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 common-sense 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	Required On Each Wireless Client
If all of your wireless clients support Wi-Fi Protected Access (WPA), we recommend Configuring WPA on the SBG940	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.
Otherwise, perform Configuring WEP on the SBG940	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

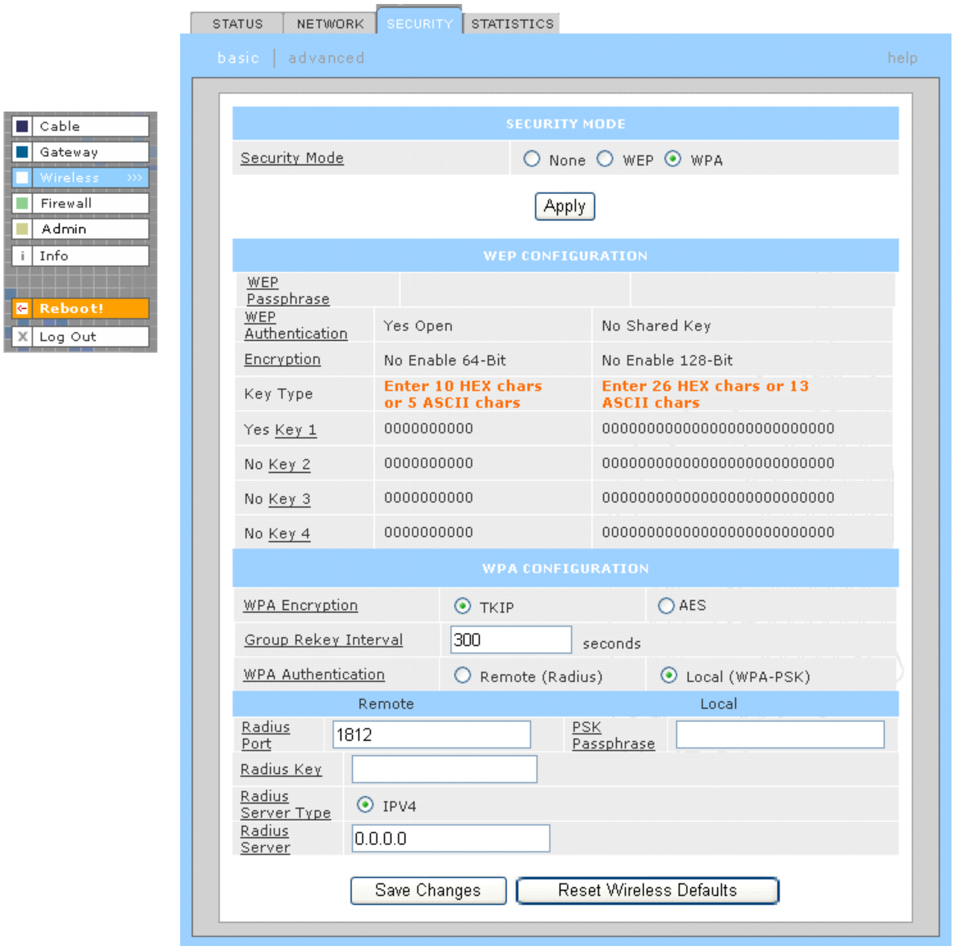
For new wireless LANs, we recommend purchasing client adapters that support WPA, such as the Motorola Wireless Notebook Adapter WN825G, Wireless PCI Adapter WPCI810G, and Wireless USB Adapter WU830G. For more information about the benefits of WPA, see the Wi-Fi Protected Access web page http://www.wifialliance.org/OpenSection/protected_access.asp.

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:



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	00000000000000000000000000
No Key 2	0000000000	00000000000000000000000000
No Key 3	0000000000	00000000000000000000000000
No Key 4	0000000000	00000000000000000000000000

WPA CONFIGURATION

WPA Encryption	● TKIP	○ AES
Group Rekey Interval	300 seconds	
WPA Authentication	○ Remote (Radius)	● Local (WPA-PSK)

Remote		Local	
Radius Port	1812	PSK Passphrase	
Radius Key			
Radius Server Type	● IPV4		
Radius Server	0.0.0.0		

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.

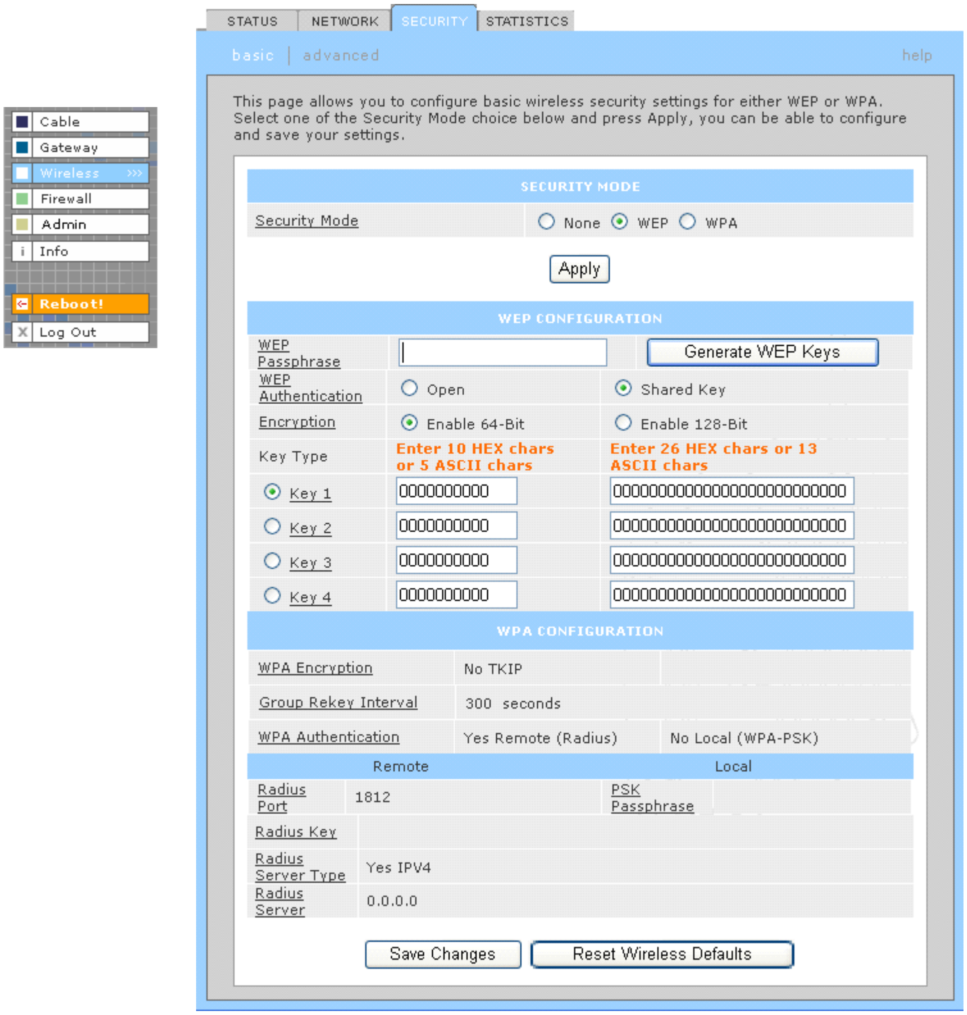
Caution!

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:



This page allows you to configure basic wireless security settings for either WEP or WPA. Select one of the Security Mode choice below and press Apply, you can be able to configure and save your settings.

SECURITY MODE

Security Mode	○ None ● WEP ○ WPA

Apply

WEP CONFIGURATION

WEP Passphrase		Generate WEP Keys
WEP Authentication	○ Open	● Shared Key
Encryption	● Enable 64-Bit	○ Enable 128-Bit
Key Type	Enter 10 HEX chars or 5 ASCII chars	Enter 26 HEX chars or 13 ASCII chars
● Key 1	0000000000	00000000000000000000000000
○ Key 2	0000000000	00000000000000000000000000
○ Key 3	0000000000	00000000000000000000000000
○ Key 4	0000000000	00000000000000000000000000

WPA CONFIGURATION

WPA Encryption	No TKIP	
Group Rekey Interval	300 seconds	
WPA Authentication	Yes Remote (Radius)	No Local (WPA-PSK)

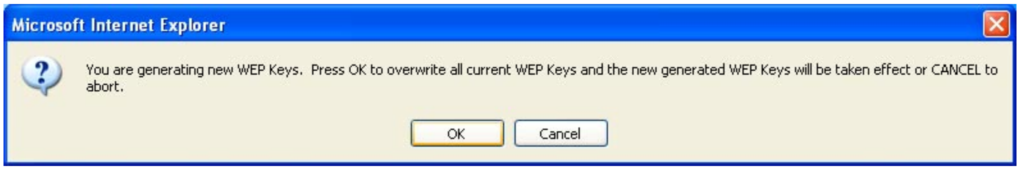
Remote		Local	
Radius Port	1812	PSK Passphrase	
Radius Key			
Radius Server Type	Yes IPV4		
Radius Server	0.0.0.0		

Save Changes   Reset Wireless Defaults

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.

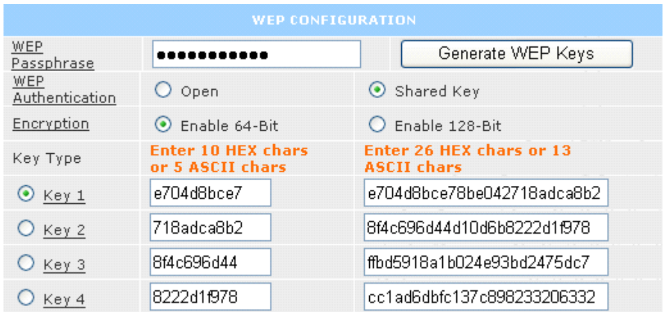
5 Click **Generate WEP Keys**. The following window is displayed:



Microsoft Internet Explorer

You are generating new WEP Keys. Press OK to overwrite all current WEP Keys and the new generated WEP Keys will be taken effect or CANCEL to abort.

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



WEP CONFIGURATION

WEP Passphrase	●●●●●●●●●●●●	Generate WEP Keys
WEP Authentication	○ Open	● Shared Key
Encryption	● Enable 64-Bit	○ Enable 128-Bit
Key Type	Enter 10 HEX chars or 5 ASCII chars	Enter 26 HEX chars or 13 ASCII chars
● Key 1	e704d8bce7	e704d8bce78be042718adca8b2
○ Key 2	718adca8b2	8f4c696d44d10d6b8222d1f978
○ Key 3	8f4c696d44	ffbd5918a1b024e93bd2475dc7
○ 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	Required On Each Wireless Client
Perform Configuring the Wireless Network Name on the SBG940 to disable Extended Service Set Identifier (ESSID) broadcasting to enable closed network operation	You must configure the identical ESSID (network name) to the SBG940.
Perform Configuring a MAC Access Control List on the SBG940 to restrict access to wireless clients with known MAC addresses	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.

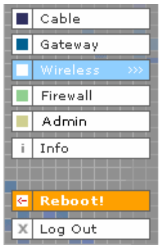
If you select Disable ESSID Broadcast, you must perform Configuring a Wireless Client with the Network Name (ESSID) on all WLAN clients (stations). Never provide your ESSID to anyone who is not authorized to use your WLAN.

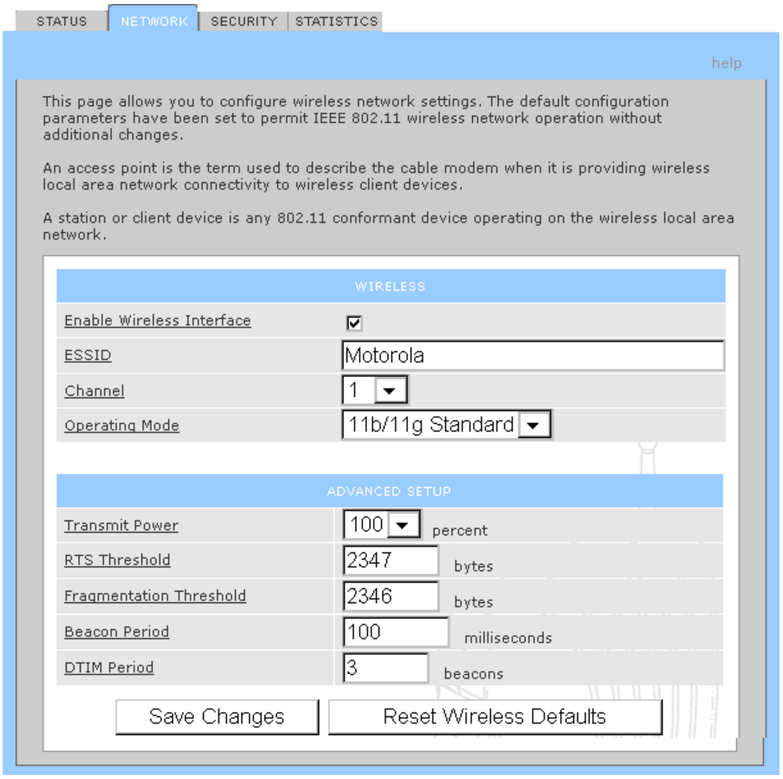
To configure the ESSID on the SBG940:

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:





This page allows you to configure wireless network settings. The default configuration parameters have been set to permit IEEE 802.11 wireless network operation without additional changes.

An access point is the term used to describe the cable modem when it is providing wireless local area network connectivity to wireless client devices.

A station or client device is any 802.11 conformant device operating on the wireless local area network.

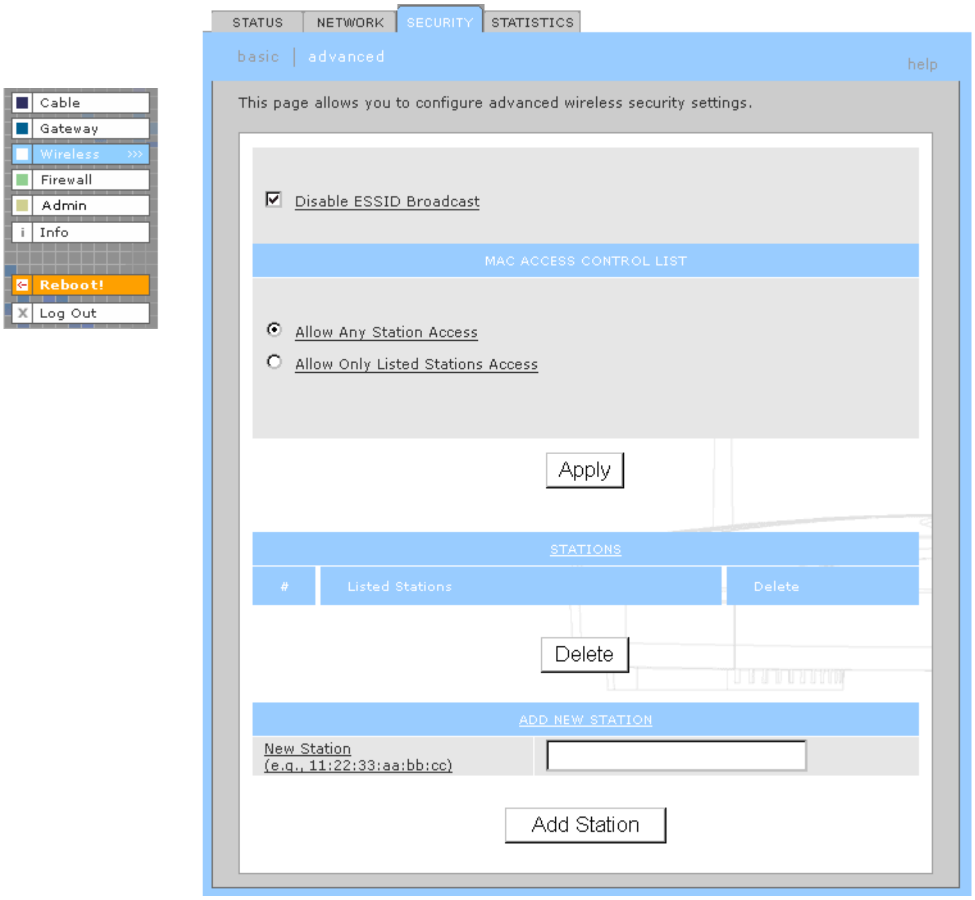
Enable Wireless Interface	☑
ESSID	Motorola
Channel	1
Operating Mode	11b/11g Standard
Transmit Power	100 percent
RTS Threshold	2347 bytes
Fragmentation Threshold	2346 bytes
Beacon Period	100 milliseconds
DTIM Period	3 beacons

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:



This page allows you to configure advanced wireless security settings.

☑ Disable ESSID Broadcast

● Allow Any Station Access

○ Allow Only Listed Stations Access

#	Listed Stations	Delete

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

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

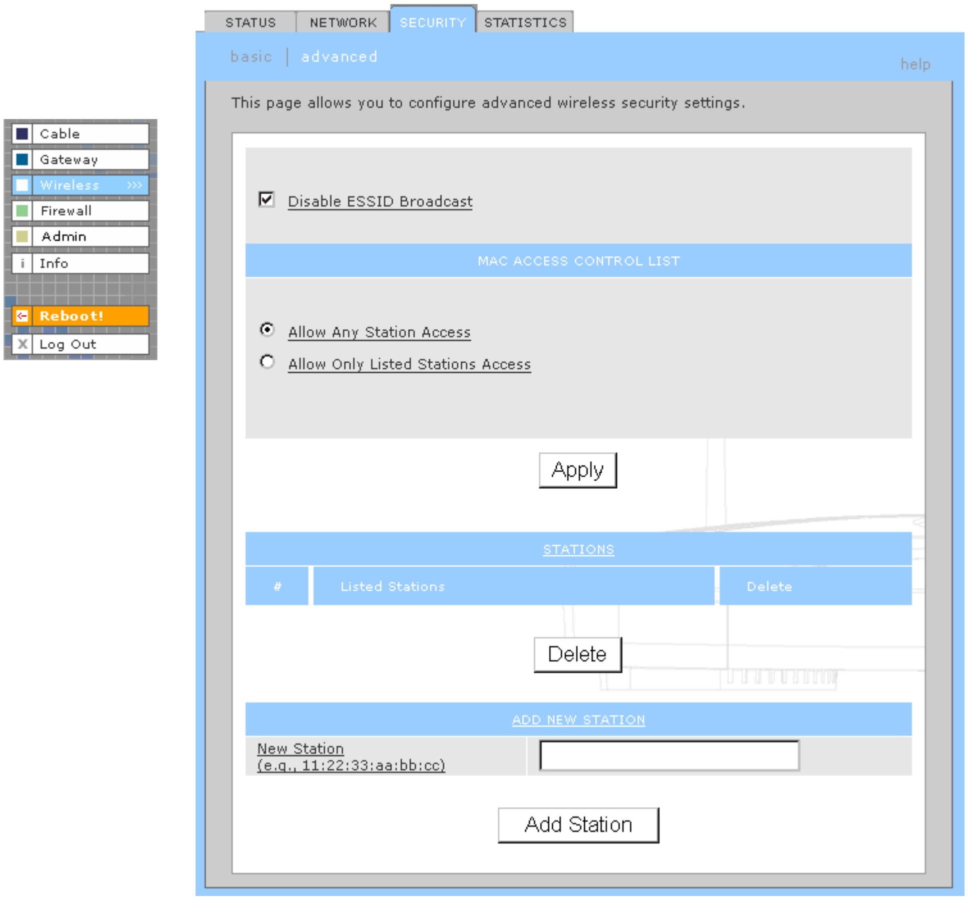
You can restrict wireless access to one to 32 wireless clients, based on the client MAC address.

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:



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

STATIONS

#	Listed Stations	Delete

ADD NEW STATION

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

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.

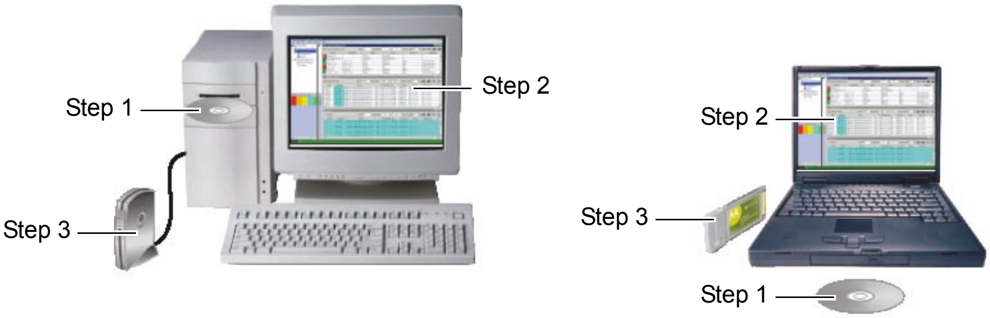
Configuring the Wireless Clients

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	On Each Client, You Need to Perform
Configuring WPA on the SBG940	Configuring a Wireless Client for WPA
Configuring WEP on the SBG940	Configuring a Wireless Client for WEP
Configuring the Wireless Network Name on the SBG940	Configuring a Wireless Client with the Network Name (ESSID)
Configuring a MAC Access Control List on the SBG940	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:

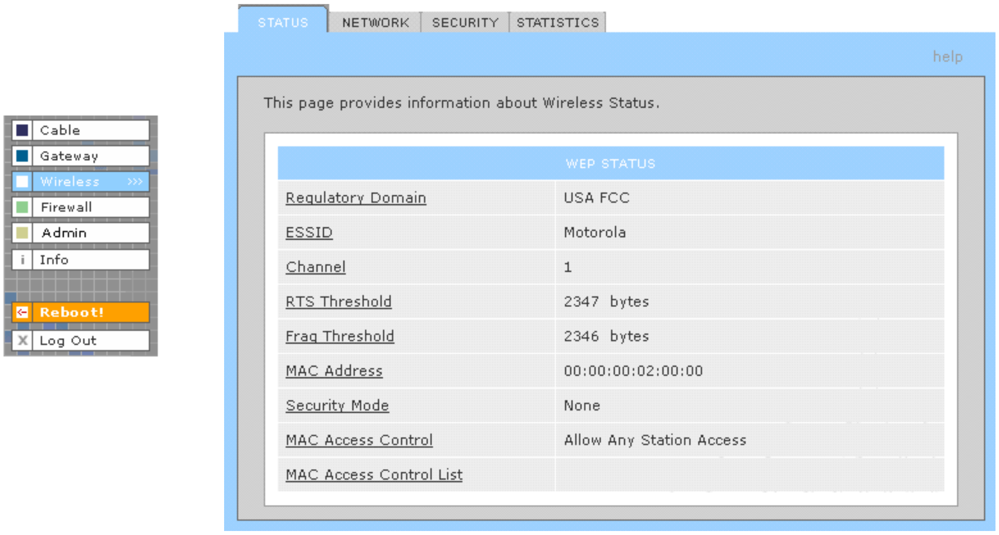
- Wireless > STATUS Page
- Wireless > NETWORK Page
- Wireless > SECURITY — basic Page
- Wireless > SECURITY — advanced Page
- Wireless > STATISTICS page

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



This page provides information about Wireless Status.

WEP STATUS	
Regulatory Domain	USA FCC
ESSID	Motorola
Channel	1
RTS Threshold	2347 bytes
Frag Threshold	2346 bytes
MAC Address	00:00:00:02:00:00
Security Mode	None
MAC Access Control	Allow Any Station Access
MAC Access Control List	

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

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"):

- 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.

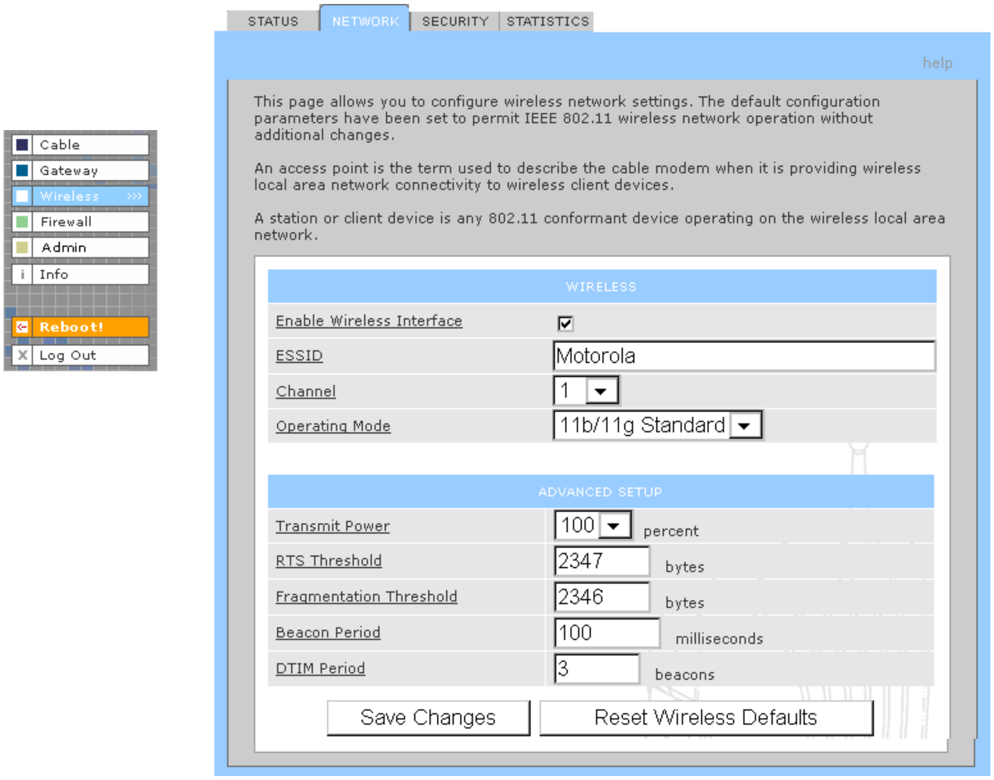
MAC Access Control List Displays the MAC addresses of wireless clients having access (see "Configuring a MAC Access Control List on the SBG940").

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.



This page allows you to configure wireless network settings. The default configuration parameters have been set to permit IEEE 802.11 wireless network operation without additional changes.

An access point is the term used to describe the cable modem when it is providing wireless local area network connectivity to wireless client devices.

A station or client device is any 802.11 conformant device operating on the wireless local area network.

WIRELESS	
Enable Wireless Interface	☑
ESSID	Motorola
Channel	1
Operating Mode	11b/11g Standard

ADVANCED SETUP	
Transmit Power	100 percent
RTS Threshold	2347 bytes
Fragmentation Threshold	2346 bytes
Beacon Period	100 milliseconds
DTIM Period	3 beacons

Wireless > NETWORK page fields

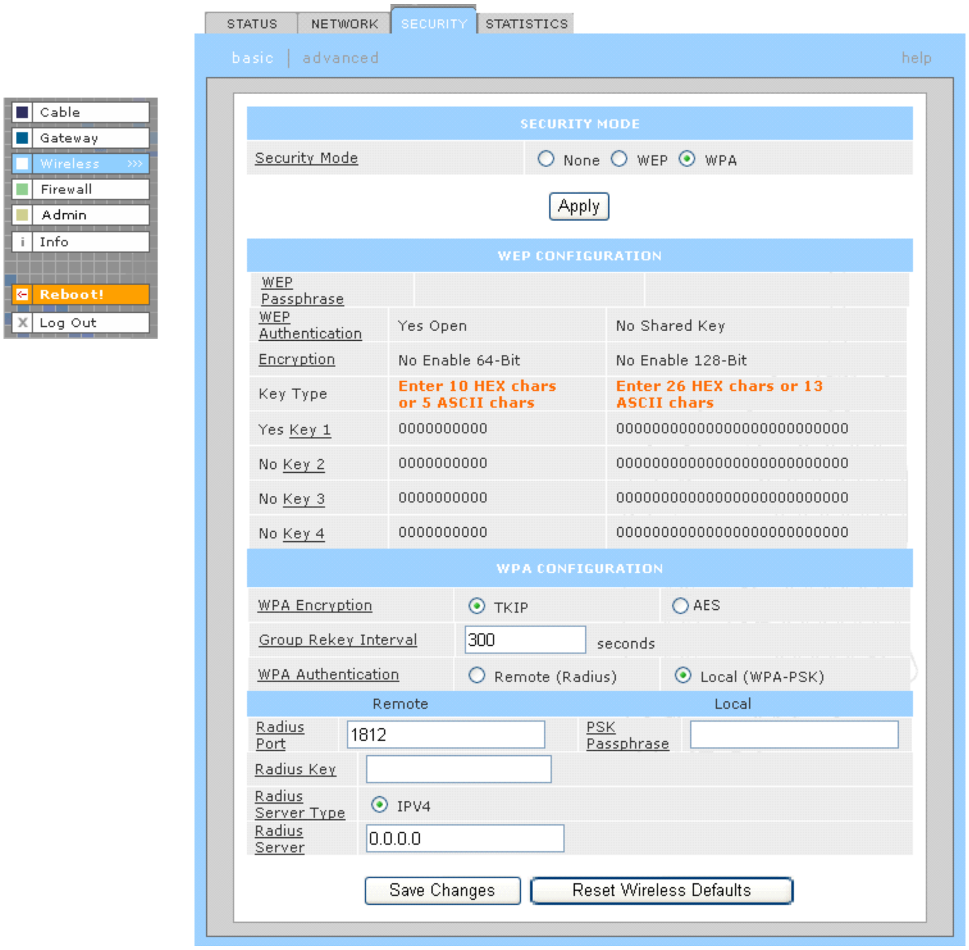
Field	Description
WIRELESS	
Enable Wireless Interface	Select this box to enable the wireless interface.
ESSID	Sets a unique network name for the SBG940 WLAN to distinguish between multiple WLANs in the vicinity. *If you select Disable ESSID Broadcast on the Wireless > SECURITY — advanced Page, all clients 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.*
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): • 11b/11g Standard — Enables all IEEE 802.11b and IEEE 802.11g clients to work with the SBG940. *We recommend using this default setting in most cases because it is more flexible.* • 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”.



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	00000000000000000000000000
No Key 2	0000000000	00000000000000000000000000
No Key 3	0000000000	00000000000000000000000000
No Key 4	0000000000	00000000000000000000000000

WPA CONFIGURATION

WPA Encryption	● TKIP	○ AES
Group Rekey Interval	300	seconds
WPA Authentication	○ Remote (Radius)	● Local (WPA-PSK)

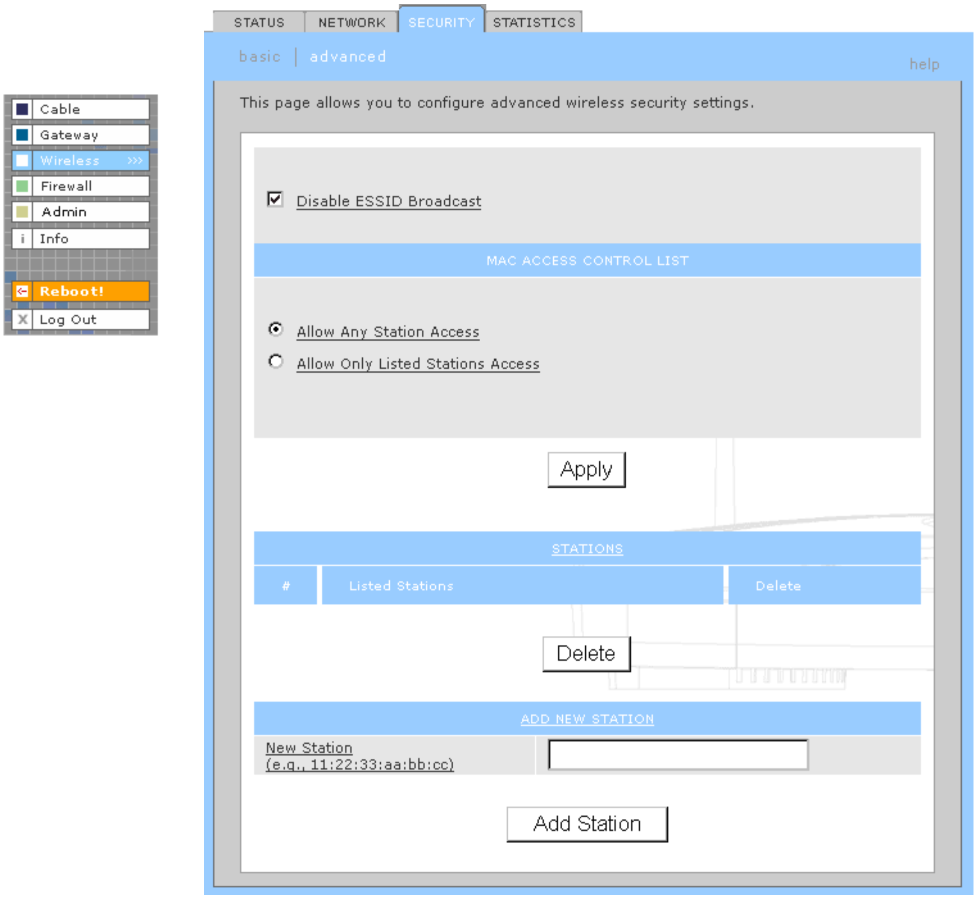
Remote		Local	
Radius Port	1812	PSK Passphrase	
Radius Key			
Radius Server Type	● IPV4		
Radius Server	0.0.0.0		

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.



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

Wireless > Security — ADVANCED page fields

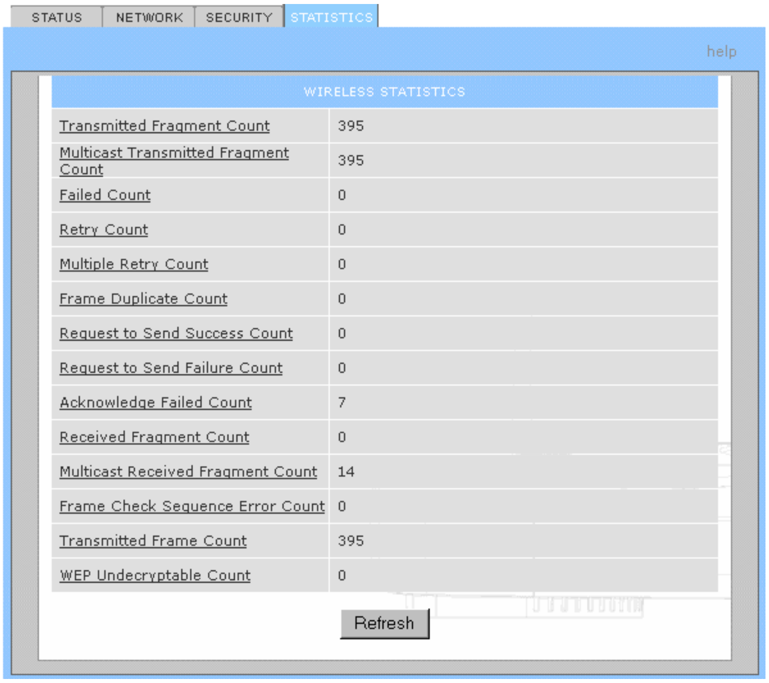
Field or Button	Description
Disable ESSID Broadcast	If selected, only wireless clients (stations) having the same Network Name (ESSID) as the SBG940 can communicate with the SBG940. Closed network operation is a SBG940 enhancement to IEEE 802.11b. The default is not selected (off).
MAC ACCESS CONTROL 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

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 the following procedures:

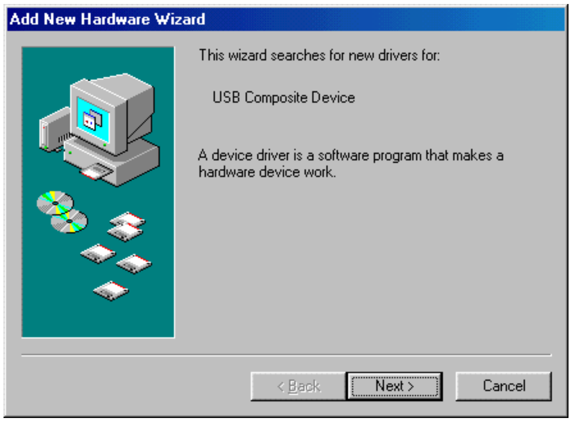
- Removing the USB Driver from Windows 98 or Windows Me
- Removing the USB Driver from Windows 2000
- Removing the USB Driver from Windows XP

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:



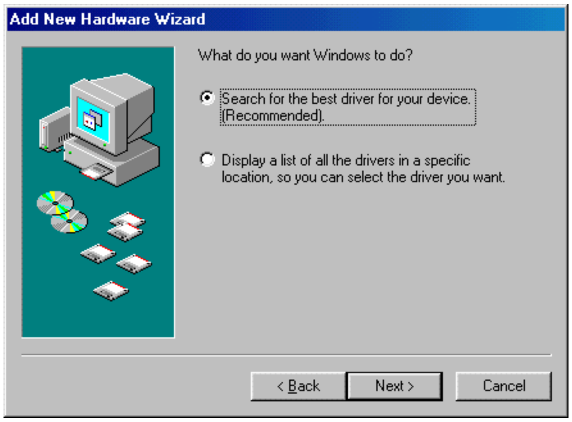
Add New Hardware Wizard

This wizard searches for new drivers for:

USB Composite Device

A device driver is a software program that makes a hardware device work.

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



Add New Hardware Wizard

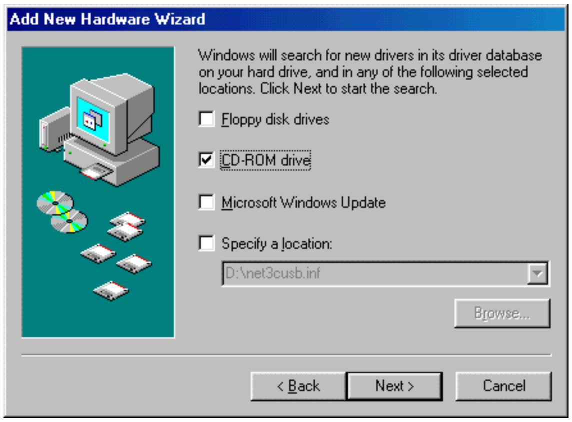
What do you want Windows to do?

● Search for the best driver for your device. (Recommended).

○ Display a list of all the drivers in a specific location, so you can select the driver you want.

4 Be sure “Search for the best driver for your device” is selected.

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



Windows will search for new drivers in its driver database on your hard drive, and in any of the following selected locations. Click Next to start the search.

□ Floppy disk drives

☑ CD-ROM drive

□ Microsoft Windows Update

□ Specify a location:

D:\net3cusb.inf

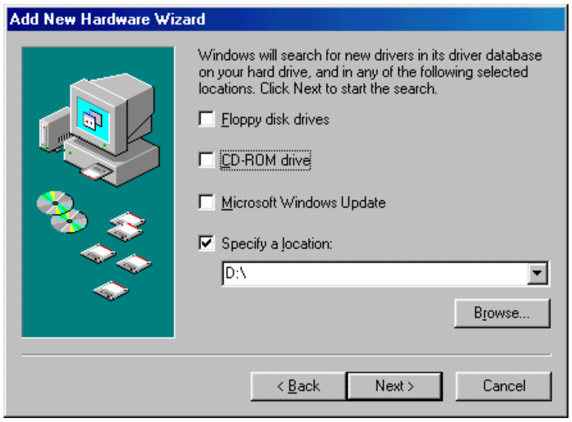
Be sure “CD-ROM drive” is the only box selected.

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:



Windows will search for new drivers in its driver database on your hard drive, and in any of the following selected locations. Click Next to start the search.

□ Floppy disk drives

□ CD-ROM drive

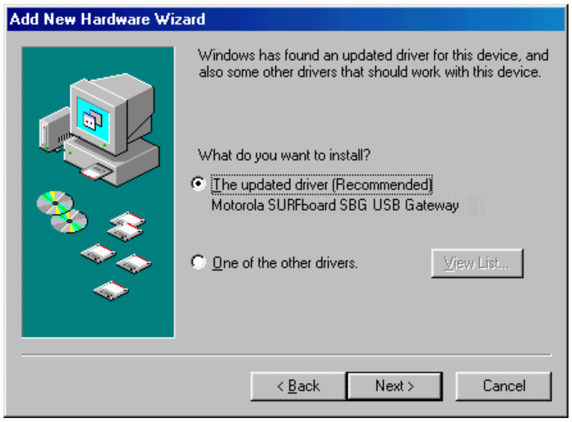
□ Microsoft Windows Update

☑ Specify a location:

D:\

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:



Add New Hardware Wizard

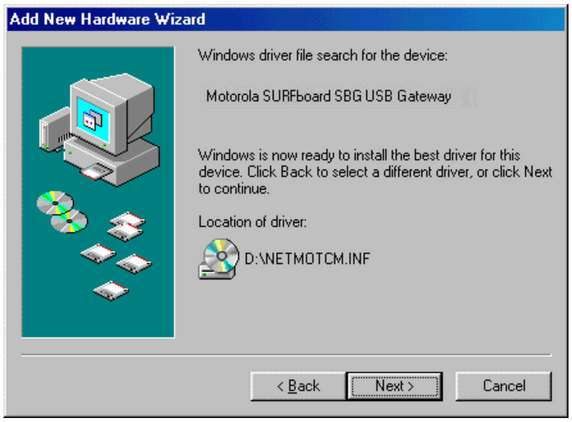
Windows has found an updated driver for this device, and also some other drivers that should work with this device.

What do you want to install?

● The updated driver (Recommended)
Motorola SURFboard SBG USB Gateway

○ One of the other drivers.

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.



Add New Hardware Wizard

Windows driver file search for the device:

Motorola SURFboard SBG USB Gateway

Windows is now ready to install the best driver for this device. Click Back to select a different driver, or click Next to continue.

Location of driver:

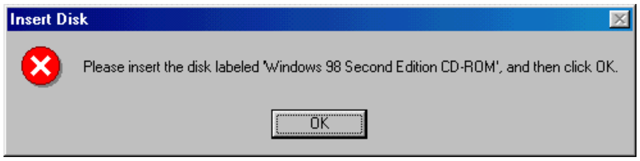
D:\NETMOTCM.INF

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**.

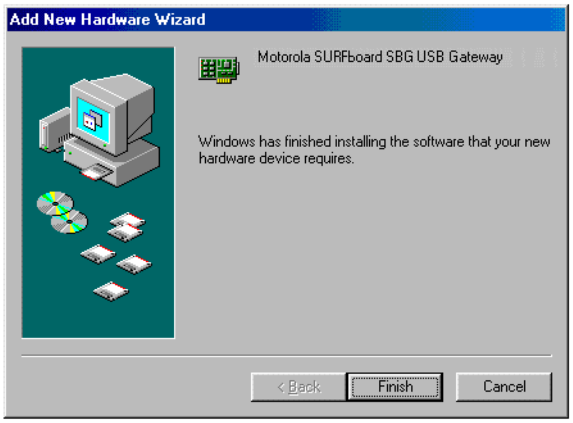
If an Insert Disk window similar to the one below is displayed, Windows 98 system files are needed to complete the installation. To install the files, insert your Windows 98 CD-ROM in the CD-ROM drive and click **OK**.



Insert Disk

Please insert the disk labeled 'Windows 98 Second Edition CD-ROM', and then click OK.

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

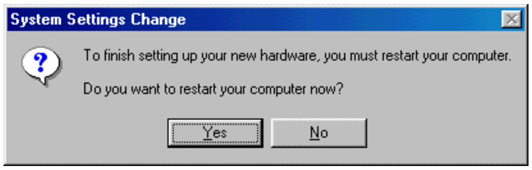


Add New Hardware Wizard

Motorola SURFboard SBG USB Gateway

Windows has finished installing the software that your new hardware device requires.

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



System Settings Change

To finish setting up your new hardware, you must restart your computer.

Do you want to restart your computer now?

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

When you finish setting up the USB driver, you can continue with "Configuring TCP/IP".

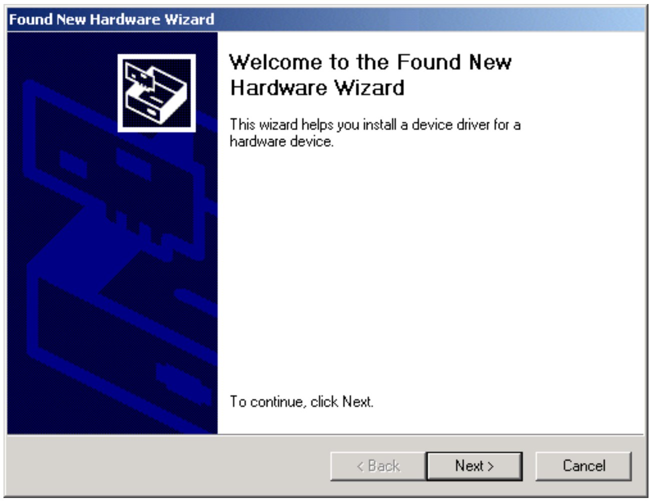
If you have difficulties setting up the USB driver, perform "Removing the USB Driver from Windows 98 or Windows Me" and repeat this procedure. If that does not correct the problem, see the *Regulatory, Safety, Software License, and Warranty Information* card provided with the SBG940 for information about 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:

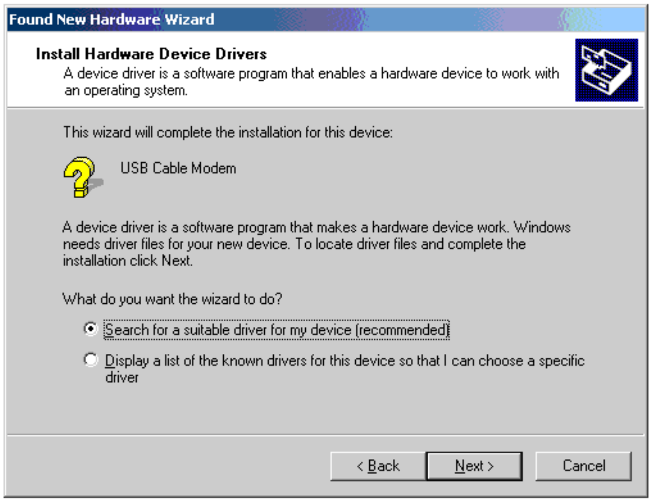

Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

This wizard helps you install a device driver for a hardware device.

To continue, click Next.

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


Found New Hardware Wizard

Install Hardware Device Drivers

A device driver is a software program that enables a hardware device to work with an operating system.

This wizard will complete the installation for this device:

USB Cable Modem

A device driver is a software program that makes a hardware device work. Windows needs driver files for your new device. To locate driver files and complete the installation click Next.

What do you want the wizard to do?

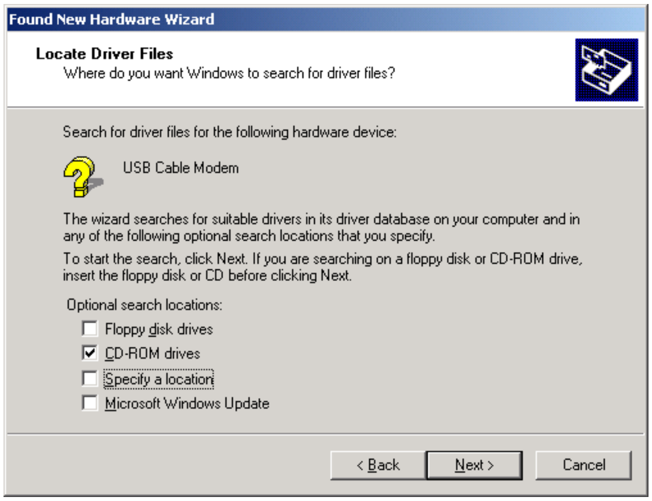
● Search for a suitable driver for my device (recommended)

○ Display a list of the known drivers for this device so that I can choose a specific driver

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:



Found New Hardware Wizard

Locate Driver Files

Where do you want Windows to search for driver files?

Search for driver files for the following hardware device:

USB Cable Modem

The wizard searches for suitable drivers in its driver database on your computer and in any of the following optional search locations that you specify.

To start the search, click Next. If you are searching on a floppy disk or CD-ROM drive, insert the floppy disk or CD before clicking Next.

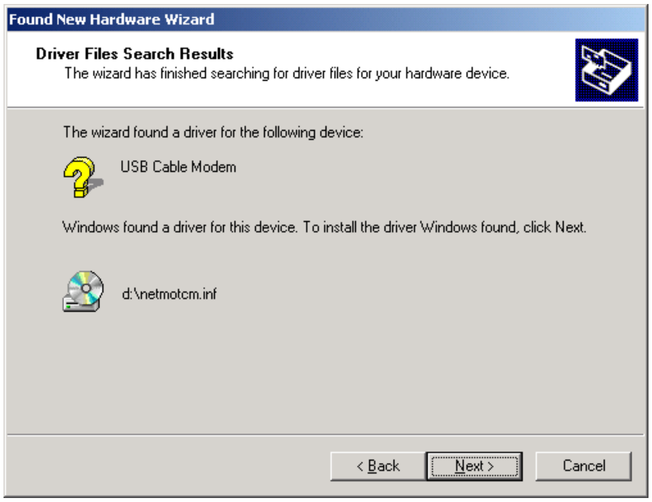
Optional search locations:

- □ Floppy disk drives
- ☑ CD-ROM drives
- □ Specify a location
- □ Microsoft Windows Update

< Back | Next > | Cancel

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

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



Found New Hardware Wizard

Driver Files Search Results

The wizard has finished searching for driver files for your hardware device.

The wizard found a driver for the following device:

USB Cable Modem

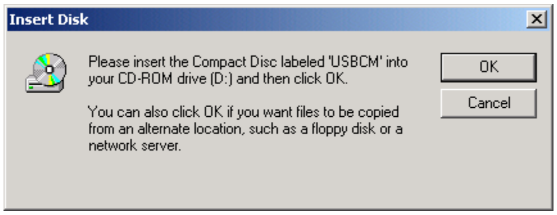
Windows found a driver for this device. To install the driver Windows found, click Next.

d:\netmotcm.inf

< Back | Next > | Cancel

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.



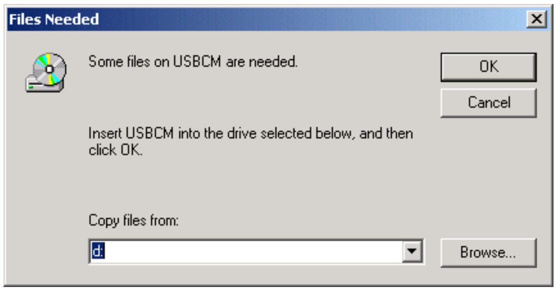
Insert Disk

Please insert the Compact Disc labeled 'USBCM' into your CD-ROM drive (D:) and then click OK.

You can also click OK if you want files to be copied from an alternate location, such as a floppy disk or a network server.

OK | Cancel

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



Files Needed

Some files on USBCM are needed.

Insert USBCM into the drive selected below, and then click OK.

Copy files from:

d:

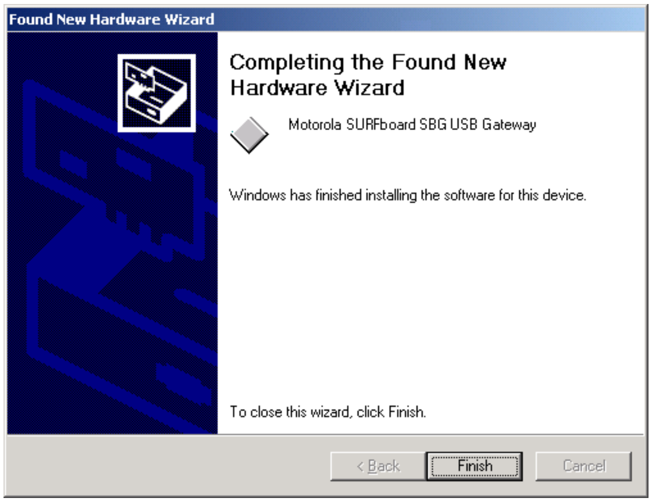
8 If necessary, select the CD-ROM drive in the Copy files from list.

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:



Found New Hardware Wizard

Completing the Found New Hardware Wizard

Motorola SURFboard SBG USB Gateway

Windows has finished installing the software for this device.

To close this wizard, click Finish.

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

When you finish setting up the USB driver, you can continue with “Configuring TCP/IP”.

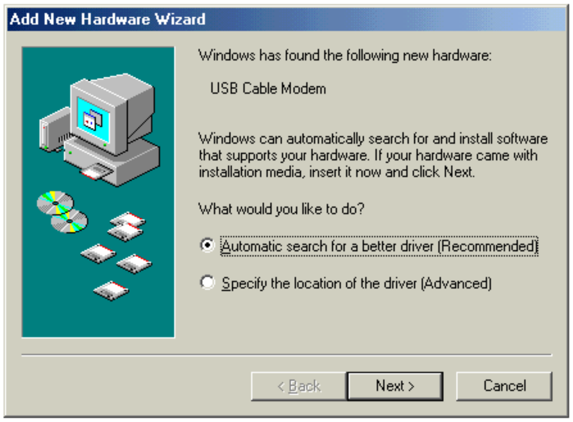
If you have any difficulties setting up the USB driver, perform “Removing the USB Driver from Windows 2000” and repeat this procedure.

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:



Add New Hardware Wizard

Windows has found the following new hardware:

USB Cable Modem

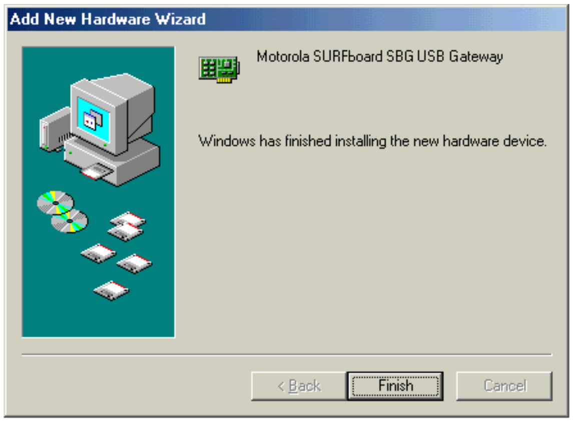
Windows can automatically search for and install software that supports your hardware. If your hardware came with installation media, insert it now and click Next.

What would you like to do?

● Automatic search for a better driver (Recommended)

○ Specify the location of the driver (Advanced)

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



Add New Hardware Wizard

Motorola SURFboard SBG USB Gateway

Windows has finished installing the new hardware device.

> 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.

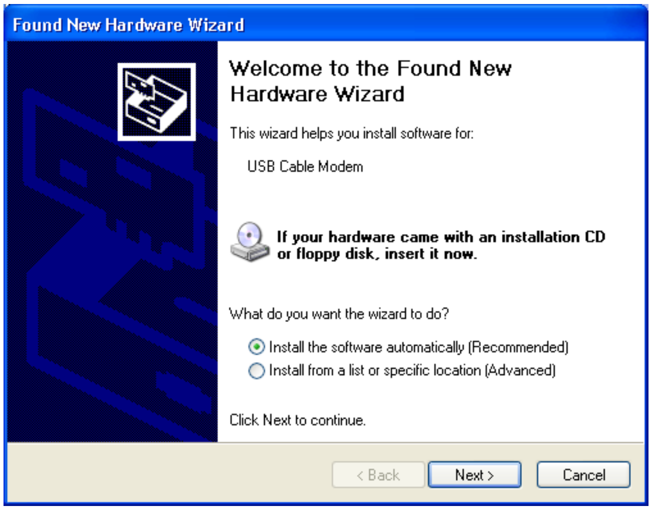
When you finish setting up the USB driver, you can continue with “Configuring TCP/IP”.

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:



Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

This wizard helps you install software for:

USB Cable Modem

If your hardware came with an installation CD or floppy disk, insert it now.

What do you want the wizard to do?

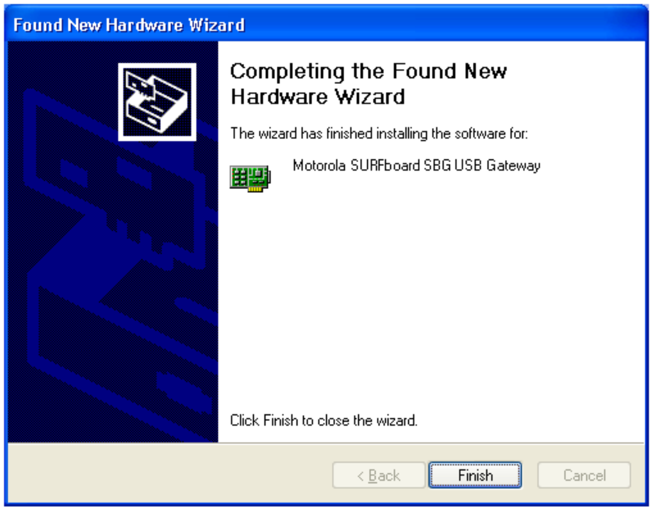
● Install the software automatically (Recommended)

○ Install from a list or specific location (Advanced)

Click Next to continue.

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:



Found New Hardware Wizard

Completing the Found New Hardware Wizard

The wizard has finished installing the software for:

Motorola SURFboard SBG USB Gateway

Click Finish to close the wizard.

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.

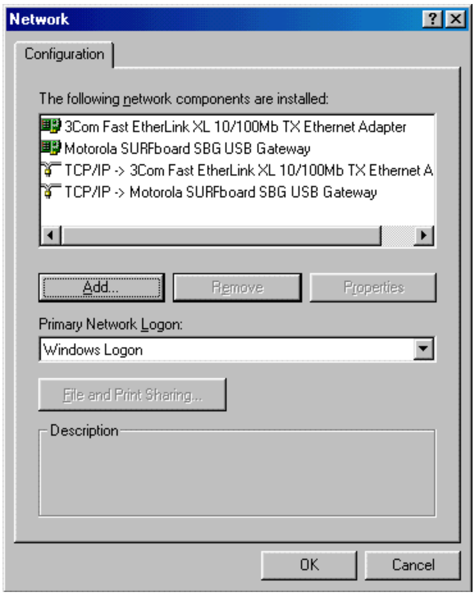
When you finish setting up the USB driver, you can continue with "Configuring TCP/IP".

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:



The following network components are installed:

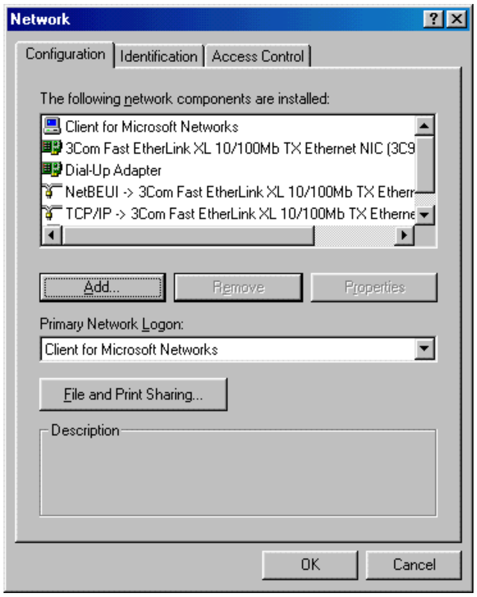
3Com Fast EtherLink XL 10/100Mb TX Ethernet Adapter
Motorola SURFboard SBG USB Gateway
TCP/IP -> 3Com Fast EtherLink XL 10/100Mb TX Ethernet A
TCP/IP -> Motorola SURFboard SBG USB Gateway

Primary Network Logon: Windows Logon

> 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:

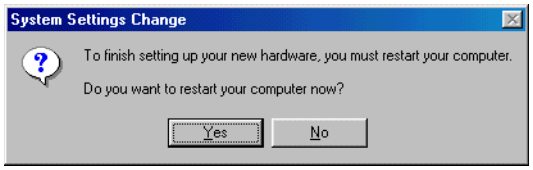


The following network components are installed:

- Client for Microsoft Networks
- 3Com Fast EtherLink XL 10/100Mb TX Ethernet NIC (3C9
- Dial-Up Adapter
- NetBEUI -> 3Com Fast EtherLink XL 10/100Mb TX Etherr
- TCP/IP -> 3Com Fast EtherLink XL 10/100Mb TX Etherne

Primary Network Logon: Client for Microsoft Networks

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



To finish setting up your new hardware, you must restart your computer.

Do you want to restart your computer now?

5 *Disconnect the USB cable from the PC or SBG940.*

6 Click **Yes** to restart the computer.

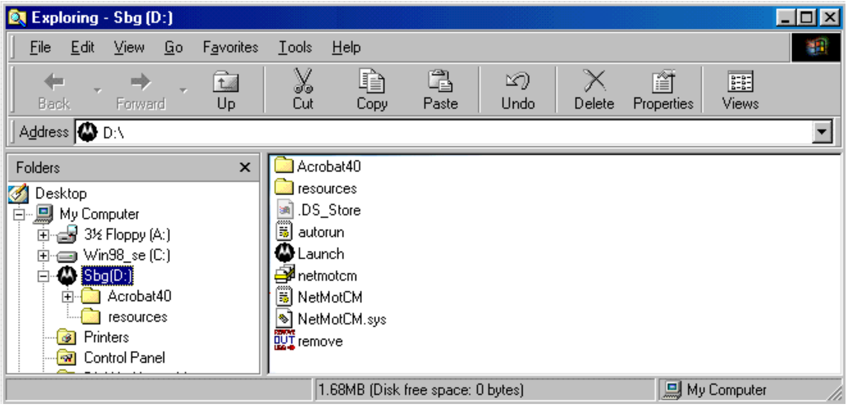
7 Insert the *SBG940 Installation* CD-ROM in the CD-ROM drive. After a short time, a window with language choices is displayed.

8 Press the **Esc** key on the keyboard to exit the start-up screens.

9 To start Windows Explorer, click **Start** and select **Run** to display the Run window.

10 Type **explorer** and click **OK.**

The Exploring window is displayed.



Address D:\

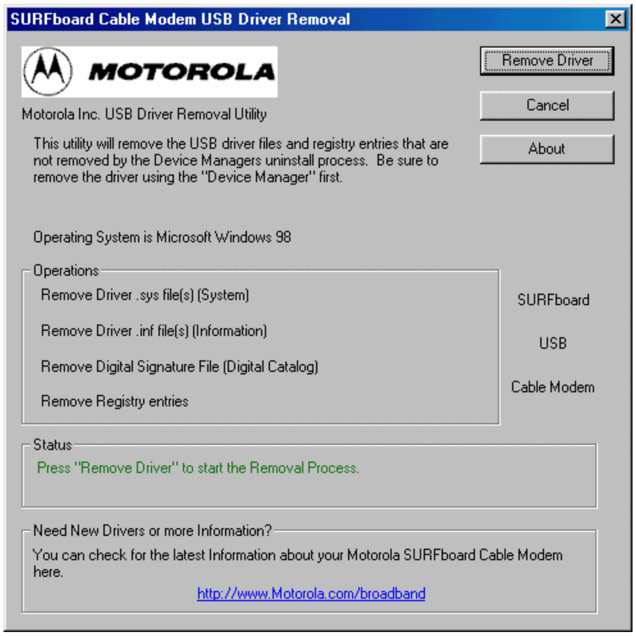
Acrobat40
resources
.DS_Store
autorun
Launch
netmotcm
NetMotCM
NetMotCM.sys
remove

1.68MB (Disk free space: 0 bytes)

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

11 Double-click the **Motorola SBG940** CD-ROM drive (D: in the image above).

12 Double-click **remove** or **remove.exe** to run the Remove utility from the *SBG940 Installation* CD-ROM. The SURFboard Cable Modem USB Driver Removal window is displayed:



Motorola Inc. USB Driver Removal Utility

This utility will remove the USB driver files and registry entries that are not removed by the Device Managers uninstall process. Be sure to remove the driver using the "Device Manager" first.

Operating System is Microsoft Windows 98

Operations
Remove Driver .sys file(s) (System)
Remove Driver .inf file(s) (Information)
Remove Digital Signature File (Digital Catalog)
Remove Registry entries

Status
Press "Remove Driver" to start the Removal Process.

Need New Drivers or more Information?
You can check for the latest Information about your Motorola SURFboard Cable Modem here.
http://www.Motorola.com/broadband

13 Click **Remove Driver**.

After you remove the USB driver, re-install it on the computer. Perform *one* of:

- Setting Up a USB Driver in Windows 98
- Setting Up a USB Driver in Windows Me

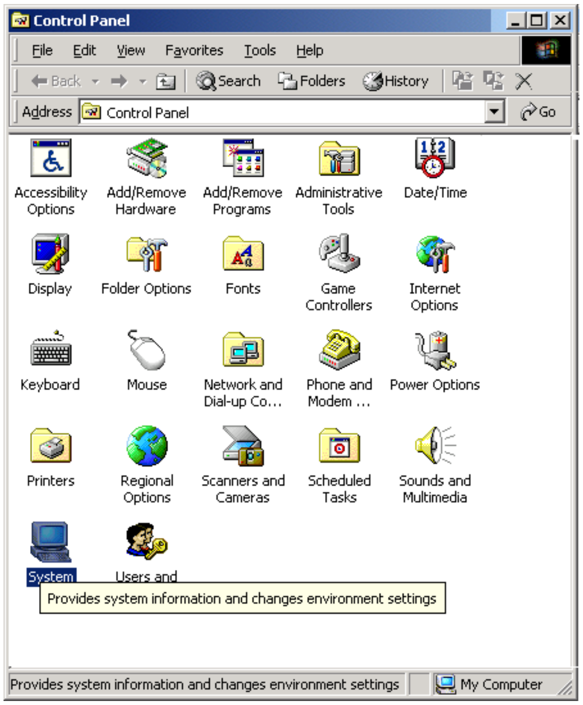
If you continue to have problems, contact your cable provider.

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:

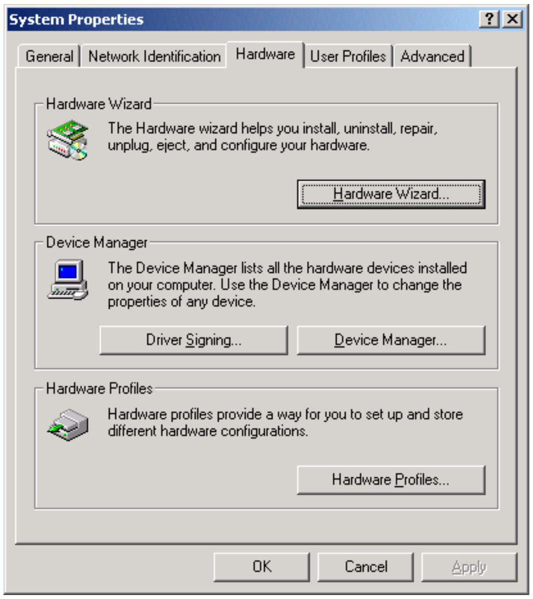


Provides system information and changes environment settings

Provides system information and changes environment settings

4 Double-click **System** to display the System Properties window.

5 Click the **Hardware** tab:

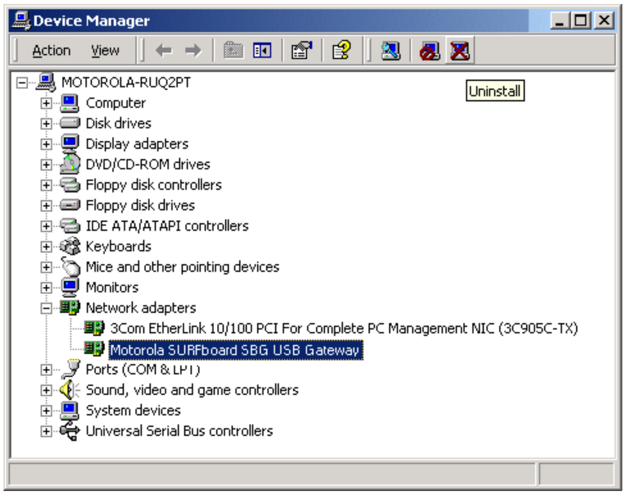


The Hardware wizard helps you install, uninstall, repair, unplug, eject, and configure your hardware.

The Device Manager lists all the hardware devices installed on your computer. Use the Device Manager to change the properties of any device.

Hardware profiles provide a way for you to set up and store different hardware configurations.

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



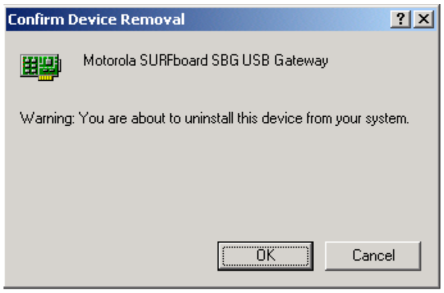
MOTOROLA-RUQ2PT
- Computer
- Disk drives
- Display adapters
- DVD/CD-ROM drives
- Floppy disk controllers
- Floppy disk drives
- IDE ATA/ATAPI controllers
- Keyboards
- Mice and other pointing devices
- Monitors
- Network adapters
  - 3Com EtherLink 10/100 PCI For Complete PC Management NIC (3C905C-TX)
  - Motorola SURFboard SBG USB Gateway
- Ports (COM & LPT)
- Sound, video and game controllers
- System devices
- Universal Serial Bus controllers

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:



Motorola SURFboard SBG USB Gateway

Warning: You are about to uninstall this device from your system.

10 Click **OK**.

11 Close the Device Manager window.

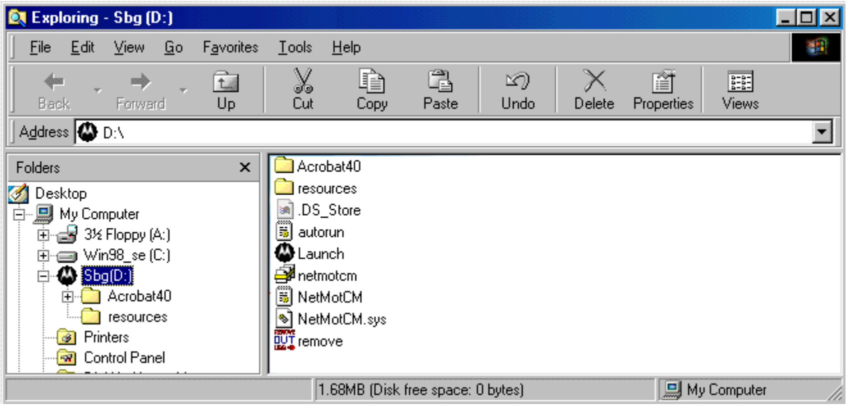
12 Close the Control Panel window.

13 Insert the *SBG940 Installation* CD-ROM in the CD-ROM drive.

14 Press the **Esc** key on the keyboard to exit the start-up screens.

15 To start Windows Explorer, click **Start** and select **Run** to display the Run window.

16 On the Run window, type **explorer** and click **OK** to display Windows Explorer:

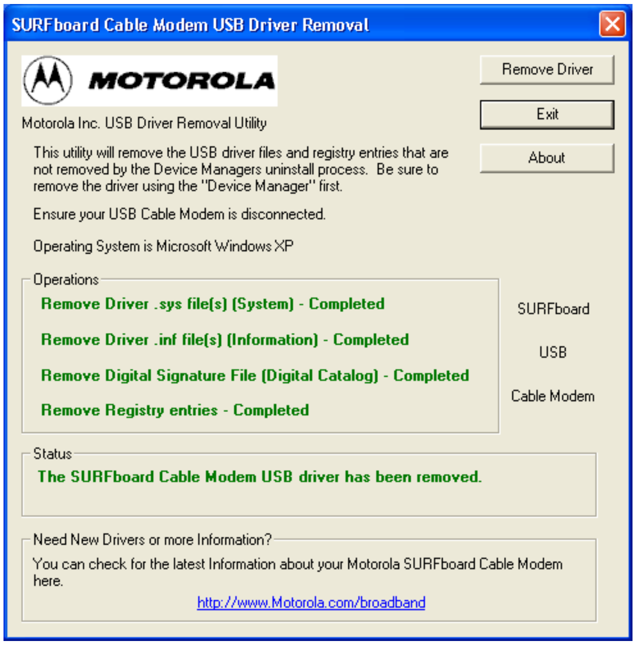


Windows Explorer may appear different than in the image. There are variations between Windows versions and you can configure Windows Explorer as you like.

17 Double-click **My Computer**.

18 Double-click the **Motorola SBG940** CD icon (D: in the image).

19 Double-click **remove** or **remove.exe** to run the Remove utility from the *SBG940 Installation* CD-ROM. The SURFboard Cable Modem USB Driver Removal window is displayed:



Motorola Inc. USB Driver Removal Utility

This utility will remove the USB driver files and registry entries that are not removed by the Device Managers uninstall process. Be sure to remove the driver using the "Device Manager" first.

Ensure your USB Cable Modem is disconnected.

Operating System is Microsoft Windows XP

Operations

Remove Driver .sys file(s) (System) - Completed

Remove Driver .inf file(s) (Information) - Completed

Remove Digital Signature File (Digital Catalog) - Completed

Remove Registry entries - Completed

Status

The SURFboard Cable Modem USB driver has been removed.

Need New Drivers or more Information?

You can check for the latest Information about your Motorola SURFboard Cable Modem here.

http://www.Motorola.com/broadband

20 *Be sure the USB cable is disconnected.*

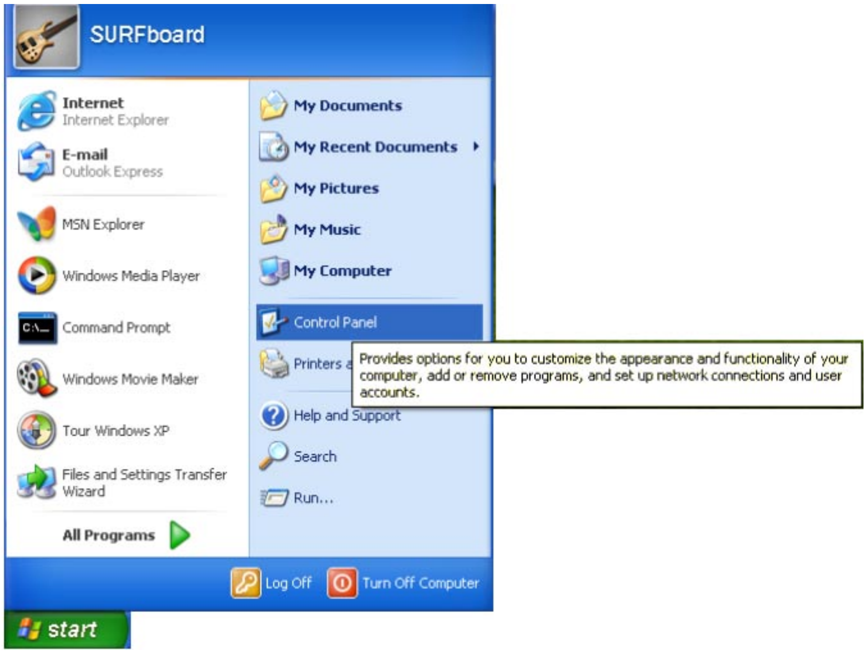
21 Click **Remove Driver.**

Informational messages similar to the ones shown are displayed on the SURFboard Cable Modem USB Driver Removal window.

After you remove the USB driver, re-install it following “Setting Up a USB Driver in Windows 2000”. If you continue to have problems, contact your cable provider.

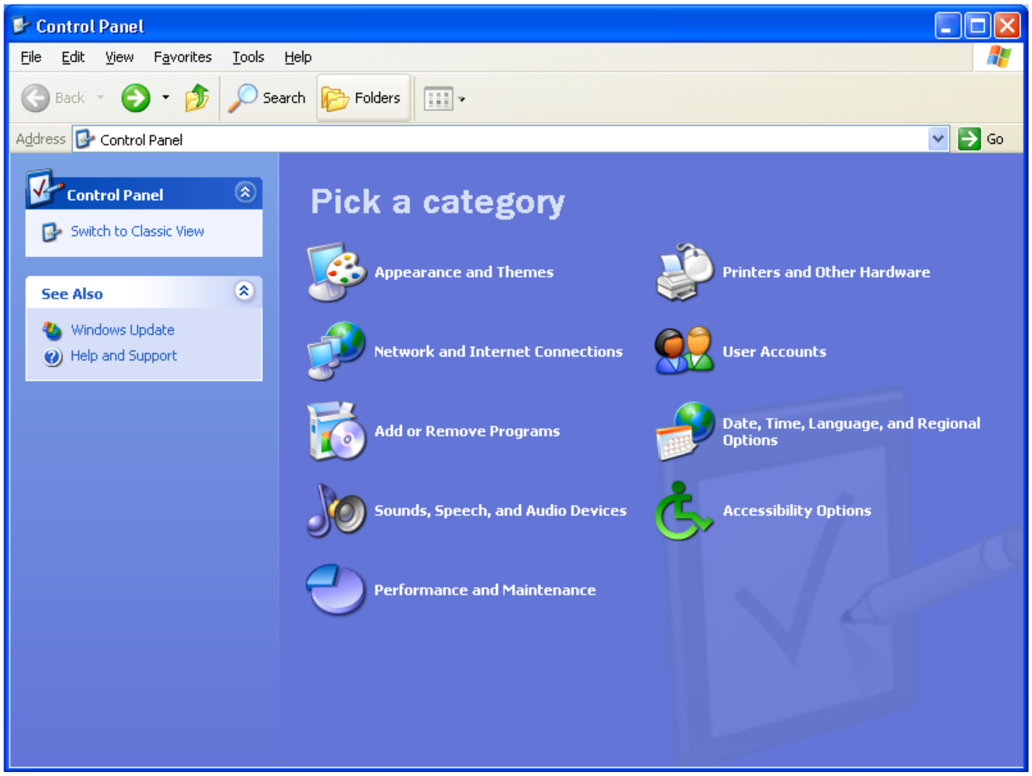
Removing the USB Driver from Windows XP

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

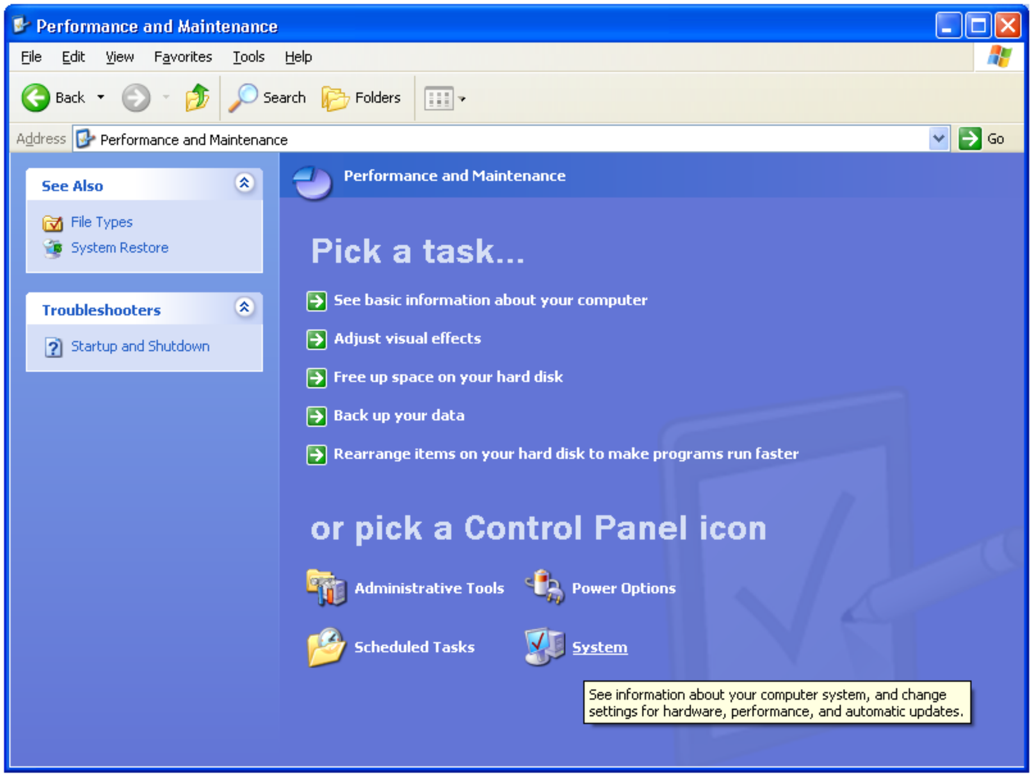


Provides options for you to customize the appearance and functionality of your computer, add or remove programs, and set up network connections and user accounts.

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



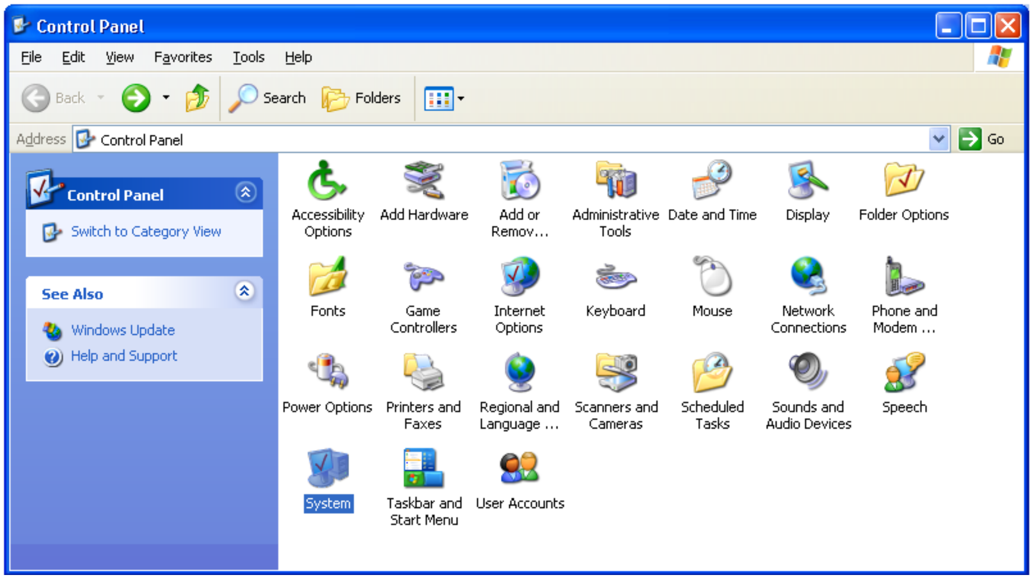
3 If a Category view similar to the image under step 2 is displayed, click **Performance and Maintenance** to display the Performance and Maintenance window. Otherwise, skip to step 5.


Performance and Maintenance
File Edit View Favorites Tools Help
Back Search Folders
Address Performance and Maintenance Go
See Also
File Types
System Restore
Troubleshooters
Startup and Shutdown
Performance and Maintenance
Pick a task...
See basic information about your computer
Adjust visual effects
Free up space on your hard disk
Back up your data
Rearrange items on your hard disk to make programs run faster
or pick a Control Panel icon
Administrative Tools
Power Options
Scheduled Tasks
System

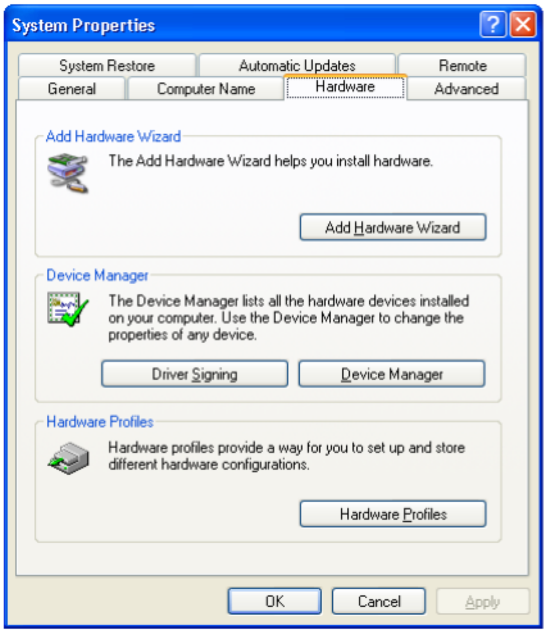
See information about your computer system, and change settings for hardware, performance, and automatic updates.

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:


System Properties

System Restore | Automatic Updates | Remote
General | Computer Name | Hardware | Advanced

Add Hardware Wizard

The Add Hardware Wizard helps you install hardware.

Add Hardware Wizard

Device Manager

The Device Manager lists all the hardware devices installed on your computer. Use the Device Manager to change the properties of any device.

Driver Signing | Device Manager

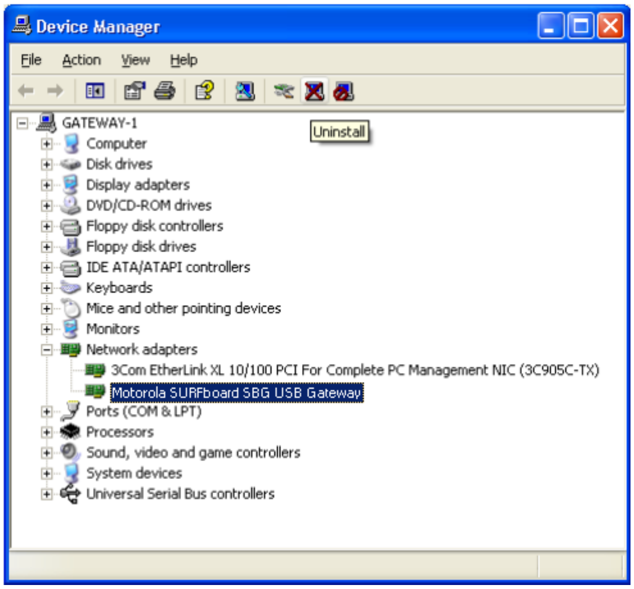
Hardware Profiles

Hardware profiles provide a way for you to set up and store different hardware configurations.

Hardware Profiles

OK | Cancel | Apply

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



```
GATEWAY-1
    Computer
    Disk drives
    Display adapters
    DVD/CD-ROM drives
    Floppy disk controllers
    Floppy disk drives
    IDE ATA/ATAPI controllers
    Keyboards
    Mice and other pointing devices
    Monitors
    Network adapters
        3Com EtherLink XL 10/100 PCI For Complete PC Management NIC (3C905C-TX)
        Motorola SURFboard SBG USB Gateway
    Ports (COM & LPT)
    Processors
    Sound, video and game controllers
    System devices
    Universal Serial Bus controllers
```

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.

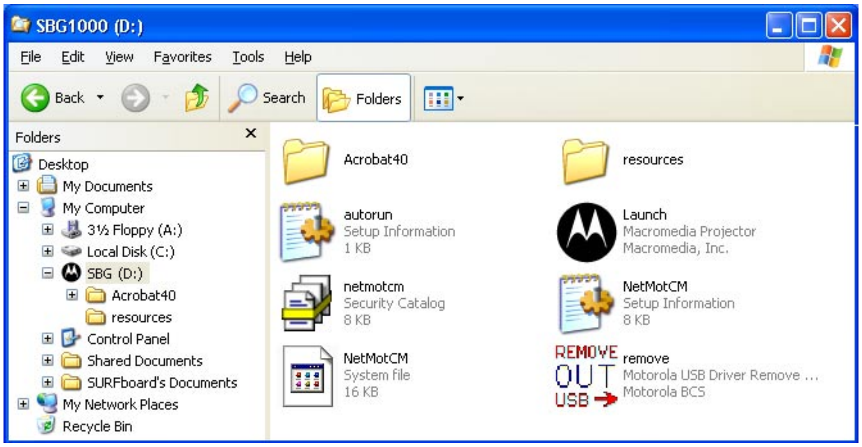
11 Close the Device Manager and Control Panel windows.

12 Insert the *SBG940 Installation* CD-ROM in the CD-ROM drive. After a short time, a window with language choices is displayed.

13 Press the **Esc** key on the keyboard to exit the start-up screens.

14 To start Windows Explorer, click **Start** and select **Run** to display the Run window.

15 Type **explorer** and click **OK** to display Windows Explorer.

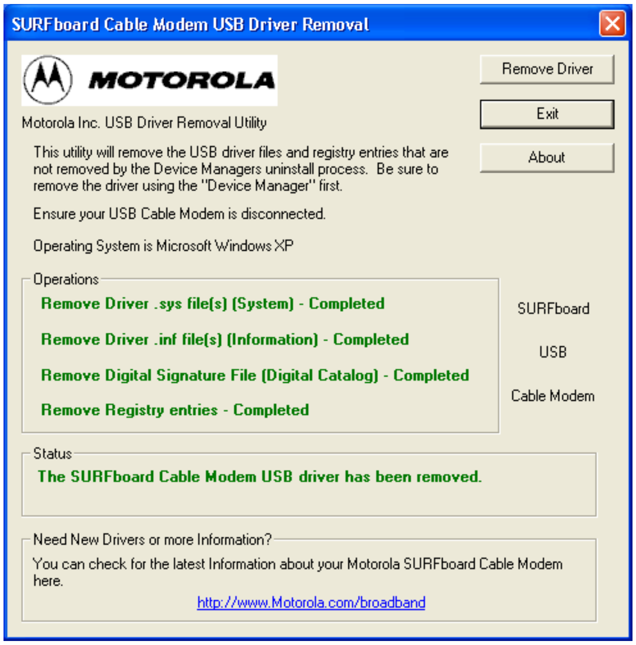


Windows Explorer may appear slightly different than in the image. There are variations between Windows versions and you can configure Windows Explorer as you like.

16 Double-click **My Computer**.

17 Double-click the **Motorola** CD icon (D: in the image).

18 Double-click **remove** or **remove.exe** to run the Remove utility from the *SBG940 Installation* CD-ROM. The SURFboard Cable Modem USB Driver Removal window is displayed:


SURFboard Cable Modem USB Driver Removal

MOTOROLA

Remove Driver

Exit

About

Motorola Inc. USB Driver Removal Utility

This utility will remove the USB driver files and registry entries that are not removed by the Device Managers uninstall process. Be sure to remove the driver using the "Device Manager" first.

Ensure your USB Cable Modem is disconnected.

Operating System is Microsoft Windows XP

Operations

Remove Driver .sys file(s) (System) - Completed

Remove Driver .inf file(s) (Information) - Completed

Remove Digital Signature File (Digital Catalog) - Completed

Remove Registry entries - Completed

SURFboard

USB

Cable Modem

Status

The SURFboard Cable Modem USB driver has been removed.

Need New Drivers or more Information?

You can check for the latest Information about your Motorola SURFboard Cable Modem here.

http://www.Motorola.com/broadband

19 Be sure the USB cable is disconnected.

20 Click **Remove Driver.** Informational messages are displayed on the SURFboard Cable Modem USB Driver Removal window.

After you remove the USB driver, re-install it following "Setting Up a USB Driver in Windows XP". 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	Turns Off During Normal Operation If
DS	The downstream receive channel cannot be acquired	The downstream channel is lost
US	The upstream send channel cannot be acquired	The upstream channel is lost
🌐	IP registration is unsuccessful	The IP registration is lost
⏻	The SBG940 is not properly plugged into the power outlet	The SBG940 is unplugged

Contact Us

In the United States and Canada, if you need assistance while working with the SBG940 and related equipment supplied by Motorola:

If you rent or lease your SBG940	Contact your cable provider.
If you own your SBG940	Call **1-877-466-8646** for technical and warranty support. Support is available 24 hours a day, seven days a week.

For information about customer service, technical support, or warranty claims, see the *Regulatory, Safety, Software License, and Warranty Information* card provided with the SURFboard 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: • +8 to +54 dBmV (32 QAM, 64 QAM) • +8 to +55 dBmV (8 QAM, 16 QAM) • +8 to +58 dBmV (QPSK) S-CDMA: • +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

[a] 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.

[b] With a CMTS supporting A-TDMA or S-CDMA *only.*

[c] 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 *wireless adapter* 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 *switch*.

broadband High bandwidth network technology that multiplexes multiple, independent carriers to carry voice, video, data, and other interactive services over a single cable. A communications medium that can transmit a relatively large amount of data in a given time period. A frequently used synonym for cable TV that can describe any technology capable of delivering multiple channels and services.

broadcast Simultaneous transmission to multiple network devices; a protocol mechanism supporting group and universal addressing. See also *multicast* and *unicast*.

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 *only.*

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 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.

On a WLAN, a client is any host that can communicate with the access point. A wireless client is also called a “station.”

CMTS A cable modem termination system is a device in the cable system headend that interfaces the HFC network to local or remote IP networks to connecting IP hosts, cable modems or gateways, and subscribers. It manages all cable modem bandwidth. It is sometimes called an edge router.

CNR carrier to noise ratio

coaxial cable (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 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:

The SBG940 is simultaneously a DHCP client and a DHCP server.

- 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 *static IP address*.

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 *half-duplex*.

G

gain The extent to which a signal is boosted. A high gain antenna increases the wireless signal level to increase the distance the signal can travel and remain usable.

gateway A device that enables communication between networks using different protocols. See also *router.*

The 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 *full-duplex*.

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 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.

Host also can mean:

- 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 On a LAN, a hub is a device that connects multiple hosts to the LAN. A hub performs no data filtering. See also *bridge* and *router*. An IP hub is typically a unit on a rack or desktop.

On an HFC network, a hub is a scaled-down headend that performs some or all headend functions for part of the system.

Hz Hertz — one cycle per second. The unit to measure the frequency that an alternating electromagnetic signal cycles through its highest and lowest states. Used to define the bands of the electromagnetic spectrum used in voice and data communications, or to define the bandwidth of a transmission medium.

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 *Ethernet*.

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 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:

- 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.

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.”

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.

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 *broadcast* and *unicast*.

mW milliwatts

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

N

NAS network access server

NAT Network Address Translation is an Internet standard for a LAN to use one set of IP addresses for internal traffic and a second set of IP addresses for external traffic. NAT provides some security because the IP addresses of SBG940 LAN computers are invisible on the Internet.

If NAT is enabled on the Gateway page, there is a one-to-one mapping between each public IP address and client IP address.

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 On a LAN, a generic term for any network device.

On an HFC network, the interface between the fiber-optic trunk and coaxial cable feeders to subscriber locations. A node is typically located in the subscriber neighborhood.

noise Random spurts of electrical energy or interface. May produce a salt-and-pepper pattern on a television picture.

O

ohm A unit of electrical resistance.

OSI The Open Systems Interconnection reference model is an illustrative model describing how data moves 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 *only*; 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 *public IP address*.

protocol A formal set of rules and conventions for exchanging data. Different computer types (for example PC, UNIX, or mainframe) can communicate if they support common protocols.

provisioning The process of 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 *POTS*.

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 *private IP address*.

Q

QAM Quadrature Amplitude Modulation uses amplitude and phase modulation to encode multiple bits of data in one signaling element. QAM achieves faster data transfer than amplitude or phase modulation alone, but the signal is more prone to errors caused by noise. QAM requires a transmission circuit with a higher CNR than alternate modulation formats such as QPSK. Two types of QAM are:

- 16 QAM 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 On IP networks, a device connecting at least two networks, which may or may not be similar. A router is typically located at a *gateway* between networks. A router operates on OSI network layer 3. It filters packets based on the IP address, examining the source and destination IP addresses to determine the best route on which to forward them.

A router is often included as part of a network switch. A router can also be implemented as software on a computer.

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 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:

- 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

A stateful-inspection firewall is more advanced than a static filter firewall.

static filter A type of firewall that examines the source and destination in the packet header based on administrator-defined rules *only*.

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 date 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 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.

Tunneling requires the following protocol types:

- 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 *broadcast* and *multicast*.

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 *access point*.

WECA The Wireless Ethernet Compatibility Alliance is a trade organization that works to ensure that all wireless devices — computer cards, laptops, air routers, PDAs, etc — can communicate with each other.

WEP Wired Equivalent Privacy encryption protects the privacy of data transmitted over a WLAN. WEP uses keys to encrypt and decrypt transmitted data. The access point must authenticate a client before it can transfer data to another client. WEP is part of IEEE 802.11b. *Because WEP can be difficult to use and does not provide very strong encryption, we recommend using WPA if possible.*

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. *We recommend using WPA if all of your client hardware supports WPA.*

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

MOTOROLA

512661-001
2/04
MGBI