters. Choose *one* of:
- Enable 64-Bit — Use only if you have wireless clients that do not support 128-bit encryption
 - Enable 128-Bit — We recommend this setting for stronger encryption; it is supported by the Motorola WN825G and WPCI810G wireless adapters and most current wireless adapters
- Key 1 to Key 4** Select the active key (1 to 4). Only *one* key can be active. You can generate WEP keys from a passphrase as described in steps 4 to 6 or type non-case-sensitive hexadecimal characters 0 to 9 and A to F to define up to:
- Four 10-character long key 64-bit WEP keys
 - Four 26-character long 128-bit WEP keys
- We recommend changing the WEP keys frequently. Never provide the WEP key to anyone who is not authorized to use your WLAN.*

- 8 Click **Save Changes** to save your changes.

If you need to restore the wireless defaults, click **Reset Wireless Defaults**.



Restricting Wireless LAN Access

The default SBG940 wireless settings enable any computer having a compatible wireless adapter to access your WLAN. To protect your network from unauthorized intrusions, you can restrict access to your WLAN to a limited number of computers on the [Wireless > SECURITY — advanced Page](#).

You can configure one or both of:

Configure on the SBG940

Perform [Configuring the Wireless Network Name on the SBG940](#) to disable **Extended Service Set Identifier (ESSID)** broadcasting to enable closed network operation

Perform [Configuring a MAC Access Control List on the SBG940](#) to restrict access to wireless clients with known MAC addresses

Required On Each Wireless Client

You must configure the identical ESSID (network name) to the SBG940.

No configuration is required on the client.



Configuring the Wireless Network Name on the SBG940

If you disable ESSID broadcasting on the SBG940, the SBG940 does not transmit the network name (ESSID). This provides additional protection because:

- Only wireless clients configured with your network name can communicate with the SBG940
- Unauthorized individuals who scan for unsecured WLANs cannot access your WLAN

Closed network operation is an enhancement of the IEEE 802.11b and IEEE 802.11g standards.

If you select *Disable ESSID Broadcast*, you must perform [Configuring a Wireless Client with the Network Name \(ESSID\)](#) on all WLAN *clients* (stations). Never provide your ESSID to anyone who is not authorized to use your WLAN.

To configure the ESSID on the SBG940:

- 1 Start the SBG940 Setup Program as described in “[Starting the SBG940 Setup Program](#)”.
- 2 On the left panel, click **Wireless**.
- 3 Click the **NETWORK** tab to display:

The screenshot shows the SBG940 Setup Program interface. On the left is a sidebar with navigation buttons: Cable, Gateway, Wireless (selected), Firewall, Admin, Info, Reboot!, and Log Out. The main window has tabs for STATUS, NETWORK (selected), SECURITY, and STATISTICS. The NETWORK tab displays a 'WIRELESS' section with the following settings: 'Enable Wireless Interface' is checked; 'ESSID' is set to 'Motorola'; 'Channel' is set to 1; and 'Operating Mode' is set to '11b/11g Standard'. Below this is an 'ADVANCED SETUP' section with 'Transmit Power' at 100 percent, 'RTS Threshold' at 2347 bytes, 'Fragmentation Threshold' at 2346 bytes, 'Beacon Period' at 100 milliseconds, and 'DTIM Period' at 3 beacons. At the bottom are 'Save Changes' and 'Reset Wireless Defaults' buttons.

- 4 In the **ESSID** field, type a unique **name**. It can be any alphanumeric, case-sensitive string up to 32 characters. The default is “Motorola.” *Do not use the default ESSID.*
- 5 Click **Save Changes** to save your changes.
- 6 To restrict WLAN access to clients configured with the same Network Name (ESSID) as the SBG940, click the **SECURITY** tab.



- 7 Click **advanced** to display the [Wireless > SECURITY — advanced](#) Page:

STATUS NETWORK SECURITY STATISTICS

basic | advanced help

This page allows you to configure advanced wireless security settings.

☒ [Disable ESSID Broadcast](#)

MAC ACCESS CONTROL LIST

☒ [Allow Any Station Access](#)
☐ [Allow Only Listed Stations Access](#)

Apply

STATIONS

#	Listed Stations	Delete
---	-----------------	--------

Delete

ADD NEW STATION

New Station
(e.g., 11:22:33:aa:bb:cc)

Add Station

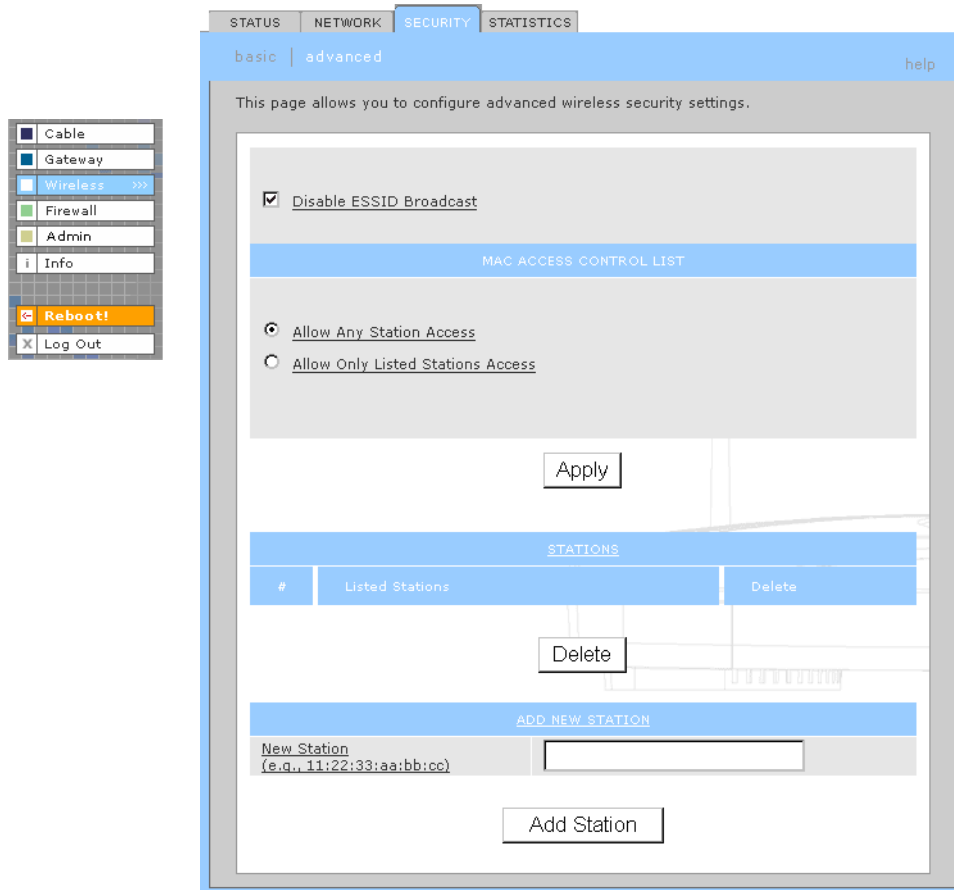
- 8 Select **Disable ESSID Broadcast** to restrict WLAN access to clients configured with the same Network Name (ESSID) as the SBG940.
- 9 Click **Apply** to save your changes.

Configuring a MAC Access Control List on the SBG940

You can restrict wireless access to one to 32 wireless clients, based on the client MAC address.

To configure a MAC access control list:

- 1 On the SBG940 Setup Program left panel, click **Wireless**.
- 2 Click the **SECURITY** tab.
- 3 Click **advanced** to display the [Wireless > SECURITY — advanced Page](#):



The screenshot shows the SBG940 Setup Program interface. On the left is a navigation pane with buttons for Cable, Gateway, Wireless (selected), Firewall, Admin, and Info. Below these are Reboot! and Log Out buttons. The main window has tabs for STATUS, NETWORK, SECURITY (selected), and STATISTICS. Under the SECURITY tab, there are sub-tabs for basic and advanced (selected). The advanced tab contains the text: "This page allows you to configure advanced wireless security settings." Below this is a section titled "MAC ACCESS CONTROL LIST". It has a checkbox for "Disable ESSID Broadcast" which is checked. Below that are two radio buttons: "Allow Any Station Access" (selected) and "Allow Only Listed Stations Access". An "Apply" button is below the radio buttons. Below the "Apply" button is a table titled "STATIONS". The table has three columns: "#", "Listed Stations", and "Delete". There is one row in the table with a "Delete" button next to it. Below the table is a section titled "ADD NEW STATION". It has a text input field with the placeholder "New Station (e.g., 11:22:33:aa:bb:cc)" and an "Add Station" button.

- 4 To restrict wireless access to systems in the MAC access control list, select **Allow Only Listed Stations Access** and click **Apply**.
- 5 To add a wireless client, type its MAC address in the format **xx:xx:xx:xx:xx:xx** in the **New Station** field and click **Add Station**.

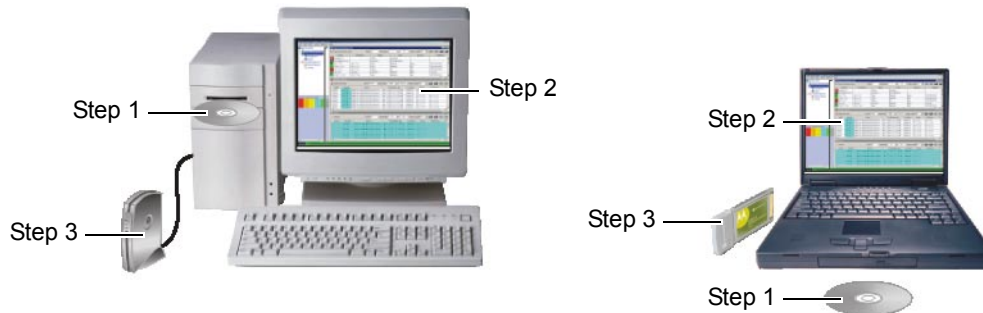
You can add up to 32 wireless clients to the MAC access control list.



Configuring the Wireless Clients

For each wireless client computer (station), install the wireless adapter — such as a Motorola [WN825G](#), [WPCI810G](#), or [WU830G](#) — following the instructions supplied with the adapter. Be sure to:

- 1 Insert the CD-ROM for the adapter in the CD-ROM drive on the client.
- 2 Install the device software from the CD.
- 3 Insert the adapter in the PCMCIA or PCI slot or connect it to the USB port.



Configure the adapter to obtain an IP address automatically. The Motorola wireless adapters are supplied with a client configuration program called Wireless Client Manager, which is installed in the Windows Startup group.

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 surf the Internet:

If You Performed

[Configuring WPA on the SBG940](#)

[Configuring WEP on the SBG940](#)

[Configuring the Wireless Network Name on the SBG940](#)

[Configuring a MAC Access Control List on the SBG940](#)

On Each Client, You Need to Perform

[Configuring a Wireless Client for WPA](#)

[Configuring a Wireless Client for WEP](#)

[Configuring a Wireless Client with the Network Name \(ESSID\)](#)

No configuration on client required



Configuring a Wireless Client for WPA

If you enabled WPA and set a PSK Passphrase by [Configuring WPA on the SBG940](#), you must configure the same passphrase (key) on each wireless client. The SBG940 cannot authenticate a client if:

- WPA is enabled on the SBG940 but not on the client
- The client passphrase does not match the SBG940 PSK Passphrase

For information about the WPA support in Windows XP, visit:

WPA Wireless Security for Home Networks

<http://www.microsoft.com/WindowsXP/expertzone/columns/bowman/03july28.asp>

Overview of the WPA Wireless Security Update in Windows XP

<http://support.microsoft.com/?kbid=815485>

You can download the Microsoft Windows XP Support Patch for Wi-Fi Protected Access from

<http://www.microsoft.com/downloads/details.aspx?FamilyId=009D8425-CE2B-47A4-ABEC-274845DC9E91&displaylang=en>

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 SBG940](#), you must configure the same WEP key on each wireless client. The SBG940 cannot authenticate a client if:

- Shared Key Authentication is enabled on the SBG940 but not on the client
- The client WEP key does not match the SBG940 WEP key

On a WLAN client equipped with a Motorola wireless adapter, you can enter the WEP Passphrase you set when you configured the SBG940. For all other wireless adapters, you must enter the 64-bit or 128-bit WEP key generated by the SBG940.

Caution!



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

Configuring a Wireless Client with the Network Name (ESSID)

To distinguish it from other nearby WLANs, you can identify your WLAN with a unique network name (also known as a network identifier or ESSID). When prompted for the network identifier, network name, or ESSID, type the **name** set in the ESSID field on the [Wireless > NETWORK Page](#) in the SBG940 Setup Program. For more information, see "[Configuring the Wireless Network Name on the SBG940](#)".

After you specify the network name, many wireless cards or adapters automatically scan for an access point such as the SBG940 and the proper channel and data rate. If your card requires you to manually start scanning for an access point, do so following the instructions in the documentation supplied with the card.

Never provide the ESSID to anyone who is not authorized to use your WLAN.



Wireless Pages in the SBG940 Setup Program

Use the Wireless pages to control and monitor the wireless interface:

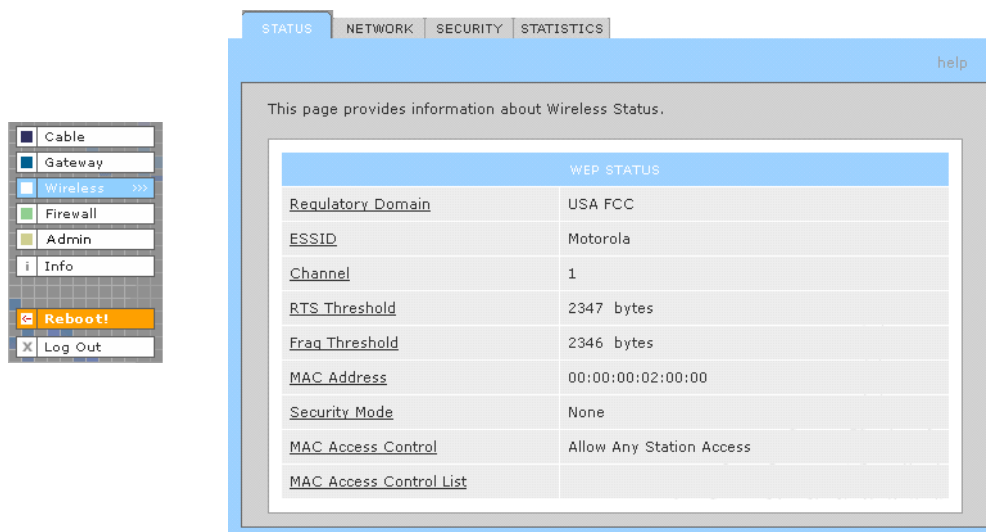
- [Wireless > STATUS Page](#)
- [Wireless > NETWORK Page](#)
- [Wireless > SECURITY — basic Page](#)
- [Wireless > SECURITY — advanced Page](#)
- [Wireless > STATISTICS page](#)

After you edit some fields and click Apply, you are warned that you must reboot for your change to take effect. Rebooting takes 10 to 15 seconds. After rebooting, you must log in again.

Wireless > STATUS Page

You can use this display-only page to:

- View the wireless interface status
- Help perform [Troubleshooting](#) for wireless network problems



Wireless > STATUS Page Fields

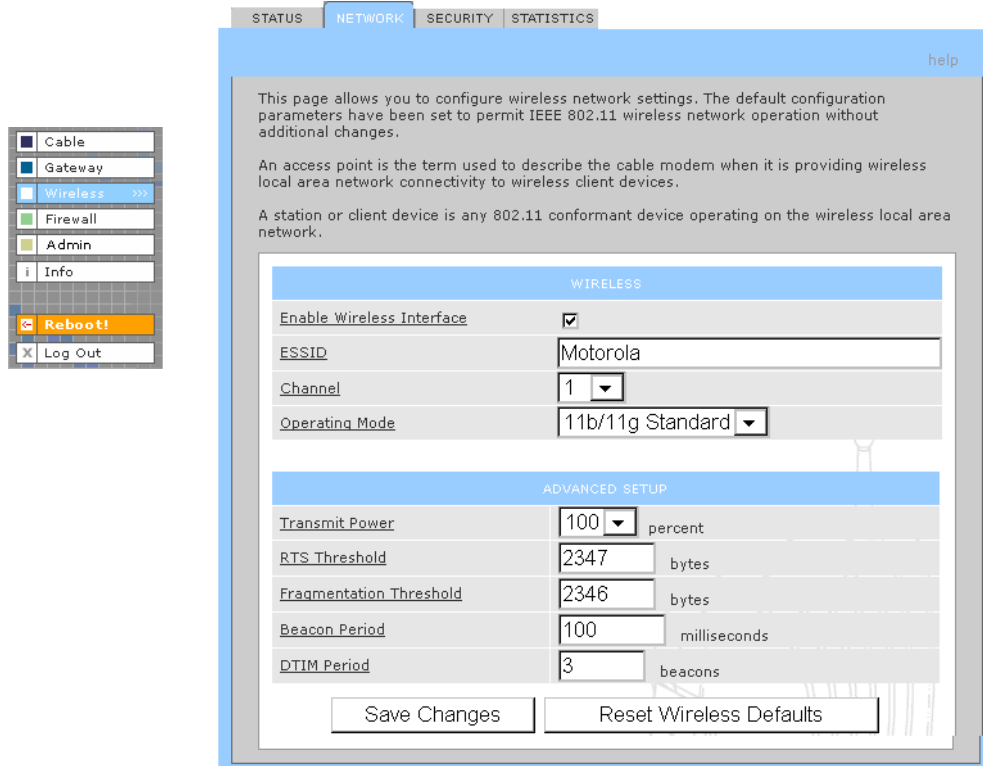
Regulatory Domain	Indicates the country the SBG940 is manufactured for. The list of channels depends on the country's standards for operation of wireless devices. Depending on the domain set at the factory, USA FCC, Europe, Spain, France, Japan, or some other country name is displayed.
ESSID	Displays the ESSID set on the Wireless > NETWORK Page . For more information, see " Configuring the Wireless Network Name on the SBG940 ". <i>Never provide the ESSID to anyone who is not authorized to use your WLAN.</i>
Channel	Displays the radio channel for the access point. If you encounter interference, you can set a different channel on the Wireless > NETWORK Page.
RTS Threshold	Displays the Request to Send Threshold set on the Wireless > NETWORK Page.
Frag Threshold	Displays the Fragmentation Threshold set on the Wireless > NETWORK Page.
MAC Address	Displays the SBG940 MAC address.
Security Mode	Displays the enabled wireless encryption type. For more information, see " Configuring WPA on the SBG940 " or " Configuring WEP on the SBG940 ".
MAC Access Control	Displays the MAC Access Control setting (see " Configuring a MAC Access Control List on the SBG940 "): <ul style="list-style-type: none"> • Allow Listed — Only clients in the MAC access control list can access the WLAN. • Allow Any Station Access — Any wireless client can access the WLAN.
MAC Access Control List	Displays the MAC addresses of wireless clients having access (see " Configuring a MAC Access Control List on the SBG940 ").

Wireless > NETWORK Page

Use this page for:

- [Configuring the Wireless Network Name on the SBG940](#)
- Configuring other WLAN settings

You can use the SBG940 to operate a WLAN without changing its default settings.



Wireless > NETWORK page fields

Field	Description
WIRELESS	
Enable Wireless Interface	Select this box to enable the wireless interface.
ESSID	Sets a unique network name for the SBG940 WLAN to distinguish between multiple WLANs in the vicinity. <i>If you select Disable ESSID Broadcast on the Wireless > SECURITY — advanced Page, all clients on the WLAN must have the same ESSID (network name) as the SBG940. It can be any alphanumeric, case-sensitive string up to 32 characters. The default is "Motorola." We strongly recommend not using the default. Never provide the ESSID to anyone who is not authorized to use your WLAN.</i>
Channel	Sets the wireless radio channel. You can change the channel if you encounter interference on the default channel. The default is 1 (one), except in countries where the first channel permitted for wireless operation is not one.

Wireless > NETWORK page fields (continued)

Field	Description
Operating Mode	Sets how the SBG940 communicates with wireless clients (stations): <ul style="list-style-type: none">• 11b/11g Standard — Enables all IEEE 802.11b and IEEE 802.11g clients to work with the SBG940. <i>We recommend using this default setting in most cases because it is more flexible.</i>• 11g Enhanced — Choose this option only if all IEEE 802.11g client adapters on the network support the performance-enhancing features of the IEEE 11g Enhanced mode. It is not supported by all IEEE 802.11g adapters.
ADVANCED SETUP	
Transmit Power	Sets the SBG940 wireless transmission power — 1, 2, 5, 10, 25, 50, or 100 mW. The default is 32 mW. Transmission power control is an optional IEEE 802.11b feature.
RTS Threshold	The Request To Send Threshold sets the minimum packet size for which the SBG940 issues an RTS before sending a packet. A low RTS Threshold can help when many clients are associated with the SBG940 or the clients are far apart and can detect the SBG940 but not each other. It can be 0 to 2347 bytes. The default is 2347.
Fragmentation Threshold	Sets the size at which packets are fragmented (sent as several packets instead of as one packet). A low Fragmentation Threshold can help when communication is poor or there is a significant interference. It can be 256 to 2346 bytes. The default is 2346.
Beacon Period	Sets the time between beacon frames sent by the SBG940 for wireless network synchronization. It can be from 1 to 999 ms. The default is 100 ms.
DTIM Period	The delivery traffic indication message (DTIM) period is the number of Beacon Periods that elapse before a wireless client operating in power save mode “listens” for buffered broadcast or multicast messages from the SBG940. It can be from 1 to 99999. The default is 3.



Wireless > SECURITY — basic Page

Use this page to configure how your SBG940 encrypts wireless transmissions. For information about using this page, see “[Encrypting Wireless LAN Transmissions](#)”. After you enable WEP or WPA on the SBG940, you must configure each WLAN client as described in “[Configuring the Wireless Clients](#)”.

☐ Cable

☐ Gateway

☒ Wireless >>>

☐ Firewall

☐ Admin

☐ Info

Reboot!

Log Out

STATUS

NETWORK

SECURITY

STATISTICS

basic | advanced

help

SECURITY MODE

Security Mode

☐ None
 ☐ WEP
 ☒ WPA

WEP CONFIGURATION

WEP Passphrase		
WEP Authentication	Yes Open	No Shared Key
Encryption	No Enable 64-Bit	No Enable 128-Bit
Key Type	Enter 10 HEX chars or 5 ASCII chars	Enter 26 HEX chars or 13 ASCII chars
Yes Key 1	0000000000	00000000000000000000000000000000
No Key 2	0000000000	00000000000000000000000000000000
No Key 3	0000000000	00000000000000000000000000000000
No Key 4	0000000000	00000000000000000000000000000000

WPA CONFIGURATION

WPA Encryption

☒ TKIP
 ☐ AES

Group Rekey Interval

300 seconds

WPA Authentication

☐ Remote (Radius)
 ☒ Local (WPA-PSK)

Remote

Radius Port

1812

Radius Key

Local

PSK Passphrase

Radius

Radius Server Type

IPV4

Radius Server

0.0.0.0

Caution!



The default Security Mode setting None provides no security for transmitted data.



Wireless > SECURITY — advanced Page

Use this page to configure advanced wireless security settings.

Wireless > Security — ADVANCED page fields

Field or Button	Description
Disable ESSID Broadcast	If selected, only wireless clients (stations) having the same Network Name (ESSID) as the SBG940 can communicate with the SBG940. Closed network operation is a SBG940 enhancement to IEEE 802.11b. The default is not selected (off).
MAC ACCESS CONTROL LIST	You can restrict wireless access to one to 32 wireless clients, based on the client MAC address.
Allow Any Station Access	If selected, any wireless client can access the SBG940 WLAN.
Allow Only Listed Stations Access	If selected, only wireless clients in the MAC access control list can access the SBG940 WLAN.
Apply	Click to apply your change.
Listed Stations	Lists the wireless clients in the MAC access control list having access if Allow Only Listed Stations Access is selected.
Delete	To delete a wireless client from the MAC access control list, select its Delete check box and click the Delete button.

**Wireless > Security — ADVANCED page fields (continued)****Field or Button****Description****ADD NEW STATION****New Station**

Type the MAC address of the wireless client to add to the MAC access control list. Use the format xx:xx:xx:xx:xx:xx. The MAC access control list can contain one to 32 clients.

Add Station

Click to add the New Station to the MAC access control list.

Wireless > STATISTICS page

Use this page to display wireless statistics.

WIRELESS STATISTICS	
Transmitted Fragment Count	395
Multicast Transmitted Fragment Count	395
Failed Count	0
Retry Count	0
Multiple Retry Count	0
Frame Duplicate Count	0
Request to Send Success Count	0
Request to Send Failure Count	0
Acknowledge Failed Count	7
Received Fragment Count	0
Multicast Received Fragment Count	14
Frame Check Sequence Error Count	0
Transmitted Frame Count	395
WEP Undecryptable Count	0

Refresh

Wireless > STATISTICS page fields**Field or Button****Description****Transmitted Fragment Count**

The number of acknowledged MAC protocol data units (MPDUs) with an address in the address 1 field or an MPDU with a multicast address in the address 1 field of type data or management.

Multicast Transmitted Fragment Count

The number of transmitted fragments when the multicast bit is set in the destination MAC address of a successfully transmitted MAC service data unit (MSDU). When operating as a STA in an ESS, where these frames are directed to the AP, this implies having received an acknowledgment to all associated MPDUs.

Failed Count

The number of MSDUs not transmitted successfully because the number of transmit attempts exceeded the IEEE 802.11b short or long retry limit.

Retry Count

The number of successfully transmitted MSDUs after one or more retransmissions.

**Wireless > STATISTICS page fields (continued)****Field or Button Description**

Multiple Retry Count	The number of successfully transmitted MSDUs after more than one retransmission.
Frame Duplicate Count	The number of frames received where the Sequence Control field indicated the frame was a duplicate.
Request To Send Success Count	The number of CTS messages received in response to RTS messages.
Request To Send Failure Count	The number of CTS messages not received in response to RTS messages.
Acknowledge Failed Count	The number of acknowledgment messages not received when expected from a data message transmission.
Received Fragment Count	The number of successfully received MPDUs of type Data or Management.
Multicast Received Fragment Count	The number of MSDUs received when the multicast bit was set in the destination MAC address.
Frame Check Sequence Error Count	The number of FCS errors detected in a received MPDU.
Transmitted Frame Count	The number of successfully transmitted MSDUs.
WEP Undecryptable Count	This number of frames received with the WEP subfield of the Frame Control field set to one and the WEP On key value mapped to the client MAC address. This indicates that the frame should not have been encrypted or was discarded due to the receiving client not having WEP enabled.
Refresh	Click to collect new data.



❖ Setting Up a USB Driver

The following subsections describe setting up a USB driver if you connect a PC to the USB port on the SBG940. Before connecting a PC to the USB port, perform *one* of the following procedures based on your Windows version:

- [Setting Up a USB Driver in Windows 98](#)
- [Setting Up a USB Driver in Windows 2000](#)
- [Setting Up a USB Driver in Windows Me](#)
- [Setting Up a USB Driver in Windows XP](#)

The SBG940 USB driver does not support Macintosh or UNIX computers. For those systems, you can connect through Ethernet *only*.

Caution!



Be sure the SBG940 Installation CD-ROM is inserted in the CD-ROM drive before you plug in the USB cable.

If you have a problem setting up the USB driver, remove it by performing *one* of:

- [Removing the USB Driver from Windows 98 or Windows Me](#)
- [Removing the USB Driver from Windows 2000](#)
- [Removing the USB Driver from Windows XP](#)

Then perform "[Running the Motorola USB Driver Removal Utility](#)" on page 104.



Setting Up a USB Driver in Windows 98

- 1 Insert the SBG940 Installation CD-ROM in the CD-ROM drive. This CD contains the USB drivers and must be inserted and read by the PC before you connect the SBG940 to the PC.
- 2 Connect the USB cable as shown in [USB Connection](#).

A few seconds after you complete the USB connection, the Add New Hardware Wizard window is displayed:



- 3 Click **Next**. The following window is displayed:



- 4 Be sure "Search for the best driver for your device" is selected.

- 5 Click **Next**. The following window is displayed:



Be sure "CD-ROM drive" is the only box selected.

- 6 Click **Next**. The message "Please wait while Windows searches for a new driver for this device" is displayed. If the computer successfully locates the driver, you can skip to step 9. If the computer does not locate the driver, the previous window is displayed again.
- 7 Select **Specify a location** and type the location of the CD-ROM drive:



To load the driver successfully, you may need to click **Browse** to manually select the NetMotCM.sys file on the CD-ROM.

- 8 Click **Next**. The following window is displayed:



- 9 Select **The updated driver...** and click **Next**. If the following window is not displayed, verify that the *SBG940 Installation* CD-ROM is properly inserted in the CD-ROM drive. If you still cannot find the correct driver file, click **Cancel** to cancel the installation and perform the procedure for ["Removing the USB Driver from Windows 98 or Windows Me"](#). Then repeat this procedure.

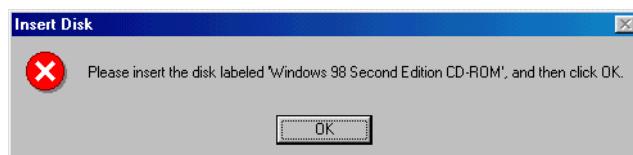


Although your SBG model number may be different than in the images in this guide, the procedure is the same.

- 10 After the window shown under step 9 is displayed, click **Next**.

If a window with the message *Copying Files...* displays and asks for the CD-ROM drive, type the CD-ROM drive **letter** (for example, "D:") and click **OK**.

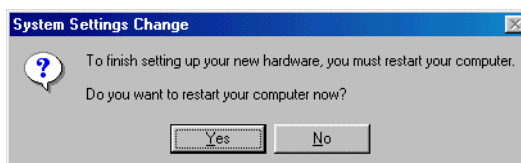
If an Insert Disk window similar to the one below is displayed, Windows 98 system files are needed to complete the installation. To install the files, insert your Windows 98 CD-ROM in the CD-ROM drive and click **OK**.



After all the necessary files are loaded, the following window is displayed to confirm a successful installation:



- 11** Click **Finish**. The Systems Settings Change window is displayed:



- 12** Click **Yes** to restart the computer.

When you finish setting up the USB driver, you can continue with “[Configuring TCP/IP](#)”.

If you have difficulties setting up the USB driver, perform “[Removing the USB Driver from Windows 98 or Windows Me](#)” and repeat this procedure. If that does not correct the problem, see the *Regulatory, Safety, Software License, and Warranty Information* card provided with the SBG940 for information about obtaining warranty service.



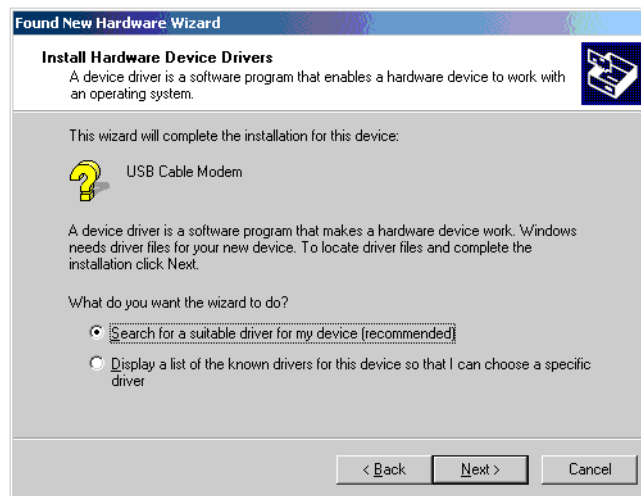
Setting Up a USB Driver in Windows 2000

- 1 Insert the SBG940 Installation CD-ROM in the CD-ROM drive. This CD contains the USB drivers and must be inserted and read by the PC before you connect the SBG940 to the PC.
- 2 Connect the USB cable as shown in [USB Connection](#).

A few seconds after you complete the USB connection, the Found New Hardware window is displayed:



- 3 Click **Next**. The following window is displayed:

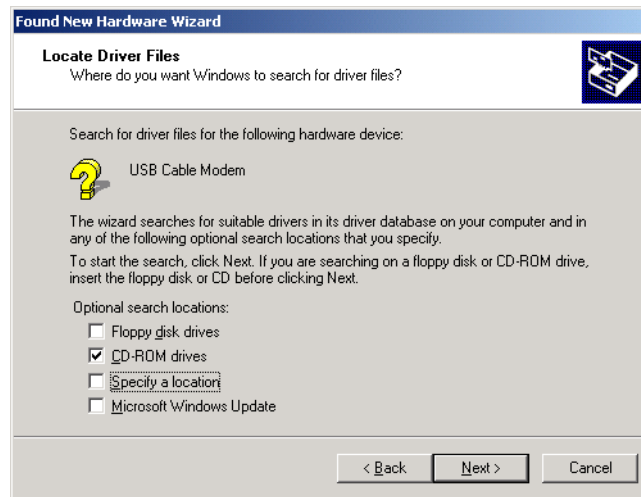


Although your SBG model number may be different than in the images in this guide, the procedure is the same.

Be sure "Search for a suitable driver for my device" is selected.

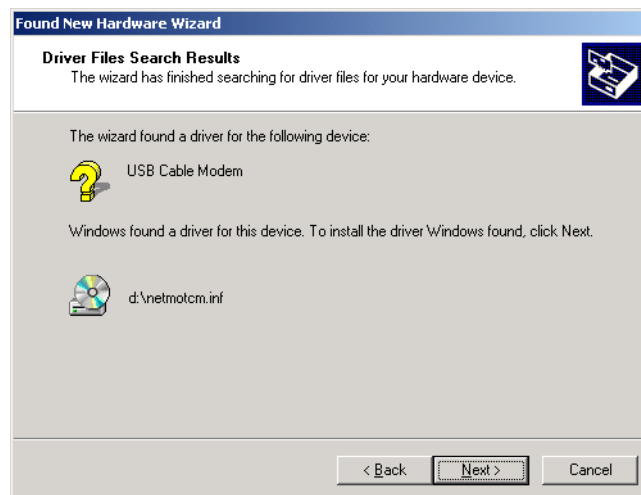


- 4 Click **Next**. The following window is displayed:



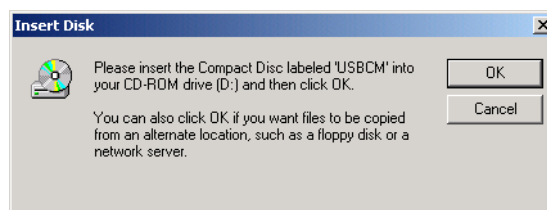
Be sure “CD-ROM drives” is the only box selected.

- 5 Click **Next**. The following window is displayed:



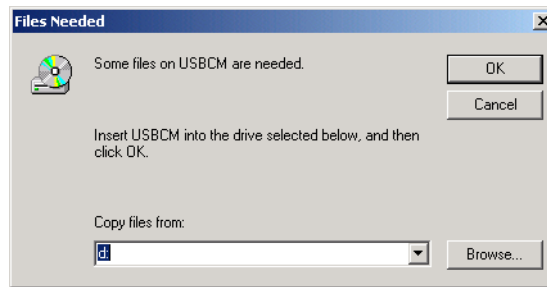
- 6 Click **Next**.

If the Insert Disk window is displayed, be sure the *SBG940 Installation* CD-ROM is in the CD-ROM drive and follow steps 7 to 12. Otherwise, you can skip to step 13.

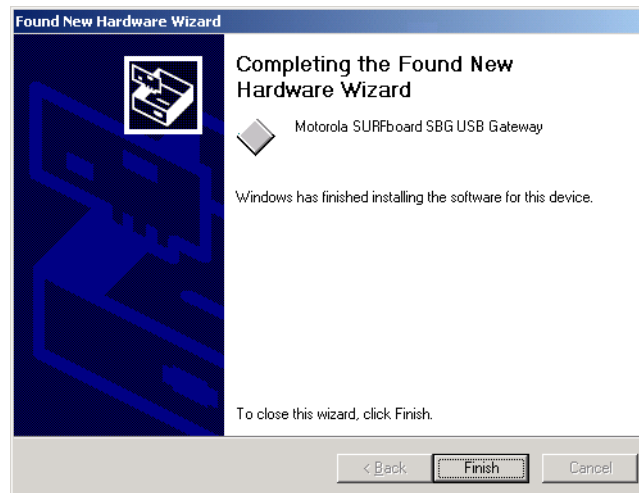




- 7 On the Insert Disk window, click **OK**. The Files Needed window is displayed:



- 8 If necessary, select the CD-ROM drive in the Copy files from list.
- 9 Click **Browse**.
- 10 Locate the NetMotCM.sys file in the CD-ROM root directory.
- 11 Double-click the **NetMotCM.sys** file. The Files Needed window is displayed.
- 12 Click **OK**. The Found New Hardware Wizard window is displayed:



- 13 Click **Finish** to complete the installation.

When you finish setting up the USB driver, you can continue with "[Configuring TCP/IP](#)".

If you have any difficulties setting up the USB driver, perform "[Removing the USB Driver from Windows 2000](#)" and repeat this procedure.

Setting Up a USB Driver in Windows Me

- 1 Insert the *SBG940 Installation CD-ROM* in the CD-ROM drive. This CD contains the USB drivers and must be inserted and read by the PC before you connect the SBG940 to the PC.

- 2 Connect the USB cable as shown in [USB Connection](#).

A few seconds after you complete the USB connection, the Add New Hardware Wizard window is displayed:



- 3 Click **Next**. Windows automatically searches for the correct USB drivers and installs them. If the installation is successful, the following window is displayed:



Although your SBG model number may be different than in the images in this guide, the procedure is the same.

- 4 If the window above is displayed, click **Finish**. Otherwise, be sure the *SBG940 Installation CD-ROM* is correctly inserted in the CD-ROM drive.

When you finish setting up the USB driver, you can continue with ["Configuring TCP/IP"](#).

Setting Up a USB Driver in Windows XP

- 1 Insert the *SBG940 Installation CD-ROM* in the CD-ROM drive. This CD contains the USB drivers and must be inserted and read by the PC before you connect the SBG940 to the PC.
- 2 Connect the USB cable as shown in [USB Connection](#).

A few seconds after you complete the USB connection, the Found New Hardware Wizard window is displayed:



- 3 Be sure "Install the software automatically" is selected.
- 4 Click **Next**. Windows automatically searches for the correct USB drivers and installs them. If the installation is successful, the following window is displayed:



Although your SBG model number may be different than in the images in this guide, the procedure is the same.

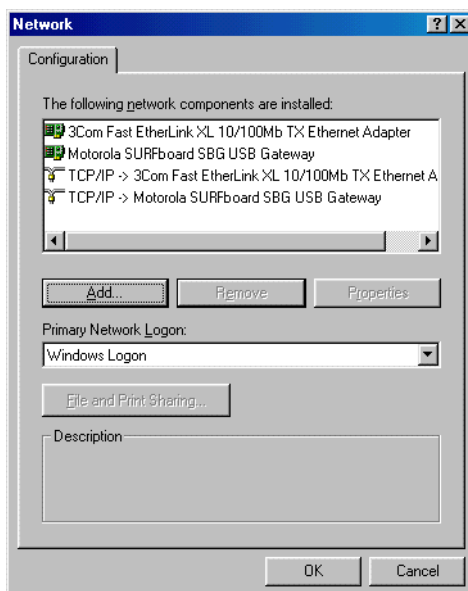
- 5 Click **Finish** to complete the installation. Otherwise, be sure the *SBG940 Installation CD-ROM* is correctly inserted in the CD-ROM drive.

When you finish setting up the USB driver, you can continue with ["Configuring TCP/IP"](#).

Removing the USB Driver from Windows 98 or Windows Me

- 1 On the Windows Desktop, right-click *one* of:
 - In Windows 98, the **Network Neighborhood** icon
 - In Windows ME, the **My Network Places** icon

The Network window is displayed:

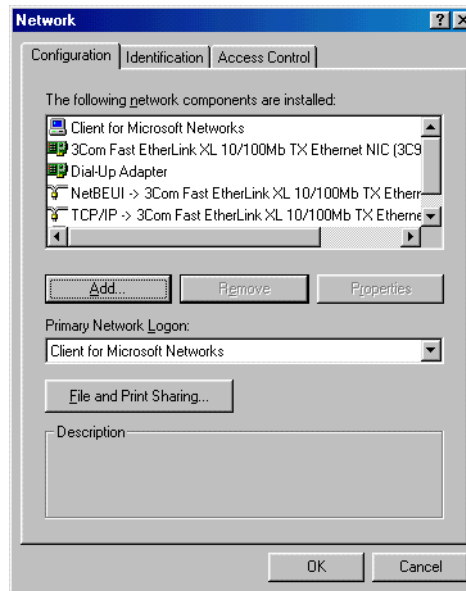


Although your SBG model number may be different than in the images in this guide, the procedure is the same.

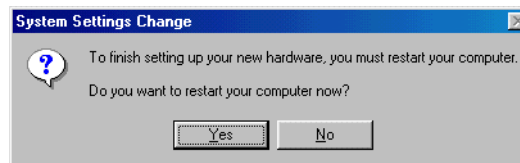
- 2 Click the **Motorola SURFboard SBG940 USB Gateway**.



- 3 Click **Remove**. The Network window no longer displays Motorola SURFboard SBG940 USB Gateway in the list:



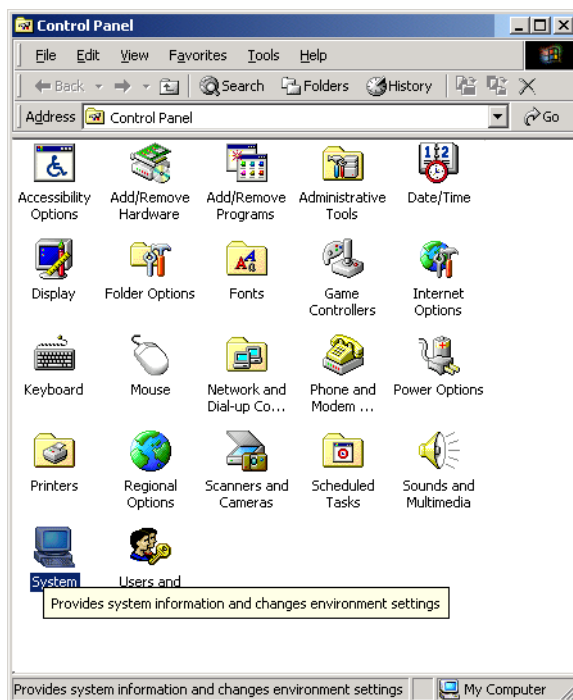
- 4 Click **OK**. The System Settings Change window is displayed:



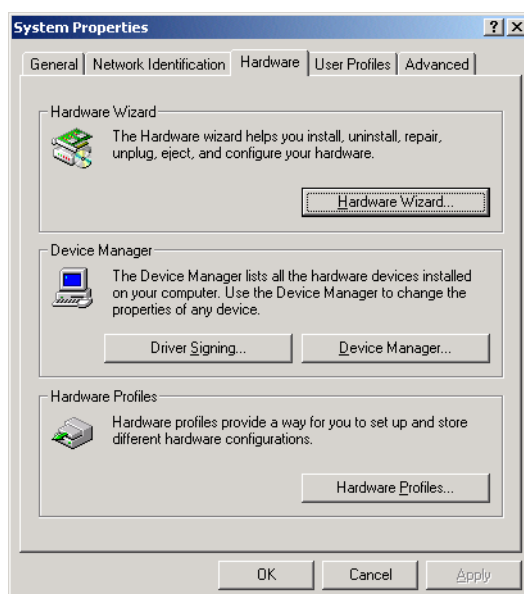
- 5 *Disconnect the USB cable from the PC or SBG940.*
- 6 Click **Yes** to restart the computer.
- 7 Perform "[Running the Motorola USB Driver Removal Utility](#)" on page 104.

Removing the USB Driver from Windows 2000

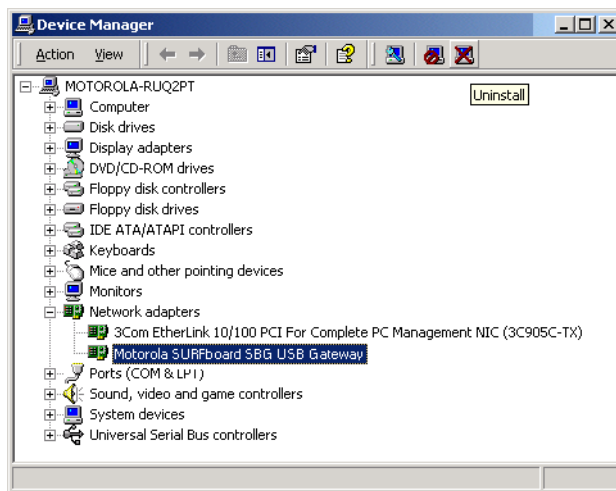
- 1 On the Windows desktop, click **Start**.
- 2 Click **Settings**.
- 3 Click **Control Panel** to display the Control Panel window:



- 4 Double-click **System** to display the System Properties window.
- 5 Click the **Hardware** tab:



- 6 Click **Device Manager** to display the Device Manager window:



Although your SBG model number may be different than in the images in this guide, the procedure is the same.

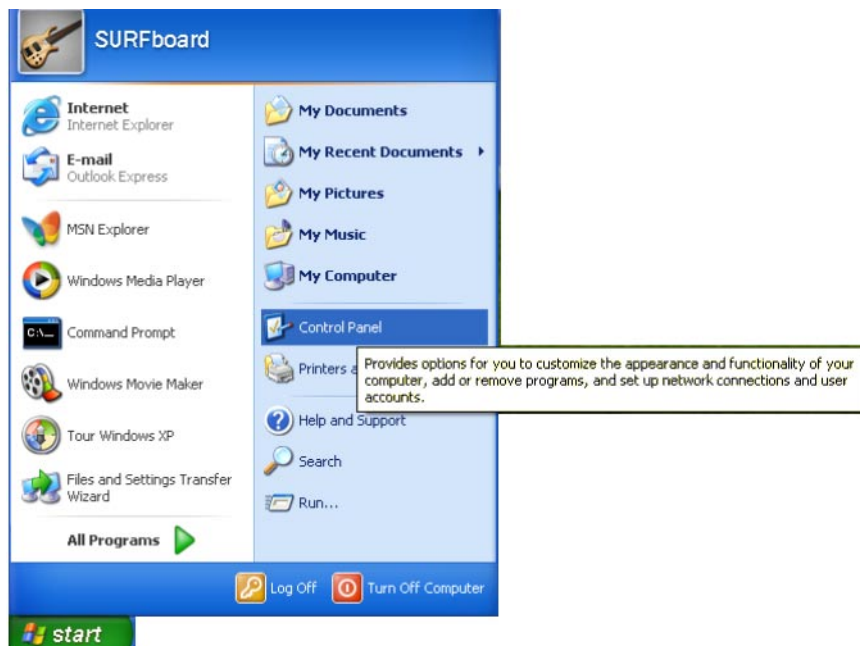
- 7 Double-click **Network Adapters**.
- 8 Click the **Motorola SURFboard SBG940 USB Gateway**. The Uninstall icon displays on the window near the top.
- 9 Click the **Uninstall** icon. The following window is displayed:



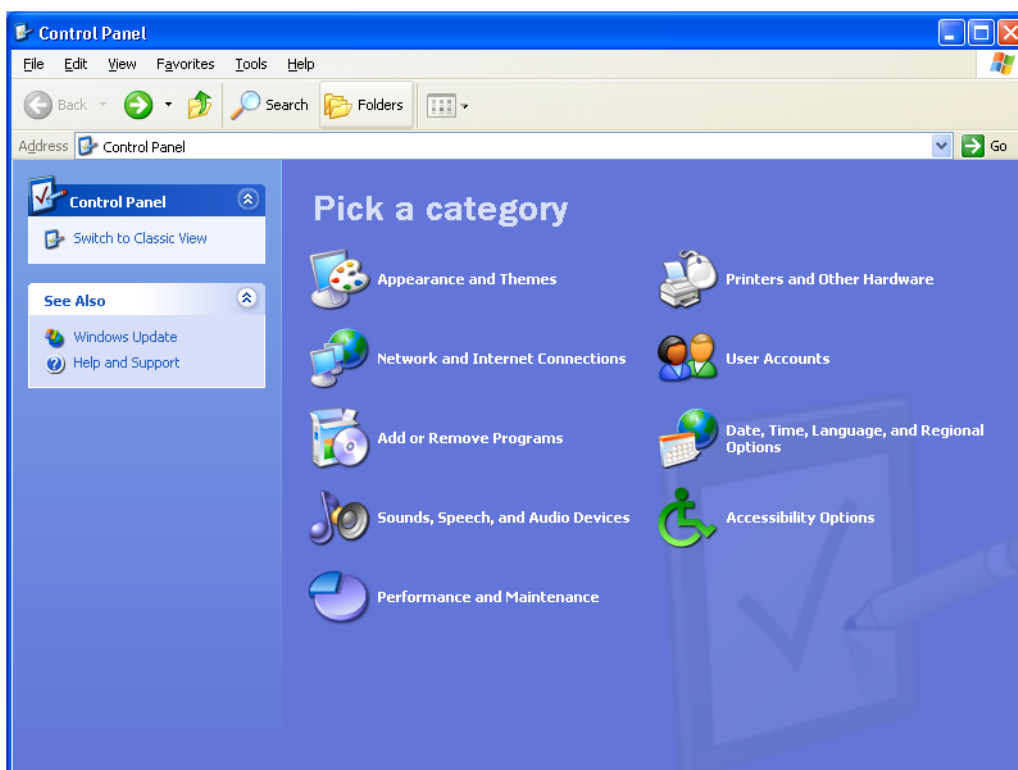
- 10 Click **OK**.
- 11 Close the Device Manager window.
- 12 Close the Control Panel window.
- 13 Perform “[Running the Motorola USB Driver Removal Utility](#)” on page 104.

Removing the USB Driver from Windows XP

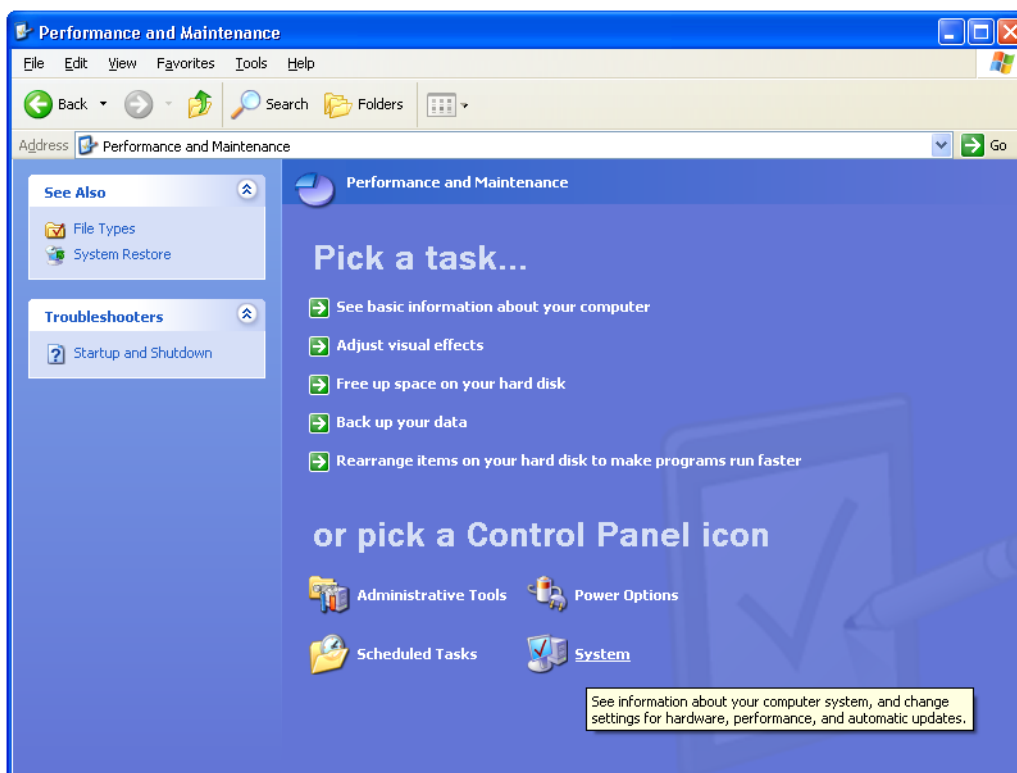
- 1 On the Windows desktop, click **Start** to display the Start window:



- 2 Click **Control Panel** to display the Control Panel window. The display varies, depending on the Windows XP view options:

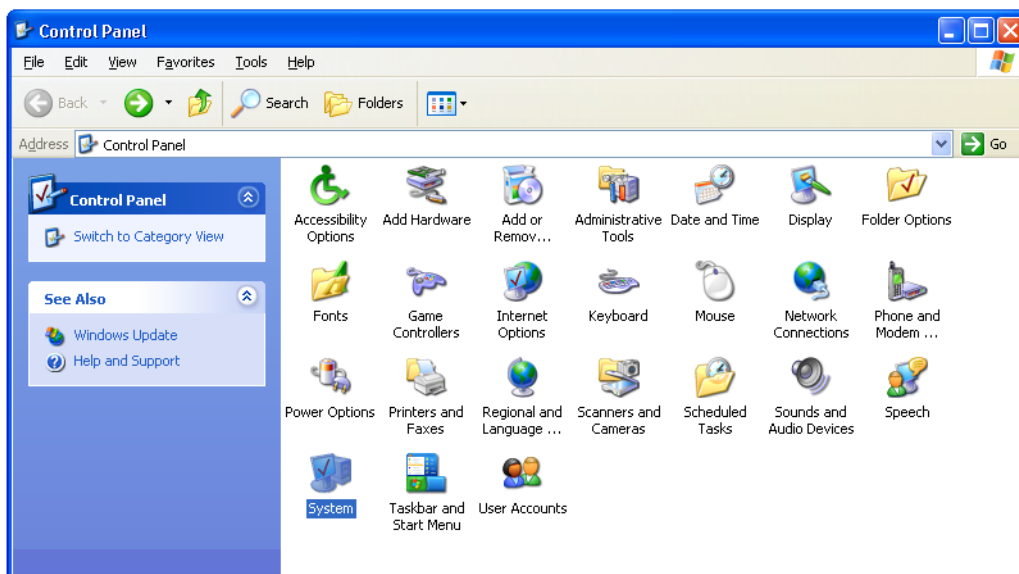


- 3 If a Category view similar to the image under step 2 is displayed, click **Performance and Maintenance** to display the Performance and Maintenance window. Otherwise, skip to step 5.

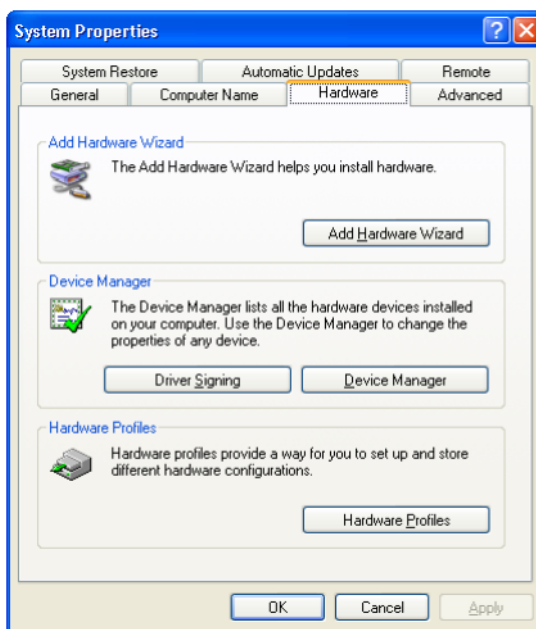


- 4 Click **System** to display the System Properties window. Skip to step 6.

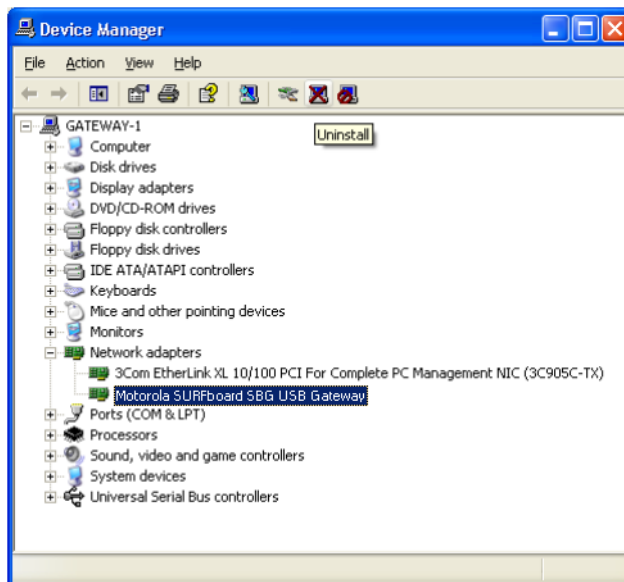
- 5 If a classic view similar to the following is displayed, double-click System to display the System Properties window:



- 6 Click the **Hardware** tab to display the Hardware page:



- 7 Click the **Device Manager** button to display the Device Manager window:



Although your SBG model number may be different than in the images in this guide, the procedure is the same.

- 8 Double-click **Network adapters**.
- 9 Click the **Motorola SURFboard SBG940 USB Gateway**. The Uninstall icon displays on the window near the top.
- 10 Click the **Uninstall** icon.
- 11 Close the Device Manager and Control Panel windows.
- 12 Perform “[Running the Motorola USB Driver Removal Utility](#)” on page 104.

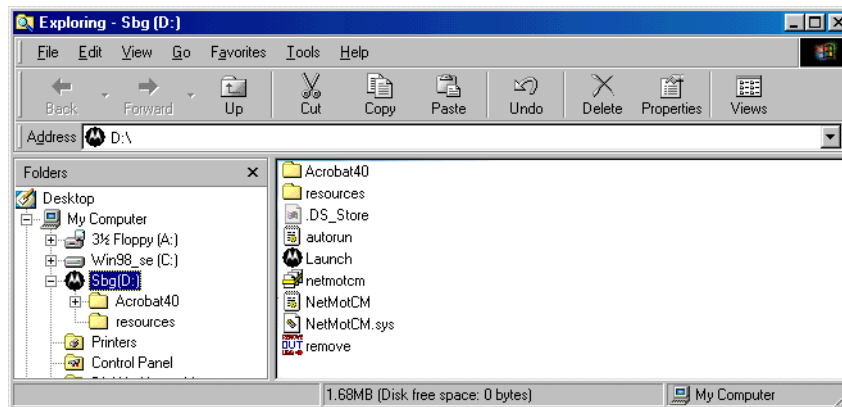
Running the Motorola USB Driver Removal Utility

Before running the Motorola USB Driver Removal Utility, you must run the Windows Device Manager by performing *one* of:

- “Removing the USB Driver from Windows 98 or Windows Me” on page 96
- “Removing the USB Driver from Windows 2000” on page 98
- “Removing the USB Driver from Windows XP” on page 100

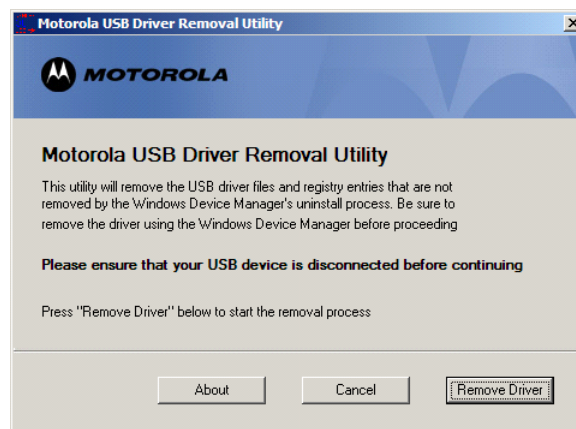
To run the Motorola USB Driver Removal Utility:

- 1 Insert the *SBG940 Installation* CD-ROM in the CD-ROM drive. After a short time, a window with language choices is displayed.
- 2 Press the **Esc** key on the keyboard to exit the start-up screens.
- 3 To start Windows Explorer, click **Start** and select **Run**. On the Run window, type **explorer** and click **OK**.



Your Windows Explorer may appear different than in the image on this page. There are variations between Windows versions and you can configure Windows Explorer as you like.

- 4 Double-click **My Computer**.
- 5 Double-click the **Motorola SBG** icon (D: in the image).
- 6 Double-click **remove** or **remove.exe** to run the Remove utility from the *SBG940 Installation* CD-ROM. The Motorola USB Driver Removal window is displayed. *Be sure the USB cable is disconnected.*



- 7 Click **Remove Driver**. A progress bar indicates that the driver is being removed.



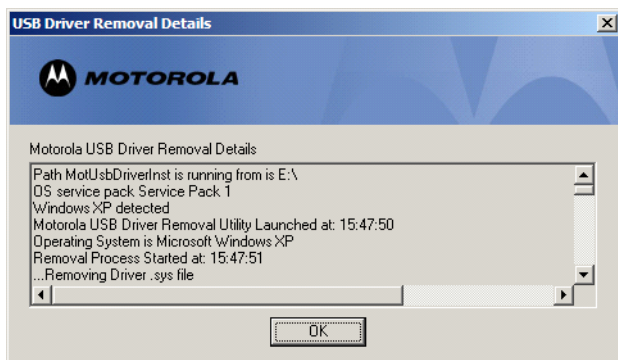
The following window displays when the USB driver has been successfully removed:



- 8 Click **Exit** to exit the Motorola USB Driver Removal Utility.

or

You can click **Details** to display informational messages about the files that were found and deleted, similar to the ones shown at left. If necessary, scroll down to view the entire list. Click **OK** to close the details window.



Re-install the USB driver following *one* of:

- [“Setting Up a USB Driver in Windows 98”](#) on page 87
- [“Setting Up a USB Driver in Windows Me”](#) on page 94
- [“Setting Up a USB Driver in Windows 2000”](#) on page 91
- [“Setting Up a USB Driver in Windows XP”](#) on page 95.

If you continue to have problems, contact your cable provider.



❖ Troubleshooting

If the solutions listed here do not solve your problem, contact your cable provider. Before calling your cable provider, try pressing the reset button on the rear panel. Resetting the SBG940 may take 5 to 30 minutes. Your service provider may ask for the status of the lights as described in [“Front-Panel Lights and Error Conditions”](#).

Problem

Possible Solutions



Power light is off

Check that the SBG940 is properly plugged into the electrical outlet.
 Check that the electrical outlet is working.
 Press the Reset button.

Cannot send or receive data

On the top front panel, note which is the first light (starting from the left) that is off. This light indicates where the error occurred as described in [“Front-Panel Lights and Error Conditions.”](#)
 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 SBG940 and wall outlet. Hand-tighten if necessary.
 Check the IP address. Follow the steps for verifying the IP address for your system. See [Configuring TCP/IP](#). Call your cable provider if you need an IP address.
 Check that the Ethernet cable is properly connected to the SBG940 and the computer.

Problems related to unsuccessful USB driver installation

Remove the USB driver. Follow the appropriate procedure for your system in [“Setting Up a USB Driver”](#).

The SBG940 Setup Program will not start

The web cache is full or close to full. In Internet Explorer, choose **Internet Options** from the **Tools** menu, and click the **General** tab. Click **Delete Files** and **Clear History**. Then try [Starting the SBG940 Setup Program](#) again.

A wireless client(s) cannot send or receive data

Perform the first four checks in [“Cannot send or receive data.”](#)

Check the **Security Mode** setting on the [Wireless > SECURITY — basic Page](#):

- If you enabled **WPA** and configured a passphrase on the SBG940, 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 SBG940, be sure each affected wireless client has the identical WEP key. If this does not solve the problem, check whether the client wireless adapter supports the type of WEP key configured on the SBG940.
- To temporarily eliminate the Security Mode as a potential issue, select None and click Apply. *After resolving your problem, be sure to re-enable wireless security.*

On the [Wireless > SECURITY — advanced Page](#):

- Check whether you turned on **Disable ESSID Broadcast**. If it is on, be sure the network name (ESSID) on each affected wireless client is identical to the ESSID on the SBG940.
- Check whether you enabled **Allow Only Listed Stations Access**. If you did, be sure the MAC address for each affected wireless client is correctly listed.

For detailed information, see [“Setting Up Your Wireless LAN”](#).

Slow wireless transmission speed with WPA enabled

On the [Wireless > SECURITY — basic Page](#), check whether the **WPA Encryption** type is TKIP. If all of your wireless clients support AES, change the WPA Encryption to AES as described in step 4 in [“Configuring WPA on the SBG940”](#).



Front-Panel Lights and Error Conditions

Light Turns Off During Startup If

DS The downstream receive channel cannot be acquired

US The upstream send channel cannot be acquired



IP registration is unsuccessful



The SBG940 is not properly plugged into the power outlet

Turns Off During Normal Operation If

The downstream channel is lost

The upstream channel is lost

The IP registration is lost

The SBG940 is unplugged



Contact Us

If you need assistance while working with the SBG940, contact your cable provider. For more information about customer service, technical support, or warranty claims, see the *Regulatory, Safety, Software License, and Warranty Information* card provided with the SBG940.

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

For more information about Motorola consumer cable products, education, and support, visit <http://broadband.motorola.com/consumers>.

Frequently-Asked Questions

Here are answers to questions our customers frequently ask:

Q What is high-speed cable Internet access?

A Cable Internet access uses cable television wires instead of telephone lines to connect to the Internet. It is extremely fast and does not tie up telephone lines for incoming or outgoing calls and faxes.

Q How fast is the Motorola SURFboard Cable Modem Gateway SBG940?

A Cable modems offer Internet access at speeds up to 100 times faster than a traditional phone modem. You can experience speeds of over 1,000 Kbps. Due to network condition such as traffic volume and the speed of the sites you visit, actual speed may vary. Many network and other factors can affect download speeds.

Q How many users can one SBG940 support?

A A single SBG940 can support up to 253 users, each assigned a unique IP address, on a Class C network.

Q What is Network Address Translation?

A NAT is a technique to translate private IP addresses on your LAN to a single IP address assigned by your cable provider that is that is visible to outside users on the Internet.

Q What are IEEE 802.11g and IEEE 802.11b?

A They are IEEE wireless network standards.

Q What type of firewall is provided on the SBG940?

A The SBG940 provides a [stateful-inspection](#) firewall. For more information, see [“Firewall”](#) and [“Setting the Firewall Policy”](#).

Q What wireless security measures are provided on the SBG940?

A To protect data transmitted over wireless connections, the SBG940 supports [WPA](#) or [WEP](#) encryption and [MAC](#) access control lists. For information, see [“Wireless Security”](#) and [“Setting Up Your Wireless LAN”](#).

Q Why is there no Standby button?

A As a security measure, current Motorola SURFboard cable modems provide a Standby button to temporarily suspend the Internet connection. Because enabling the SBG940 [firewall](#) provides high security levels while connected, the Standby button is not required.

Q Can I still watch cable TV while using my SBG940?

A Yes, your cable TV line can carry the TV signal while you send and receive information on the Internet.

Q What are CableLabs Certified, DOCSIS, and Euro-DOCSIS?

A CableLabs Certified, DOCSIS, and Euro-DOCSIS are the industry standards for high-speed data distribution over cable television system networks. They are intended to ensure that all compliant cable modems interface with all compliant cable systems. Your SBG940 is DOCSIS or Euro-DOCSIS certified.

Q If I have an SBG940, can I still use my old 28.8 Kbps or 56 Kbps modem?

A Yes you can. However, once you've experienced the speed of cable Internet access, you'll never again want to wait for traditional dial-up services.

Q Do I need to change my Internet service provider (ISP)?

A Currently, most Internet service providers do not provide cable Internet access. Contact your cable company for your specific information.

Q Do I need to subscribe to cable TV to get cable Internet access?

A No, but you will need to subscribe to cable Internet service. Some systems require that you subscribe to basic service before you can get Internet access and/or offer a discount when you use your own SBG940. Check with your local cable company for specific information.

Q What type of technical support is available?

A For questions about your Internet service, connection, or SBG940, call your cable provider.

Q What do I do if my SBG940 stops working?

A “[Troubleshooting](#)” provides tips to diagnose problems and simple solutions. If you continue to have problems, call your cable provider.

Q Can multiple game players on the SBG940 LAN log onto the same game server and play simultaneously with just one public IP address?

A It depends on the game server. For more information about gaming, see “[Gaming Configuration Guidelines](#)”.

Specifications

Wireless

Standards compliance	IEEE 802.11g, IEEE 802.11b DSSS, IEEE 802.11g OFDM
RF frequency range	2.412 to 2.462 GHz for North America 2.412 to 2.835 GHz for Japan
Data rate	1 Mbps DBPSK 2 Mbps DQPSK 5.5 or 11 Mbps CCK 6, 9, 12, 18, 24, 36, 48, or 54 Mbps OFDM
Modulation	1 Mbps DBPSK 2 Mbps DQPSK 5.5, 11 Mbps CCK 6, 9, 12, 18, 24, 36, 48, 54 Mbps OFDM
Number of channels	Europe = 13, Spain = 2, France = 4, US = 11, Japan = 14
Transmit power	+17 dBm (EIRP)
Receive sensitivity	-65 dBm at 54 Mbps

Router

Ethernet standards compliance	IEEE 802.3, IEEE 802.3u
Routing protocol	RIP V2
Number of uplink ports	4

Electrical

Input voltage range	100 – 240 VAC, 50 – 60 Hz
Power consumption	9 watts (nominal)

Environmental

Operating temperature	0° to 40° C, -150 to 10000 ft.
Storage temperature	-30° to 80° C
Humidity	5 to 95% RH, non-condensing

Antennas	One external removable antenna, with a unique connector per FCC requirements One external adjustable non-removable antenna
-----------------	---

LED Indicators	One Power, one Receive (DS), one Send (US), one Online, one Internet, one USB, one Wireless, and four Ethernet
-----------------------	--

Interfaces	One AC power, one F-type, one USB Series B, and four RJ-45
-------------------	--

Dimensions	290 mm (11.5 in.) wide x 160 mm (5.5 in.) deep x 70 mm (2.5 in) tall
-------------------	--

Weight	1.8 lbs (unit only)
---------------	---------------------

Downstream

Modulation	64 or 256 QAM
Maximum data rate ^a	38 Mbps
Frequency range	88 to 860 MHz (30 kHz minimum step size)
Bandwidth	6 MHz
Maximum symbol rate	5.069 Msym/s (64 QAM) 5.361 Msym/s (256 QAM)
Operating level range	-15 to +15 dBmV
Input impedance	75 ohms (nominal)
Frequency range	88 to 860 MHz

Upstream

Modulation	QPSK or 8 ^b , 16, 32 ^b , 64 ^b , or 128 ^b QAM
Modulation rate (nominal)	TDMA: 160, 320, 640, 1280, 2560, and 5120 KHz S-CDMA: 1280, 2560, and 5120 KHz
Maximum data rate ^c	30 Mbps
Bandwidth	TDMA: 200, 400, 800, 1600, 3200, and 6400 ^b kHz S-CDMA: 1600, 3200, and 6400 kHz
Symbol rates	160, 320, 640, 1280, and 2560 ksym/s
Operating level range (one channel)	TDMA: <ul style="list-style-type: none">• +8 to +54 dBmV (32 QAM, 64 QAM)• +8 to +55 dBmV (8 QAM, 16 QAM)• +8 to +58 dBmV (QPSK) S-CDMA: <ul style="list-style-type: none">• +8 to +53 dBmV (all modulations)
Output impedance	75 ohms nominal
Frequency range	5 to 42 MHz (edge to edge)
Output return loss	> 6 dB (5 to 42 MHz)

General

Cable interface	F-Connector, female, 75 ohm
CPE network interface	USB, Ethernet 10/100Base-T (auto sensing)
CPE wireless interface	IEEE 802.11g
Data protocol	TCP/IP

- Actual speed will vary. Upload and download speeds are affected by several factors including, but not limited to network traffic and services provided by your cable provider, computer equipment, server type, number of connections to the server, and the availability of Internet routers.
- With a CMTS supporting A-TDMA or S-CDMA *only*.
- Actual speed will vary. Maximum speed of 30 Mbps is only attainable with A-TDMA or S-CDMA technology.

Glossary

This glossary defines terms and lists acronyms used with the SBG940.

To return to your previous page, click the Acrobat Go to Previous View  button.

A

access point	A device that provides WLAN connectivity to wireless clients (stations). The SBG940 acts as a wireless access point.
adapter	A device or card that connects a computer, printer, or other peripheral device to the network or to some other device. A <i>wireless adapter</i> connects a computer to the WLAN.
address translation	See NAT.
ALG	Application level gateway triggers are required by some file transfer (for example, FTP), game, and video conferencing applications to open one or more ports to enable the application to operate properly.
American Wire Gauge (AWG)	A standard system used to designate the size of electrical conductors; gauge numbers are inverse to size.
ANSI	The American National Standards Institute is a non-profit, independent organization supported by trade organizations, industry, and professional societies for standards development in the United States. This organization defined ASCII and represents the United States to the International Organization for Standardization.
ANX	Automotive Network Exchange
ARP	Address Resolution Protocol broadcasts a datagram to obtain a response containing a MAC address corresponding to the host IP address. When it is first connected to the network, a client sends an ARP message. The SBG940 responds with a message containing its MAC address. Subsequently, data sent by the computer uses the SBG940 MAC address as its destination.
ASCII	The American Standard Code for Information Interchange refers to alphanumeric data for processing and communication compatibility among various devices; normally used for asynchronous transmission.
asynchronous timing	The SBG940 uses synchronous timing for upstream data transmissions. The CMTS broadcasts messages that bandwidth is available. The SBG940 reserves data bytes requiring x-number of mini-slots. The CMTS replies that it can receive data at a specified time (synchronized). At the specified time, the SBG940 transmits the x-number of data bytes.
attenuation	The difference between transmitted and received power resulting from loss through equipment, transmission lines, or other devices; usually expressed in decibels.
authentication	A process where the CMTS verifies that access is authorized, using a password, trusted IP address, or serial number.
authorization	Part of the process between a CMTS and the cable modem or gateway to enable Baseline Privacy.
auto-MDIX	Automatic medium-dependent interface crossover detects and corrects cabling errors by automatically reversing the send and receive pins on any port. It enables the use of straight-through wiring between the SBG940 Ethernet port and any computer, printer, or hub.

To return to your previous page, click the Acrobat Go to Previous View  button.

B

bandwidth	The transmission capacity of a medium in terms of a range of frequencies. Greater bandwidth indicates the ability to transmit more data over a given period of time.
Baseline Privacy	An optional feature that encrypts data between the CMTS and the cable modem or gateway. Protection of service is provided by ensuring that a cable modem or gateway, uniquely identified by its MAC address, can only obtain keys for services it is authorized to access.
baud	The analog signaling rate. For complex modulation modes, the digital bit rate is encoded in multiple bits per baud, for example, 64 QAM encodes 6 bits per baud and 16 QAM encodes 4 bits per baud.
BCP	Binary Communication Protocol
BER	The bit error rate is the ratio of the number of erroneous bits or characters received from some fixed number of bits transmitted.
binary	A numbering system that uses two digits, 0 and 1.
bit rate	The number of bits (digital 0s and 1s) transmitted per second in a communications channel. It is usually measured in bits per second bps.
BPKM	Baseline Protocol Key Management encrypts data flows between a cable modem or gateway and the CMTS. The encryption occurs after the cable modem or gateway registers to ensure data privacy across the RF network.
bps	bits per second
bridge	An OSI layer 2 networking device that connects two LANs using similar protocols. It filters frames based on the MAC address to reduce the amount of traffic. A bridge can be placed between two groups of hosts that communicate a lot together, but not so much with the hosts in the other group. The bridge examines the destination of each packet to determine whether to transmit it to the other side. See also <i>switch</i> .
broadband	High bandwidth network technology that multiplexes multiple, independent carriers to carry voice, video, data, and other interactive services over a single cable. A communications medium that can transmit a relatively large amount of data in a given time period. A frequently used synonym for cable TV that can describe any technology capable of delivering multiple channels and services.
broadcast	Simultaneous transmission to multiple network devices; a protocol mechanism supporting group and universal addressing. See also <i>multicast</i> and <i>unicast</i> .

To return to your previous page, click the Acrobat Go to Previous View  button.

C

CableHome	A project of CableLabs and technology suppliers to develop interface specifications for extending high-quality cable-based services to home network devices. It addresses issues such as device interoperability, QoS, and network management. CableHome will enable cable service providers to offer more services over HFC. It will improve consumer convenience by providing cable-delivered services throughout the home.
CableLabs	A research consortium that defines the interface requirements for cable modems and acknowledges that tested equipment complies with DOCSIS.
cable modem	A device installed at a subscriber location to provide data communications over an HFC network. Unless otherwise specified, all references to "cable modem" in this documentation refers to DOCSIS or Euro-DOCSIS cable modems <i>only</i> .
cable modem configuration file	File containing operational parameters that a cable modem or gateway downloads from the cable provider TFTP server during registration.
circuit-switched	Network-connection scheme used in the traditional PSTN telephone network where each connection requires a dedicated path for its duration. An alternative is packet-switched.
Class C network	An IP network containing up to 253 hosts. Class C IP addresses are in the form "network.network.network.host."
client	<p>In a client/server architecture, a client is a computer that requests files or services such as file transfer, remote login, or printing from the server. Also called a CPE.</p> <p>On a WLAN, a client is any host that can communicate with the access point. A wireless client is also called a "station."</p>
CMTS	A cable modem termination system is a device in the cable system headend that interfaces the HFC network to local or remote IP networks to connecting IP hosts, cable modems or gateways, and subscribers. It manages all cable modem bandwidth. It is sometimes called an edge router.
CNR	carrier to noise ratio
coaxial cable (coax)	A type of cable consisting of a center wire surrounded by insulation and a grounded shield of braided wire. The shield minimizes electrical and radio frequency interference. Coaxial cable has high bandwidth and can support transmission over long distances.
CoS	Class of service traffic management or scheduling functions are performed when transferring data upstream or downstream on HFC.
CPE	Customer premise equipment, typically computers, printers, etc., are connected to the cable modem or gateway at the subscriber location. CPE can be provided by the subscriber or the cable provider. Also called a client.
crosstalk	Undesired signal interfering with the desired signal.
CSMA/CD	carrier sense multiple access with collision detection

To return to your previous page, click the Acrobat Go to Previous View  button.

D

datagram	In RFC 1594, a datagram is defined as “a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.” For the most part, it has been replaced by the term packet.
default route	The route by which packets are forwarded when other routes in the routing table do not apply.
dB	decibel
dBc	Signal level expressed in dB relative to the unmodulated carrier level desired.
dBm	A unit of measurement referenced to one milliwatt across specified impedance. 0dBm = 1 milliwatt across 75 ohms.
dBmV	Signal level expressed in dB as the ratio of the signal power in a 75-ohm system to a reference power when 1 mV is across 75 ohms.
demodulation	An operation to restore a previously modulated wave and separate the multiple signals that were combined and modulated on a subcarrier.
DHCP	<p>A Dynamic Host Configuration Protocol server dynamically assigns IP addresses to client hosts on an IP network. DHCP eliminates the need to manually assign static IP addresses by “leasing” an IP address and subnet mask to each client. It enables the automatic reuse of unused IP addresses:</p> <p><i>The SBG940 is simultaneously a DHCP client and a DHCP server.</i></p> <ul style="list-style-type: none">• A DHCP server at the cable system headend assigns a public IP address to the SBG940 and optionally to clients on the SBG940 LAN.• The SBG940 contains a built-in DHCP server that assigns private IP addresses to clients.
distortion	An undesired change in signal waveform within a transmission medium. A nonlinear reproduction of the input waveform.
DMZ	A “de-militarized zone” is one or more hosts logically located between a private LAN and the Internet. A DMZ prevents direct access by outside users to private data. (The term comes from the geographic buffers located between some conflicting countries such as North and South Korea.) In a typical small DMZ configuration, the DMZ host receives requests from private LAN users to access external web sites and initiates sessions for these requests. The DMZ host cannot initiate a session back to the private LAN. Internet users outside the private LAN can access only the DMZ host. You can use a DMZ to set up a web server or for gaming without exposing confidential data.
DNS	The Domain Name System is the Internet system for converting domain names to IP addresses. A DNS server contains a table matching domain names such as Internetname.com to IP addresses such as 192.169.9.1. When you access the world-wide web, a DNS server translates the URL displayed on the browser to the destination website IP address. The DNS lookup table is a distributed Internet database; no one DNS server lists all domain name to IP address matches.
DOCSIS	The CableLabs Data-Over-Cable Service Interface Specification defines interface standards for cable modems, gateways, and supporting equipment to deliver data between an HFC network and a computer systems or television sets. To emphasize its use as a cable modem standard, DOCSIS is now called CableLabs Certified Cable Modems. Euro-DOCSIS is DOCSIS adapted for use in Europe.
domain name	A unique name, such as motorola.com, that maps to an IP address. Domain names are typically much easier to remember than are IP addresses.
DSSS	Direct Sequence Spread Spectrum

To return to your previous page, click the Acrobat Go to Previous View  button.

dotted-decimal format	Method of representing an IP address or subnet mask using four decimal numbers called octets. Each octet represents eight bits. In a class C IP address, the octets are "network.network.network.host." The first three octets together represent the network address and the final octet is the host address. In the SBG940 LAN default configuration, 192.168.100 represents the network address. In the final octet, the host address can be from 2 to 254.
download	To copy a file from one computer to another. You can use the Internet to download files from a server to a computer. A DOCSIS or Euro-DOCSIS cable modem or gateway downloads its configuration file from a TFTP server during start-up.
downstream	In a cable data network, the direction of data received by the computer from the Internet.
driver	Software that enables a computer to interact with a network or other device. For example, there are drivers for printers, monitors, graphics adapters, modems, Ethernet, USB, HPNA, and many others.
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum is an IEEE 802.11b RF modulation protocol.
dynamic IP address	An IP address that is temporarily leased to a host by a DHCP server. The opposite of <i>static IP address</i> .

E

encapsulate	To include data into some other data unit to hide the format of the included data.
encode	To alter an electronic signal so that only an authorized user can unscramble it to view the information.
encrypt	To encode data.
endpoint	A VPN endpoint terminates the VPN at the router so that computers on the SBG940 LAN do not need VPN client software to tunnel through the Internet to the VPN server.
ESSID	The Extended Service Set Identifier or network name is a unique identifier that wireless clients use to associate with an access point to distinguish between multiple WLANs in the same area. All clients on a WLAN must have the same ESSID as the access point. On the SBG940, you can set the ESSID on the Wireless > NETWORK page.
Ethernet	The most widely used LAN type, also known as IEEE 802.3. The most common Ethernet networks are 10Base-T, which provide transmission speeds up to 10 Mbps, usually over unshielded, twisted-pair wire terminated with RJ-45 connectors. Fast Ethernet (100Base-T) provides speeds up to 100 Mbps. "Base" means "baseband technology" and "T" means "twisted pair cable." Each Ethernet port has a physical address called the MAC address.
Euro-DOCSIS	A tComLabs standard that is DOCSIS adapted for use in Europe
event	A message generated by a device to inform an operator or the network management system that something has occurred.
expansion slot	A connection point in a computer where a circuit board can be inserted to add new capabilities.
EAP	Extensible Authentication Protocol

To return to your previous page, click the Acrobat Go to Previous View  button.

F

FCS	frame check sequence
F-type connector	A type of connector used to connect coaxial cable to equipment such as the SBG940.
firewall	A security software system on the SBG940 that enforces an access control policy between the Internet and the SBG940 LAN.
flow	A data path moving in one direction.
FEC	Forward error correction is a technique to correct transmission errors without requiring the transmitter to resend any data.
FDMA	Frequency Division Multiple Access is a method to allow multiple users to share a specific radio spectrum. Each active user is assigned an individual RF channel (or carrier) with the carrier frequency of each channel offset from its adjacent channels by an amount equal to the channel spacing, which allows the required bandwidth per channel.
frame	A unit of data transmitted between network nodes that contains addressing and protocol control data. Some control frames contain no data.
frequency	Number of times an electromagnetic signal repeats an identical cycle in a unit of time, usually one second, measured in Hz, kHz, MHz, or GHz.
FTP	File Transfer Protocol is a standard Internet protocol for exchanging files between computers. FTP is commonly used to download programs and other files to a computer from web pages on Internet servers.
full-duplex	The ability to simultaneously transmit and receive data. See also <i>half-duplex</i> .

G

gain	The extent to which a signal is boosted. A high gain antenna increases the wireless signal level to increase the distance the signal can travel and remain usable.
gateway	A device that enables communication between networks using different protocols. See also <i>router</i> . The SBG940 enables up to 253 computers supporting IEEE 802.11b, Ethernet, or USB to share a single broadband Internet connection.
gateway IP address	The address of the default gateway router on the Internet. Also known as the "giaddr."
GHz	Gigahertz — one billion cycles per second.
GUI	graphical user interface

To return to your previous page, click the Acrobat Go to Previous View  button.

H

H.323	A suite of protocols created by the ITU for interactive video-conferencing, data sharing, and audio applications such as VoIP.
half-duplex	Network where only one device at a time can transmit data. See also <i>full-duplex</i> .
headend	A location that receives TV programming, radio programming, data, and telephone calls that it modulates onto the HFC network. It also sends return data and telephone transmissions. Headend equipment includes transmitters, preamplifiers, frequency terminals, demodulators, modulators, and other devices that amplify, filter, and convert incoming broadcast TV signals to wireless and cable channels.
header	The data at the beginning of a packet that identifies what is in the packet.
hexadecimal	A base-sixteen numbering system that uses sixteen sequential numbers (0 to 9 and the letters A to F) as base units before adding a new position. On computers, hexadecimal is a convenient way to express binary numbers.
HFC	A hybrid fiber/coaxial cable network uses fiber-optic cable as the trunk and coaxial cable to the subscriber premises.
hop	The interval between two routers on an IP network. The number of hops a packet traverses toward its destination (called the hop count) is saved in the packet header. For example, a hop count of six means the packet has traversed six routers. The packet hop count increases as the time-to-live (TTL) value decreases.
host	<p>In IP, a host is any computer supporting end-user applications or services with full two-way network access. Each host has a unique host number that combined with the network number forms its IP address.</p> <p>Host also can mean:</p> <ul style="list-style-type: none">• A computer running a web server that serves pages for one or more web sites belonging to organization(s) or individuals• A company that provides this service• In IBM environments, a mainframe computer
HTML	Hyper Text Markup Language
hub	<p>On a LAN, a hub is a device that connects multiple hosts to the LAN. A hub performs no data filtering. See also <i>bridge</i> and <i>router</i>. An IP hub is typically a unit on a rack or desktop.</p> <p>On an HFC network, a hub is a scaled-down headend that performs some or all headend functions for part of the system.</p>
Hz	Hertz — one cycle per second. The unit to measure the frequency that an alternating electromagnetic signal cycles through its highest and lowest states. Used to define the bands of the electromagnetic spectrum used in voice and data communications, or to define the bandwidth of a transmission medium.

To return to your previous page, click the Acrobat Go to Previous View  button.

I

IANA	The Internet Numbering Address Authority (IANA) is an organization under the Internet Architecture Board (IAB) of the Internet Society that oversees IP address allocation. It is under a contract from the U.S. government.
ICMP	Internet Control Message Protocol is a protocol used for error, problem, and informational messages sent between IP hosts and gateways. ICMP messages are processed by the IP software and are not usually apparent to the end-user.
ICSA	The International Computer Security Association is the security industry's main source of research, intelligence, and product certification.
IEEE	The Institute of Electrical and Electronics Engineers, Inc. (http://www.ieee.org) is an organization that produces standards, technical papers, and symposiums for the electrical and electronic industries and is accredited by ANSI.
IEEE 802.11b IEEE 802.11g	IEEE wireless network standards.
IEEE 802.3	See <i>Ethernet</i> .
IETF	The Internet Engineering Task Force (http://www.ietf.org) is an open international community of network designers, operators, vendors, and researchers to develop and maintain Internet architecture. Technical working groups issue working documents called Internet-Drafts. The IETF publishes review versions of the drafts called requests for comments (RFCs).
IGMP	Internet Group Membership Protocol the Internet multicasting standard. IGMP establishes and maintains a database of group multicast addresses and interfaces to which a multicast router forwards multicast packets. IGMP runs between multicast hosts and their immediately-neighboring multicast routers.
IGMP spoofing	A process where a router acts as an IGMP querier for multicast hosts and an IGMP host to a multicast router.
impedance	The total opposition to AC electron current flow within a device. Impedance is typically 75 ohms for coax cable and other CATV components.
impulse noise	Noise of very short in duration, typically of the order of 10 microseconds. It is caused by electrical transients such as voltage spikes, electric motors turning on, and lightning or switching equipment that bleed over to the cable.
ingress noise	Noise typically caused by discrete frequencies picked up by the cable plant from radio broadcasts or an improperly grounded or shielded home appliance such as a hair dryer. Ingress is the major source of cable system noise.
Internet	A worldwide collection of interconnected networks using TCP/IP.
Internetwork	A collection of interconnected networks allowing communication between all devices connected to any network in the collection.
IP	Internet Protocol is a set of standards that enable different types of computers to communicate with one another and exchange data through the Internet. IP provides the appearance of a single, seamless communication system and makes the Internet a virtual network.

To return to your previous page, click the Acrobat Go to Previous View  button.

IP address	<p>A unique 32-bit value that identifies each host on a TCP/IP network. TCP/IP networks route messages based on the destination IP address. An IP address has two parts:</p> <ul style="list-style-type: none">• The network address is assigned by IANA.• The SBG940 network administrator assigns a host address to each host connected to the SBG940, automatically using its DHCP server or as a static IP address. <p>For a Class C network, the first 24 bits are the network address and the final 8 bits are the host address; in dotted-decimal format it appears "network.network.network.host."</p> <p>If you enable the SBG940 DHCP client on the WAN page, the cable provider automatically assigns the network address, subnet mask, domain name, and DNS server to provide a continuous Internet connection.</p>
IPSec	The Internet Protocol Security protocols are IETF authentication and encryption standards for secure packet exchange over the Internet. IPSec works at OSI layer 3 and secures everything on the network.
IKE	Internet Key Exchange
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
ISO	The International Organization for Standardization (http://www.iso.ch) is a worldwide federation of national standards bodies from approximately 140 countries. ISO is a non-governmental organization established in 1947 to promote the development of standardization and related activities in the world with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological, and economic activity.
ISP	Internet Service Provider
ITU	International Telecommunications Union

K

kHz	kilohertz — one thousand cycles per second
------------	--

To return to your previous page, click the Acrobat Go to Previous View  button.

L

L2F	Layer 2 Forwarding is an OSI layer 2 protocol that establishes a secure tunnel across the Internet to create a virtual PPP connection between the user and the enterprise network. L2F is the most established and stable layer 2 tunneling protocol.
L2TP	Layer 2 Tunnel Protocol is a PPP extension that enables ISPs to operate VPNs. L2TP merges the best features of the PPTP and L2F. L2TP is the emerging IETF standard.
LAC	An L2TP access concentrator is a device to which the client directly connects through which PPP frames are tunneled to the LNS. The LAC need only implement the media over which L2TP operates to transmit traffic to one or more LNSs. The LAC may tunnel any protocol carried within PPP. The LAC initiates incoming calls and receives outgoing calls. A LAC is analogous to an L2F NAS.
LAN	A local area network provides a full-time, high-bandwidth connection over a limited area, such as a building or campus. Ethernet is the most widely used LAN standard.
layer	In networks, layers are software protocol levels. Each layer performs functions for the layers above it. OSI is a reference model having seven functional layers.
LCP	Link Control Protocol establishes, configures, and tests data link connections used by PPP.
latency	The time required for a signal to pass through a device. It is often expressed in a quantity of symbols.
LED	light-emitting diode
LNS	An L2TP network server is a termination point for L2TP tunnels where PPP frames are processed and passed to higher layer protocols. An LNS can operate on any platform that terminates PPP. The LNS handles the server side of the L2TP protocol. L2TP relies only on the single media over which L2TP tunnels arrive. The LNS can have a single LAN or WAN interface but can terminate calls arriving at any of the LACs full range of PPP interfaces (asynchronous, synchronous, ISDN, V.120, etc.). The LNS initiates outgoing calls and receives incoming calls. An LNS is analogous to a home gateway in L2F technology.
loopback	A test that loops the transmit signal to the receive signal. Usually the loopback test is initiated on a network device. The test is used to verify a path or to measure the quality of a signal on that path.

To return to your previous page, click the Acrobat Go to Previous View  button.

M

MAC address	The Media Access Control address is a unique, 48-bit value permanently saved in ROM at the factory to identify each Ethernet network device. It is expressed as a sequence of 12 hexadecimal digits printed on a Label on the Bottom of the SBG940 . You need to provide the HFC MAC address to the cable provider. Also called an Ethernet address, physical address, hardware address, or NIC address.
MB	One megabyte; equals 1,024 x 1,024 bytes, 1,024 kilobytes, or about 8 million bits.
Mbps	Million bits per second (megabits per second). A rate of data transfer.
media	The various physical environments through which signals pass; for example, coaxial, unshielded twisted-pair (UTP), or fiber-optic cable.
MIB	A management information base is a unique hierarchical structure of software objects used by the SNMP manager and agent to configure, monitor, or test a device.
MHz	Megahertz — one million cycles per second. A measure of radio frequency.
MPDU	MAC protocol data unit (PDU)
MSDU	MAC service data unit
MSO	Multiple Systems Operator. A company that owns and operates more than one cable system. Also called a group operator.
MTU	The Maximum Transmission Unit is the largest amount of data that can be transmitted in one discrete message on a given physical network. The MTU places an upper bound on the size of a message that can be transferred by the network in a single frame. Messages exceeding the MTU must be fragmented before transmission, and reassembled at the destination.
multicast	A data transmission sent from one sender to multiple receivers. See also <i>broadcast</i> and <i>unicast</i> .
mW	milliwatts

To return to your previous page, click the Acrobat Go to Previous View  button.

N

NAS	network access server
NAT	<p>Network Address Translation is an Internet standard for a LAN to use one set of IP addresses for internal traffic and a second set of IP addresses for external traffic. NAT provides some security because the IP addresses of SBG940 LAN computers are invisible on the Internet.</p> <p>If NAT is enabled on the Gateway page, there is a one-to-one mapping between each public IP address and client IP address.</p>
NAPT	Network Address Port Translation is the most common form of address translation between public and private IP addresses. NAPT is a mapping of one public IP address to many private IP addresses. If NAPT is enabled on the Gateway page, one public IP address is mapped to an individual private IP address for up to 245 LAN clients.
NEC	National Electrical Code (United States) — The regulations for construction and installation of electrical wiring and apparatus, suitable for mandatory application by a wide range of state and local authorities.
network	Two or more computers connected to communicate with each other. Networks have traditionally been connected using some kind of wiring.
network driver	Software packaged with a NIC that enables the computer to communicate with the NIC.
network layer	Layer 3 in the OSI architecture that provides services to establish a path between open systems. The network layer knows the address of the neighboring nodes, packages output with the correct network address data, selects routes, and recognizes and forwards to the transport layer incoming messages for local host domains.
NIC	A network interface card converts computer data to serial data in a packet format that it sends over the LAN. A NIC is installed in an expansion slot or can be built-in. Every Ethernet NIC has a MAC address permanently saved in its ROM.
node	<p>On a LAN, a generic term for any network device.</p> <p>On an HFC network, the interface between the fiber-optic trunk and coaxial cable feeders to subscriber locations. A node is typically located in the subscriber neighborhood.</p>
noise	Random spurts of electrical energy or interface. May produce a salt-and-pepper pattern on a television picture.

O

ohm	A unit of electrical resistance.
OSI	The Open Systems Interconnection reference model is an illustrative model describing how data moves from an application on the source host through a network to an application on the destination host. It is a conceptual framework developed by ISO that is now the primary model for intercomputer communications. OSI is a model <i>only</i> ; it does not define a specific networking interface.

To return to your previous page, click the Acrobat Go to Previous View  button.

P

packet	The unit of data that is routed between the sender and destination on the Internet or other packet-switched network. When data such as an e-mail message or other file is sent over the Internet, IP on the sender divides the data into uniquely-numbered packets. The packet header contains the source and destination IP addresses. The individual packets may travel different routes. When all packets arrive at the destination, IP at that end reassembles the packets. The header and the data can vary in length. Packet and datagram are similar in meaning.
packet-switched	A scheme to handle transmissions on a connectionless network such as the Internet. An alternative is circuit-switched.
PacketCable	A CableLabs-led project to define a common platform to deliver advanced real-time multimedia services over two-way HFC cable plant. Built on DOCSIS 1.1, PacketCable networks use IP technology as the basis for a highly-capable multimedia architecture.
pass-through	A pass-through client on the SBG940 LAN obtains its public IP address from the cable provider DHCP server.
PAT	Port Address Translation
PCI	
PCMCIA	The Personal Computer Memory Card International Association sets international standards for connecting peripherals to portable computers. Laptop computers typically have a PCMCIA slot that can hold one or two PC Cards to provide features such as Ethernet connectivity.
PDA	personal desktop assistant
PDU	A protocol data unit is a message containing operational instructions used for SNMP. The basic SNMP V2 PDU types are get-request, get-next-request, get-bulk-request, response, set-request, inform-request, and trap.
periodic ranging	Ranging that is performed on an on-going basis after initial ranging has taken place.
physical layer	Layer 1 in the OSI architecture. It provides services to transmit bits or groups of bits over a transmission link between open systems. It entails the electrical, mechanical, and handshaking procedures.
piggybacking	A process that occurs when a cable modem simultaneously transmits data and requests additional bandwidth.
PING	A network utility that tests host reachability by sending a small packet to the host and waiting for a reply. If you PING a computer IP address and receive a reply, you know the computer is reachable over the network. It also stands for "Packet InterNet Groper."
PMD	The physical media-dependent sublayer of the physical layer which transmits bits or groups of bits over particular types of transmission links between open systems. It entails the electrical, mechanical, and handshaking procedures.
point-to-point	Physical connection made from one point to another.
POTS	The "plain old telephone service" offered through the PSTN; basic analog telephone service. POTS uses the lowest 4 kHz of bandwidth on twisted pair wiring.
port	On a computer or other electronic device, a port is a socket or plug used to physically connect it to the network or to other devices. in TCP/IP, a port is a number from 0 to 65536 used logically by a client program to specify a server program. Ports 0 to 1024 are reserved

To return to your previous page, click the Acrobat Go to Previous View  button.

port mirroring	A feature that enables one port (source) on the SBG940 to be copied to another port (destination) to be studied. The destination mirrors the transmitted (from) or received (to) data on the source port to enable the person managing the network to monitor activity.
port triggering	A mechanism that allows incoming communication with specified applications. Primarily used for gaming applications.
PPP	Point-to-Point Protocol is used to transport other protocols, typically for simple links over serial lines. It is most commonly used to access the Internet with a dial-up modem.
PPTP	Point-to-Point Tunneling Protocol encapsulates other protocols. It is a new technology to create VPNs developed jointly by several vendors.
private IP address	An IP address assigned to a computer on the SBG940 LAN by the DHCP server on the SBG940 for a specified lease time. Private IP addresses are used by the SBG940 LAN only; they are invisible to devices on the Internet. See also <i>public IP address</i> .
protocol	A formal set of rules and conventions for exchanging data. Different computer types (for example PC, UNIX, or mainframe) can communicate if they support common protocols.
provisioning	The process of autodiscovery or manually configuring a cable modem on the CMTS.
PSTN	The public switched telephone network is the traditional circuit-switched, voice-oriented telephone network. See also <i>POTS</i> .
public IP address	The IP address assigned to the SBG940 by the cable provider. A public IP address is visible to devices on the Internet. See also <i>private IP address</i> .

Q

QAM	Quadrature Amplitude Modulation uses amplitude and phase modulation to encode multiple bits of data in one signaling element. QAM achieves faster data transfer than amplitude or phase modulation alone, but the signal is more prone to errors caused by noise. QAM requires a transmission circuit with a higher CNR than alternate modulation formats such as QPSK. Two types of QAM are: <ul style="list-style-type: none">• 16 QAM encodes four bits per symbol as one of 16 possible amplitude and phase combinations.• 64 QAM encodes six bits per symbol as one of 64 possible amplitude and phase combinations.
QPSK	Quadrature Phase Shift Key (QPSK) modulation sends two bits of information per symbol period with one symbol 90 degrees out of phase with other symbols. The four constellation points represented by the coordinates (0,0 - 0,1 - 1,0 - 1,1) represent the four possible combinations.
QoS	Quality of service describes the priority, delay, throughput, and bandwidth of a connection.

To return to your previous page, click the Acrobat Go to Previous View  button.

R

RADIUS	Remote Authentication Dial-In User Service server typically used in large corporate settings.
RAS	Remote Access Server
registration	How a cable modem makes itself known to the CMTS. The cable modem configuration file and authorization are verified and the CoS is negotiated.
return loss	A measurement of the quality of the match of the device to the cable system. Return loss is the ratio of the amount of power reflected by the device. A return loss of 20 dB or greater is preferred.
RF	Radio Frequency — signals used by the CMTS transmitter and receiver to send data over HFC. The carrier is modulated to encode the digital data stream for transmission across the cable network.
RFC	Request for Comments published on the IETF or other websites. Many RFCs become international standards.
RJ-11	The most common type of connector for household or office phones.
RJ-45	An 8-pin modular connector; the most common connector type for 10Base-T or 100Base-T Ethernet networks.
ROM	read-only memory
router	<p>On IP networks, a device connecting at least two networks, which may or may not be similar. A router is typically located at a <i>gateway</i> between networks. A router operates on OSI network layer 3. It filters packets based on the IP address, examining the source and destination IP addresses to determine the best route on which to forward them.</p> <p>A router is often included as part of a network switch. A router can also be implemented as software on a computer.</p>
routing table	A table listing available routes that is used by a router to determine the best route for a packet.
RTS	request to send

To return to your previous page, click the Acrobat Go to Previous View  button.

S

server	In a client/server architecture, a dedicated computer that supplies files or services such as file transfer, remote login, or printing to clients.
scope	The set of IP addresses that a DHCP server can lease to clients.
service provider	A company providing cable data services to subscribers.
SID	A service ID is a unique 14-bit identifier the CMTS assigns to a cable modem or gateway that identifies the traffic type it carries (for example, data or voice). The SID provides the basis for the CMTS to allocate bandwidth to the cable modem and implement CoS.
SDU	service data unit
SME	small and medium enterprise
SMTP	Simple Mail Transfer Protocol is a standard Internet protocol for transferring e-mail.
SNMP	Simple Network Management Protocol is a standard to monitor and manage networks and network devices. Data is exchanged using PDU messages.
SOHO	small office home office
spectrum	A specified range of frequencies used for transmission of electromagnetic signals.
spectrum allocation	An allocation of portions of the available electromagnetic spectrum for specific services, such as AM, FM, or personal communications.
splitter	A device that divides the signal from an input cable between two or more cables.
stateful inspection	<p>A type of firewall that tracks each connection traversing all firewall interfaces to ensure validity. In addition to examining the source and destination in the packet header based on static rules, a stateful inspection firewall:</p> <ul style="list-style-type: none">• Examines packet headers on context established by previous packets that traversed the firewall• Monitors the connection state and saves it in a table• Closes ports until a connection to a specific port is requested• May examine the packet contents up through the application layer to determine more than just the source and destination <p>A stateful-inspection firewall is more advanced than a static filter firewall.</p>
static filter	A type of firewall that examines the source and destination in the packet header based on administrator-defined rules <i>only</i> .
static IP address	An IP address that is permanently assigned to a host. Normally, a static IP address must be assigned manually. The opposite of dynamic IP address.
static route	A manually-defined route.
station	IEEE 802.11b term for wireless client.
subscriber	A home or office user who accesses television, data, or other services from a cable provider.
subnet mask	A bit mask that is logically ANDed with the destination IP address of a packet to determine the network address. A router routes packets using the network address.
subnetwork	A part of a network; commonly abbreviated "subnet." When subnetting is used, the host portion of the IP address is divided into a subnet and host number. Hosts and routers use the subnet mask to identify the bits used for the network and subnet number.

To return to your previous page, click the Acrobat Go to Previous View  button.

switch	On an Ethernet network, a switch filters frames based on the MAC address, in a manner similar to a bridge. A switch is more advanced because it can connect more than two segments.
symbol rate	Also known as baud rate, is a measure of the number of times per second a signal in a communications channel varies, or makes a transition between states (states being frequencies, voltage levels or phase angles). Usually measured in symbols per second (sps).
SYSLOG	A de-facto UNIX standard for logging system events.

T

TBCP	Tagged Binary Communication Protocol
TCP	Transmission Control Protocol on OSI transport layer four, provides reliable transport over the network for data transmitted using IP (network layer three). It is an end-to-end protocol defining rules and procedures for data exchange between hosts on top of connectionless IP. TCP uses a timer to track outstanding packets, checks error in incoming packets, and retransmits packets if requested.
TCP/IP	The Transmission Control Protocol/Internet Protocol suite provides standards and rules for data communication between networks on the Internet. It is the worldwide internetworking standard and the basic communications protocol of the Internet.
TFTP	Trivial File Transfer Protocol is a very simple protocol used to transfer files.
TKIP	Temporal Key Integrity Protocol
transparent bridging	A method to enable all hosts on the wired Ethernet LAN, WLAN, and USB connection to communicate as if they were all connected to the same physical network.
transport layer	Layer of the OSI concerned with protocols for error recognition and recovery. This layer also regulates information flow.
trunk	Electronic path over which data is transmitted.
TTL	The time to live is the number of routers (or hops) a packet can traverse before being discarded. When a router processes a packet, it decreases the TTL by 1. When the TTL reaches zero, the packet is discarded.
tunnel	<p>To place packets inside other packets to send over a network. The protocol of the enclosing packet is understood by each endpoint, or tunnel interface, where the packet enters and exits the network. VPNs rely on tunneling to create a secure network.</p> <p>Tunneling requires the following protocol types:</p> <ul style="list-style-type: none">• A carrier protocol, such as TCP, used by the network that the data travels over• An encapsulating protocol, such as IPSec, L2F, L2TP, or PPTP, that is wrapped around the original data• A passenger protocol, such as IP, for the original data
two-way	A cable system that can transmit signals in both directions to and from the headend and the subscriber.

To return to your previous page, click the Acrobat Go to Previous View  button.

U-Z

UDP	User Datagram Protocol
unicast	A point-to-point data transmission sent from one sender to one receiver. This the normal way you access websites. See also <i>broadcast</i> and <i>multicast</i> .
upstream	In a cable data network, upstream describes the direction of data sent from the subscriber computer through the cable modem to the CMTS and the Internet.
USB	Universal Serial Bus is a computer interface for add-on devices such as printers, scanners, mice, modems, or keyboards. USB supports data transfer rates of 12 Mbps and plug-and-play installation. You can connect up to 127 devices to a single USB port.
UTP	unshielded twisted pair (wire)
VLAN	A virtual local area network is group of devices on different LAN segments that are logically configured to communicate as if they are connected to the same wire.
VoIP	Voice over Internet Protocol is a method to exchange voice, fax, and other information over the Internet. Voice and fax have traditionally been carried over traditional telephone lines of the PSTN using a dedicated circuit for each line. VoIP enables calls to travel as discrete data packets on shared lines. VoIP is an important part of the convergence of computers, telephones, and television into a single integrated information network.
VPN	A virtual private network is a private network that uses "virtual" connections (tunnels) routed over a public network (usually the Internet) to provide a secure and fast connection; usually to users working remotely at home or in small branch offices. A VPN connection provides security and performance similar to a dedicated link (for example, a leased line), but at much lower cost.
WAN	A wide-area network provides a connection over a large geographic area, such as a country or the whole world. The bandwidth depends on need and cost, but is usually much lower than for a LAN.
WAP	Wireless access point or Wireless Access Protocol. See also <i>access point</i> .
WECA	The Wireless Ethernet Compatibility Alliance is a trade organization that works to ensure that all wireless devices — computer cards, laptops, air routers, PDAs, etc — can communicate with each other.
WEP	Wired Equivalent Privacy encryption protects the privacy of data transmitted over a WLAN. WEP uses keys to encrypt and decrypt transmitted data. The access point must authenticate a client before it can transfer data to another client. WEP is part of IEEE 802.11b. <i>Because WEP can be difficult to use and does not provide very strong encryption, we recommend using WPA if possible.</i>
WiFi	Wireless fidelity (pronounced y-phi) brand name applied to products supporting IEEE 802.11b.
Wireless Cable Modem Gateway	The Motorola SURFboard Wireless Cable Modem Gateway is a single device that combines a cable modem, router, Ethernet switch, wireless access point, and DHCP server for SOHO or SME use.
WLAN	wireless LAN
world wide web	An interface to the Internet that you use to navigate and hyperlink to information.
WPA	Wi-Fi Protected Access (WPA) encryption, as described on the Wi-Fi Alliance Wi-Fi Protected Access web page http://www.wifialliance.org/OpenSection/protected_access.asp). It is a far more robust form of encryption than WEP. <i>We recommend using WPA if all of your client hardware supports WPA.</i>

To return to your previous page, click the Acrobat Go to Previous View  button.

❖ Software License

Motorola, Inc., Broadband Communications Sector ("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.

The Software includes associated media, any printed materials, and any "on-line" or electronic documentation, as well as any updates, revisions, bug fixes, or drives obtained by you from Motorola or your service provider. 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., Broadband Communications Sector, 101 Tournament Drive, Horsham, PA 19044.

Visit our website at:
www.motorola.com



515398-001
5/04
MGBI