User Guide

WN825
Wireless Notebook Adapters
WN825G and WN825GP

MOTOROLA
intelligence everywhere™

WN825G

WN825GP

This device must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product.

FCC Compliance Class B Digital Device

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

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

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

Canadian Compliance

This Class B digital apparatus meets all requirements of the Canadian Interference Causing Equipment Regulations. Cet appareil numérique de la classe B respects toutes les exigences du Règlement sur le matériel brouilleur du Canada.

FCC Declaration of Conformity

Motorola, Inc., Broadband Communications Sector, 101 Tournament Drive, Horsham, PA 19044, 1-215-323-1000, declares under sole responsibility that the WN825G and WPCI810G comply with 47 CFR Parts 2 and 15 of the FCC Rules as a Class B digital device. This device complies with Part 15 of FCC Rules. Operation of the device is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference that may cause undesired operation.

Wireless LAN and your Health

Caution: Exposure to Radio Frequency Radiation.

To comply with the FCC RF exposure compliance requirements, the separation distance between the antenna and any person's body (including hands, wrists, feet, and ankles) must be at least 20 cm (8 inches).

Restrictions on Use of Wireless Devices

In some situations or environments, the use of wireless devices may be restricted by the proprietor of the building or responsible representatives of the organization. For example, these situations may include:

- Using wireless equipment on board an airplane.
- Using wireless equipment in any environment where the risk of interference to other devices or services is perceived or identified as harmful.

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

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

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

FCC Certification

The WN825GP/WN825G and WPCI810GP/WPCI810G contain a radio transmitter and accordingly has been certified as compliant with 47 CFR Part 15 of the FCC Rules for intentional radiators. Products that contain a radio transmitter are labeled with FCC ID and the FCC logo.

Canada - Industry Canada (IC)

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

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

Cet appareil numérique de la classe B respects toutes les exigences du Règlement sur le matériel brouilleur du Canada

Europe - European Declaration of Conformity

All products with the CE marking comply with the EMC Directive (89/336/EEC), the Low Voltage Directive (73/23/EEC), and the R&TTE Directive (1999/5/EC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms and the equivalent international standards:

- ETS 300-826, 301 489-1General EMC requirements for radio devices.
- ETS 300-328-2 Technical requirements for Radio equipment.
- EN 60950 Safety

Caution: This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. Contact local authority for regulations.

Contents

Section 1:Overview

Section 2:Installation

Section 3:Configuration

Section 1:Overview

Congratulations on purchasing the Motorola® Wireless Notebook Adapter WN825GP or the Motorola Wireless Notebook Adapter WN825G[1].

With the WN825, laptop computers are free to join and enjoy all the benefits of an 802.11g wireless home or small office network. Once connected, you can access a single broadband connection with everyone else on the network. You can also share files, pictures, peripherals, printers, and more. You'll need one WN825 for each laptop.

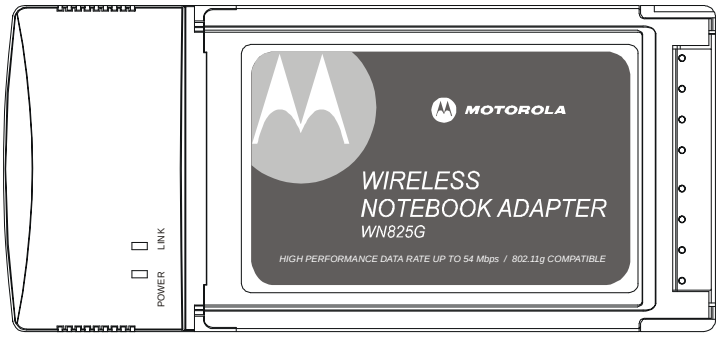
The WN825 complies with the 802.11b and the new, nearly 5-times-faster, 802.11g wireless standard. With Wi-FI® Protected Access (WPA) included, your wireless connections are robust and secure, giving you the confidence to communicate without fear that the signal could be compromised.

After installing the adapter card, you'll have the ability to wirelessly connect to your network to: send and receive emails, to print documents, or game online from your PC.

The WN825GP comes loaded with Performance Enhancement technology that accelerates your wireless network and your fun. This new technology boosts wireless performance among compatible Motorola devices up to 35% faster than over standard 802.11g networking.

With the ever-increasing number of wireless Hotspots, you'll be accessing the Internet and keeping up with your email in airports, hotels, coffee shops, and convention centers.

Wireless Notebook Adapter WN825



[1] Unless otherwise stated, this User Guide will use WN825 as the generic term for both the WN825G and WN825GP. The images of the adapter in this User Guide might or might not look exactly like your specific device.

Features

The WN825 has the following features:

- CD-ROM based Installation Wizard to provide easy installation
- Device Configuration and Status Utility
- Wireless security using WPA with TKIP encryption, 802.1X with AES and EAP-type Authentication
- Compatibility with both 802.11g and 802.11b network standards
- Upgradeable driver to stay current with the latest specifications

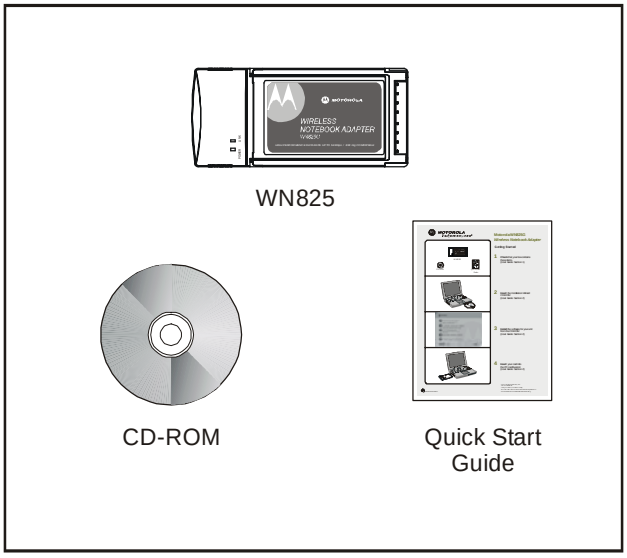
Understanding Your User Guide

The User Guide is subdivided into the following sections:

Overview	Describes the WN825 and its functions, the technology used, and recommended practices for using it.
Installation	Provides instructions for installing the hardware and setting up the firmware to get your adapter up and running.
Configuration and Status	Describes the Configuration and Status Utility that manages your WN825.
Troubleshooting	Provides a list of frequently asked questions and possible solutions.
Glossary	List of terms and acronyms.

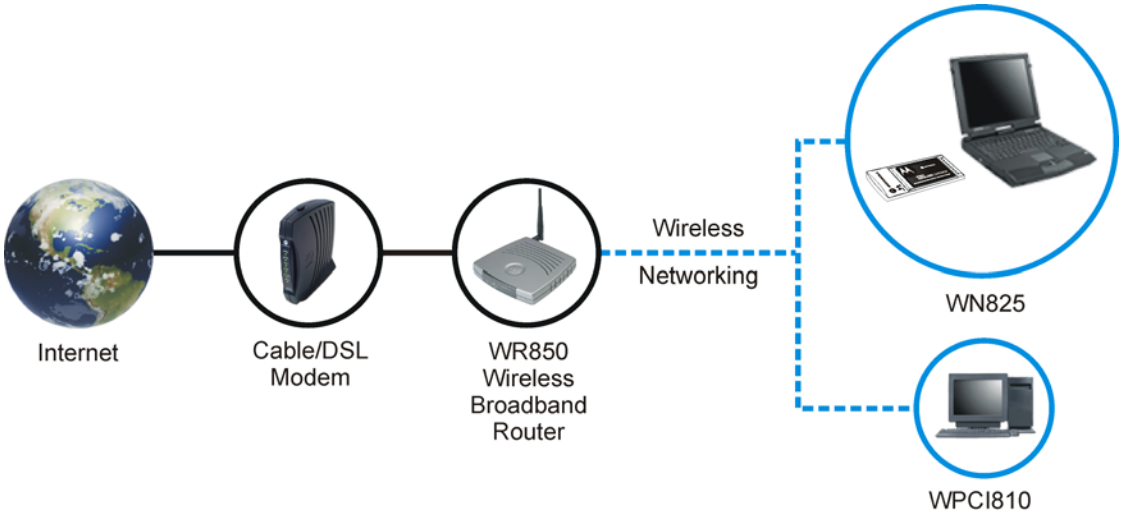
Box Contents

Your box contains the following:



Simple Home Network Diagram

Your wireless notebook adapter card, allows you to access files, printers, and an Internet connection on your network. A sample Local Area Network (LAN) is shown below:



In the example above, the Internet communicates with the modem, which in turn communicates with the router. The router acts as the gateway to your network, sending information to whichever device asks for information. The adapter card enables your notebook PC to be part of the wireless network.

Wireless Connections

Your wireless adapter card uses a radio transmission technology defined by the Institute of Electrical and Electronics Engineers (IEEE) called 802.11 Wireless Fidelity (Wi-Fi). This standard is subdivided into distinct categories of speed and the frequency spectrum used, designated by the lower case letter after the standard.

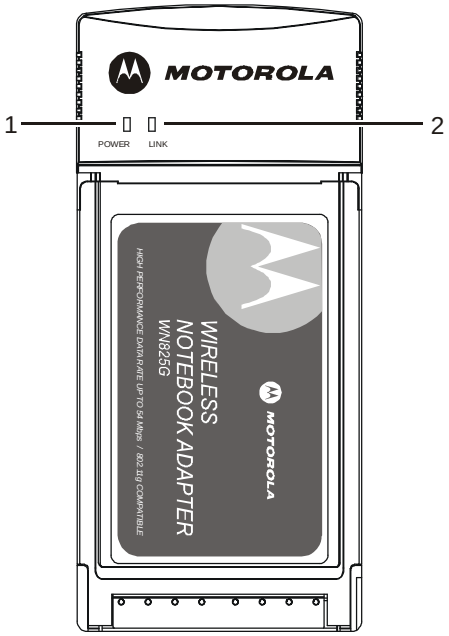
For example, your adapter card can work with both the ‘b’ and ‘g’ specifications. The 802.11b specification transmits data rates up to 11 Mbps while the 802.11g specification transmits data rates up to 54 Mbps. Both standards operate in the 2.4 GHz range. These are theoretical speeds so your performance may vary.

A Word About Data Rates: Data rate is the speed at which individual bits of data flow through a channel. It is not the same speed at which entire files are uploaded or downloaded. These speeds will vary, and are often less than the maximum data rate. Upload and download speeds are affected by several factors including, but not limited to: the capacity of and the services offered by your cable operator or broadband service provider, channel capacity, network traffic, computer equipment, type of server, number of connections to server, and availability of Internet router(s).

Adapter Card Physical Description

Top of Adapter Card

The following illustration shows the top of the WN825:

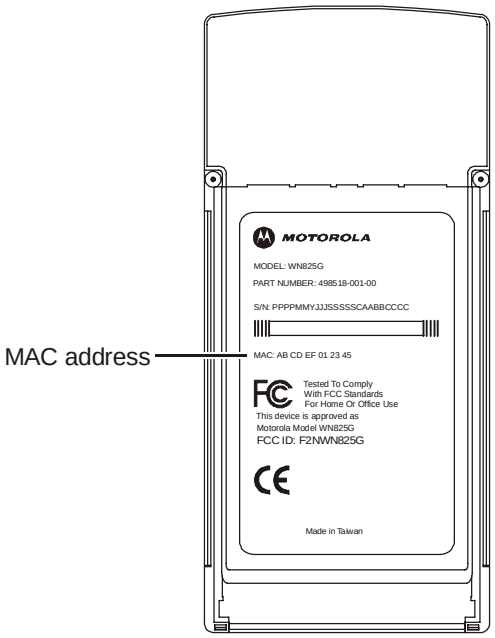


The WN825 has the following features:

	Feature	Description
1	Power LED	Indicates that the card is powered
2	Link LED	Indicates the activity of the wireless network traffic

Bottom of Adapter Card

The following illustration shows the bottom of the WN825:



The following describes the features on the bottom of the WN825:

Feature	Description
Label	Includes the model number, part number, serial number, and MAC Address
MAC Address	Location of the adapter card's MAC Address

Section 2:Installation

Before You Begin

You need to collect information so that you can setup your WN825 correctly. Depending upon where you are connecting, the type of information required is divided between business (enterprise users) and home settings (small office/home office).

Also, you need to consider the type of security to enable for your wireless connection. A discussion of the types of security available follows this section.

Enterprise Users

Obtain the following information from your network administrator:

- Network names (SSID) of the specific wireless networks to which you are going to connect.
- WPA (Wi-Fi Protected Access) wireless network key information (may include network authentication type, encryption type, network key) for any WPA enabled networks to which you want to connect.
- WEP (Wired Equivalent Privacy) wireless network key information (network key) for any WEP enabled networks to which you want to connect.
- For Microsoft® Windows® networking, the customer name and workgroup name.
- For a network account, the domain name, a user name and password.
- An IP address (if not using a DHCP server).
- Networks connected to an authentication server, if any.

Small Office/Home Office Users

The access point that communicates with the WN825 has a pre-assigned network name (SSID) that the WN825 recognizes upon startup.

- If you are setting up a new wireless network with WEP security, the WN825 should use the same network key you used for your network.

  For more information on WEP security, see "Security Options".

- If you are connecting to an existing WEP enabled network, obtain the network key from the access point.
- If you are connecting to a WPA-enabled access point, obtain the WPA (Wi-Fi Protected Access) wireless network key information (network authentication type, encryption type, network key) from the access point.

Security Options

The WN825 is designed for both the home user and business. WPA (Wi-Fi Protected Access) protocol is designed into the WN825. WPA is a powerful, standards-based, interoperable security technology for wireless local area networks (the subset of the future IEEE Std 802.11i standard) that encrypts data sent over radio waves.

The WPA protocol was developed to overcome the weaknesses of the WEP (Wired Equivalent Privacy) protocol. Both protocols require the use of network key information, and either protocol can be enabled or disabled, depending on the type of network connection being made.

Various options are available for selecting network authentication and data encryption. It is important for you to understand these options when deciding which (if any) security protocol to use.

Security Example

If you want to use a more secure protocol, the wireless network to which you are connecting must also support that protocol. For example, you decide to enable WPA-PSK on your WN825, a good choice because of the robust security WPA-PSK offers. However, the slightly older wireless network you want to connect to only supports WEP, which means that you cannot use WPA (and should use WEP) because the security protocols must match between the network adapter and the access point.

The options supported by the adapter:

Network Authentication		Data Encryption	
Option	**Description**	**Option**	**Description**
Open	A network can be set up either to use or not use a network key for data encryption. WEP is the type of encryption used. Open WEP is the first-generation basic level security for wireless networks.	Disabled	No encryption used.
		WEP	A network key used.
Shared	The network operates in Shared Key authentication mode when a network key is used for data encryption. Data encryption can be enabled or disabled. WEP is the type of encryption used. The Shared Key authentication mode is the least secure.	Disabled	No encryption used.
		WEP	A network key used.
WPA	The network operates in IEEE 802.1x authentication mode. This mode is for environments with a Remote Access Dial-In User Service (RADIUS) infrastructure. This environment requires heavy technical support to set up and maintain and is used by large corporations. In a RADIUS environment, various Extensible Authentication Protocols (EAPs) are supported. These may include TLS, TTLS, PEAP, and LEAP.	TKIP	A network key used (more secure).
		AES	A network key used (most secure).
WPA-PSK	For infrastructure environments without the RADIUS infrastructure. WPA-PSK supports the use of a pre-shared key. WPA-PSK is the next generation of wireless network security for home and small office environments.	TKIP	A network key used (more secure).
		AES – available with Windows XP with WPA patch, using Wireless Zero Configuration	A network key used (most secure).

Install Your Card

To install the software and hardware:

1. Insert the supplied CD-ROM into the CD-ROM drive. The software automatically starts the Installation Wizard program.
2. Follow the prompts to set up your adapter card.

   If Windows 98SE prompts you for the original Windows CD-ROM, insert the CD-ROM, and direct Windows to its proper location (for example, D:\WIN98).
3. Locate an empty CardBus slot on your notebook computer.
4. With the adapter card product-label and LEDs facing up, insert the adapter card into the CardBus slot:

5. Complete the installation instructions supplied on the CD-ROM.

Device Configuration Setup

After installing the adapter card and software, you will need to connect to a network. Refer to Section 3: Configuration for information on how to create detailed connectivity profiles so you can connect to a wireless network, setup security, and setup modes of operation.

Section 3:Configuration

You can use the information in this section to:

- Discover available wireless networks
- Setup operation modes
- Create connectivity profiles
- Set up security
- Monitor the wireless network / environment
- Perform diagnostic discovery

The screenshots shown may look slightly different from the ones in your version of the software.

Icon Description

The icon in you system tray (the area at the bottom right of your screen in your Task Bar) allows you to view the status of the wireless connection and access the Motorola Wireless Configuration Utility.

The following table describes the icons used by the utility.

Antenna Icons

	The radio transmitter has been disabled from the utility. To enable, access the utility's Wireless Networks tab.
	There are no networks available.
	The signal strength is Very Low.
	The signal strength is Low.
	The signal strength is Good.
	The signal strength is Very Good.
	The signal strength is Excellent. The small bars on either side of the antenna indicate network activity. The bar on the left indicates receive and the bar on the right indicates transmit.

Wireless Network Icons

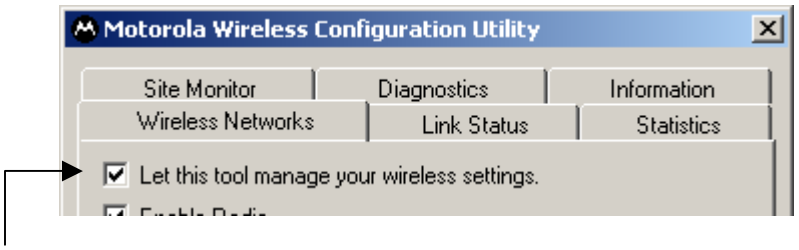
	The infrastructure network is connected and communicating.
	The infrastructure network is configured or available, but not communicating.
	The infrastructure network is not available.
	The ad-hoc network is connected.
	The configured ad-hoc network is not available.

Enabling the Motorola Wireless Configuration Utility

Windows XP users have the option of using the Wireless Zero Configuration utility, but will be limited in the amount of status information available. Motorola's Wireless Configuration Utility provides more wireless information about the network.

To enable the Motorola Wireless Configuration Utility:

1 Right-click the **antenna icon** in the system tray and select **Open Utility**. The Motorola Wireless Configuration Utility window is displayed:



2 Check **Let this tool manage your wireless settings** if not enabled.

3 Unless you are using Windows XP, do not clear **Let this tool manage your wireless settings**. If using Windows XP, you can use the Windows XP Wireless Zero Configuration (WZC) utility to manage your wireless client adapter.

4 Click **OK** to save your changes.

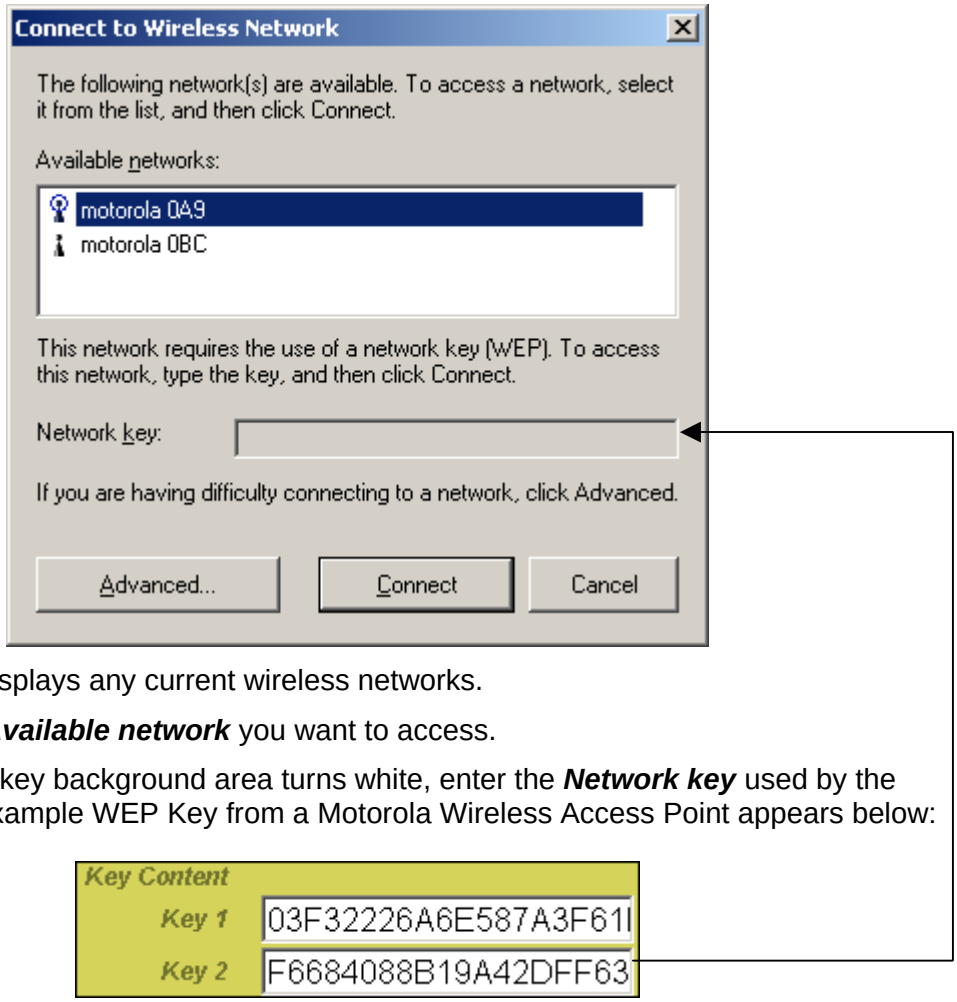
Connecting to an Existing Wireless Network

After the adapter card is installed, a red antenna icon displays in your computer's system tray  .

The Motorola Wireless Configuration Utility automatically searches for available wireless networks. A list of networks appears when you open the utility from the system tray. Wireless Networks identify themselves with their Network Name (SSID), as seen in the Available networks field in the example below.

To quickly connect to an existing wireless network:

1 Click the **antenna icon**. The Connect to Wireless Network window is displayed:



The window displays any current wireless networks.

2 Highlight the ***Available network*** you want to access.

3 If the Network key background area turns white, enter the ***Network key*** used by the network. An example WEP Key from a Motorola Wireless Access Point appears below:

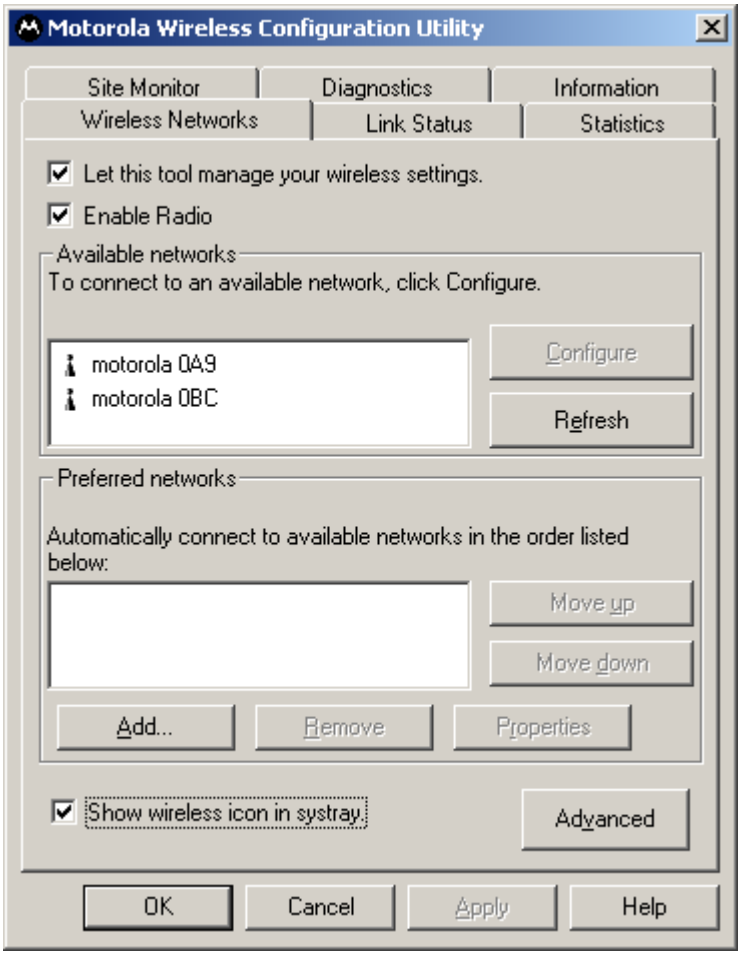
4 Click **Connect** to access to your wireless network.

Configuring a New Wireless Network

If you want to connect to a wireless network that is not in the Available networks field, you can configure a network profile.

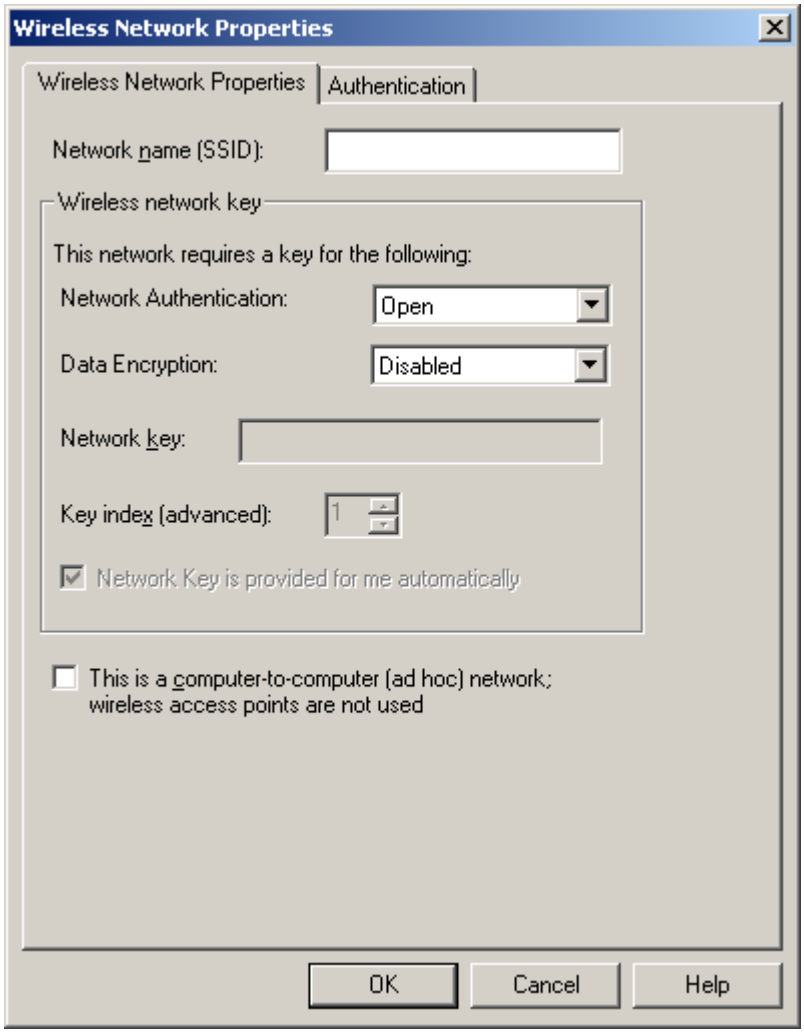
1 Right-click the **antenna icon** in the system tray and select **Open Utility**.

2 The Motorola Wireless Configuration Utility window is displayed:



3 Click **Add**.

4 The Wireless Network Properties window is displayed.



5 Enter information for the new wireless network based on the descriptions in the following table.

Field	Description
Network name (SSID)	Enter a Network Name (SSID) of no more than 32 alphanumeric characters. This is the SSID for a particular wireless network. *The Network Name (SSID) is case-sensitive.*

Field	Description
Network Authentication	Select if your access point requires authentication. Match the authentication used by the network.

Open	No authentication is used.
Shared	The Pre-Shared Key (PSK) authentication method is used.
802.1X	IEEE port based network access control authentication method is used.
WPA	Wi-Fi® Protected Access (WPA) authentication (802.1X) is used with an EAP type.
WPA-PSK	WPA authentication (802.1X) is used with a Pre-Shared Key, which enables you to enter a static Network key.
CCKM	Cisco® proprietary standard Lightweight Extensible Authentication Protocol (LEAP).

Note: If you select WPA, WPA-PSK, or CCKM, you may be required to enter further information on the *Authentication* tab. Ask your network administrator for additional information.

Data Encryption Select the type of security encryption algorithm used. The available types of encryption are based on the type of the authentication selected.

Disabled	No encryption. Available only with Open and Shared authentication.
WEP	Deselect *Network Key is provided for me automatically* and enter the Key provided by the network. Available only with Open, Shared, 802.1X, and CCKM Authentication.
TKIP	Available with WPA, WPA-PSK, and CCKM Authentication.
AES	Available with WPA and WPA-PSK Authentication.
CKIP	Available with CCKM (Cisco Centralized Key Management) Authentication.

Network key Enter the security key for data encryption, when WEP or WPA-PSK is selected. This can be entered in ASCII or hexadecimal for WEP and in ASCII for WPA-PSK.

Field	Description
Key index (advanced)	There are four Keys (1, 2, 3, 4) that can be selected for WEP. The key index selected here must match the network's key index.
The key is provided for me automatically	Select if the key is automatically provided. Most often, the key is not automatically provided, so you have to un-check this box and enter the network key. If using a RADIUS server, the key is automatically provided.
This is a computer-to-computer (ad hoc) network	Select if the network you are creating or accessing is a computer-to computer (ad hoc) network. If you are attempting to connect to an infrastructure network, then do not select this setting.

6 After entering the information for this network, click **OK**. The Wireless Network window is displayed and the new network is listed in the Preferred networks area.

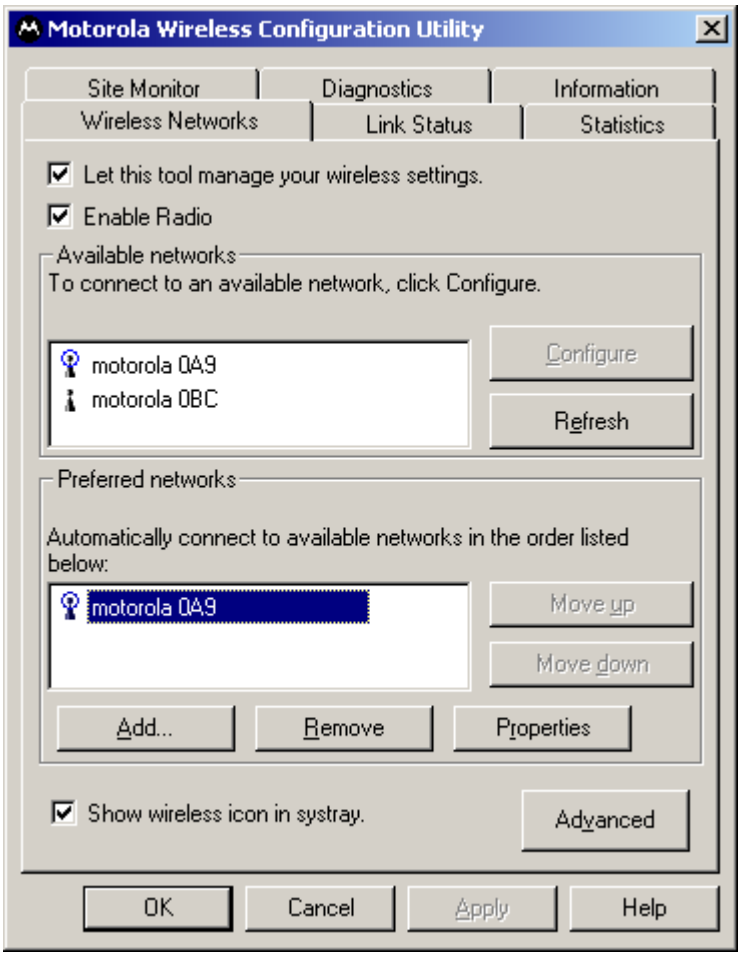
7 Your computer is connected to the selected network when you see a blue bubble on top of the icon for that network. If the blue bubble does not appear, click **Refresh**. If it still does not appear, double-check that the wireless settings match the configuration of the wireless network.

Modifying Properties for a Configured Wireless Network

To configure network properties for a configured wireless network:

1 Right-click the **antenna icon** in the system tray and select **Open Utility**.

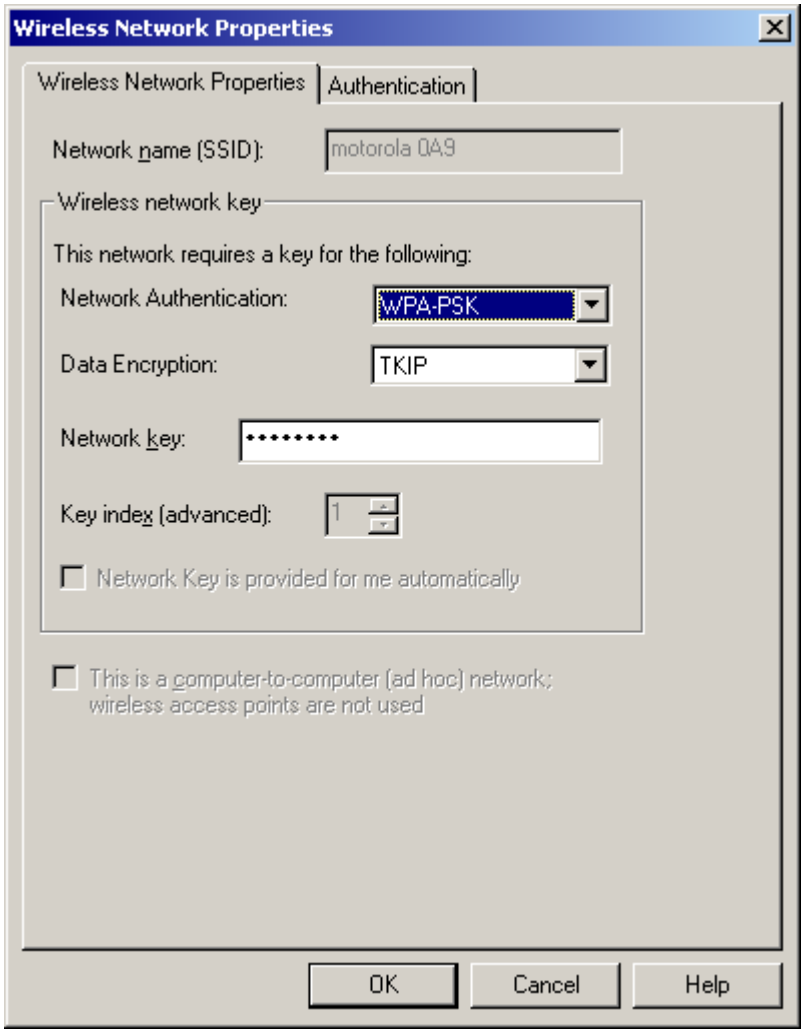
2 The Motorola Wireless Configuration Utility window displays:



Your computer automatically connects to the network displayed at the top of the **Preferred networks** list.

3 In the Preferred networks list, highlight the ***network*** you want to configure and click **Properties**.

4 The Wireless Network Properties window displays with the current settings:



5 If the network requires Network Authentication, select the type of authentication required. WPA and CCX might require further Authentication options found on the Authentication tab. Match the setting used by the network.

6 If the network requires Data Encryption, select the type of encryption required. Match the setting used by the network.

7 If using WPA-PSK, enter the Pass Phrase in the Network key field.

– In the example above, the network is configured for **WPA-PSK** for Authentication and **TKIP** for Encryption.

8 For additional information about the fields on this window, refer to Configuring a New Wireless Network.

9 Click **OK** to save your changes.

Performance Enhancement

This feature applies only to the WN825GP Wireless Notebook Adapter.

When enabled, the wireless data throughput of a WN825GP Wireless Notebook Adapter is boosted when used exclusively with Performance Enhanced base stations, such as the WR850GP Wireless Router and/or WA840GP Wireless Access Point.

When the Performance Enhancement feature is enabled, the wireless network can still support non-Performance Enhanced client devices, including standard 802.11g and/or 802.11b devices. Under these conditions the network steps down to support full backward compatibility, but the WN825GP will still function normally.

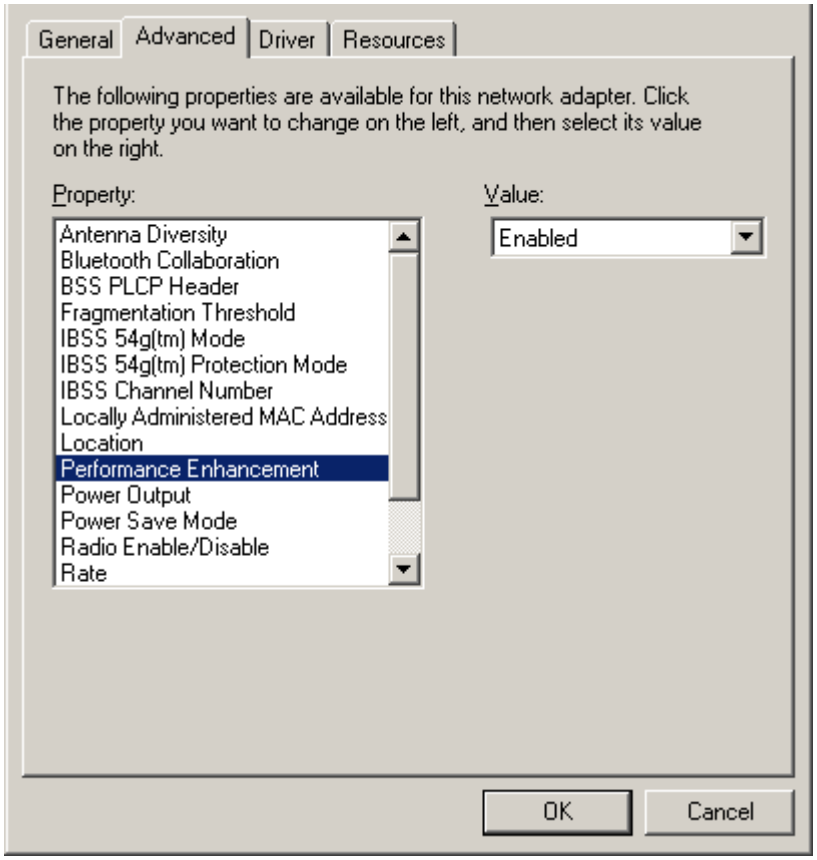
1 Click **Start**, click **Settings**, and then click **Control Panel**.

2 Click **System** and select the **Hardware** tab.

3 Click **Device Manager**.

4 Click **Network adapters**.

5 Click **Motorola Wireless Network Adapter WN825** and select the **Advanced** tab.



6 To toggle the feature on or off, select **Enabled** or **Disabled** from the Value drop down menu.

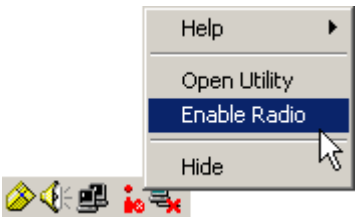
7 Click **OK** to save the changes and exit.

Controlling the Radio

You may need to turn off the radio to comply with restrictions prohibiting the emission of radio signals; for example, while onboard a commercial aircraft.

1 To disable the radio using the antenna icon, right-click the **antenna icon** in the system tray and click **Disable Radio**.

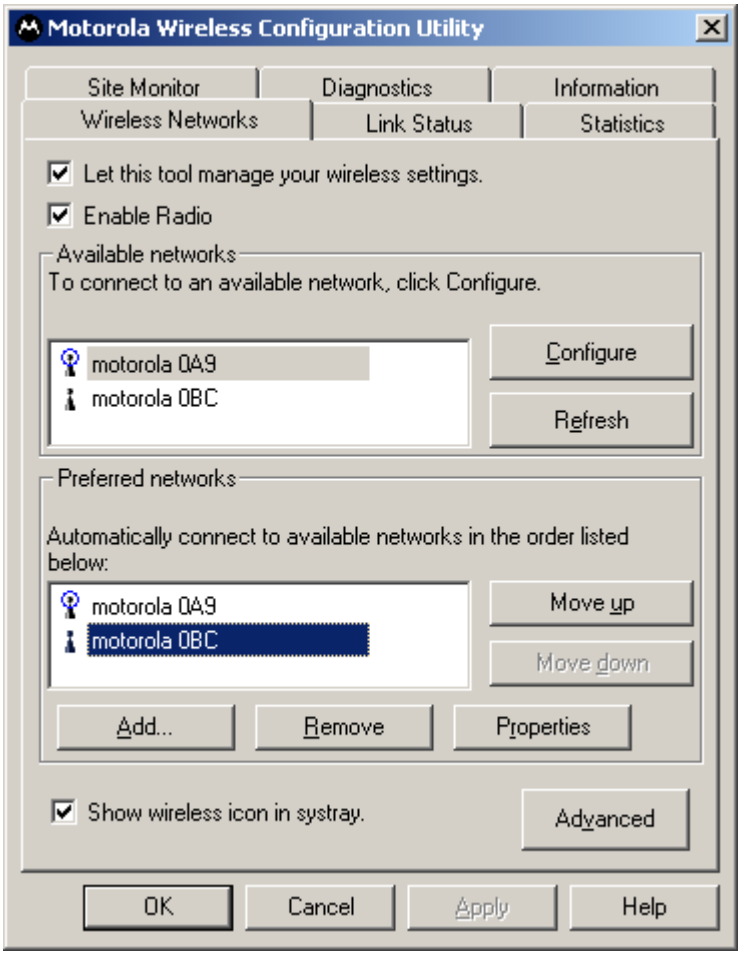
2 To enable the radio, right-click the **antenna icon** and click **Enable Radio**.



Preferred Networks – Setting up the Connection Order

There are two ways to specify the order that the adapter uses to connect to an available network in your Preferred networks list:

- Using the Move Up and Move Down buttons
- Using Advanced Selection Rules



Move Up and Move Down buttons

Use the Move up and Move down buttons to move a network up and down in the list of Preferred networks. The adapter tries to connect to a wireless network in the order you specify in the Preferred networks list.

To move a network within the list:

1 Highlight the ***network*** you want to move.

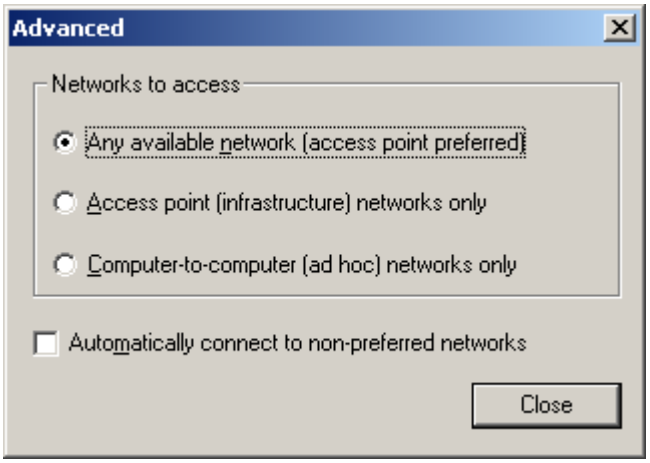
2 Click either the **Move up** or **Move down** button depending on where you want the selected network to appear in the list. In the example above, the 2nd network is selected, and the **Move up** button is active, showing that you can move that network up when the button is clicked.

Advanced Selection Rules

You can use some advanced rules for displaying networks from the list of Preferred networks.

To select an advanced rule:

1 From the Motorola Wireless Configuration Utility window, on the Wireless Networks tab, click **Advanced**. The Advanced window displays:



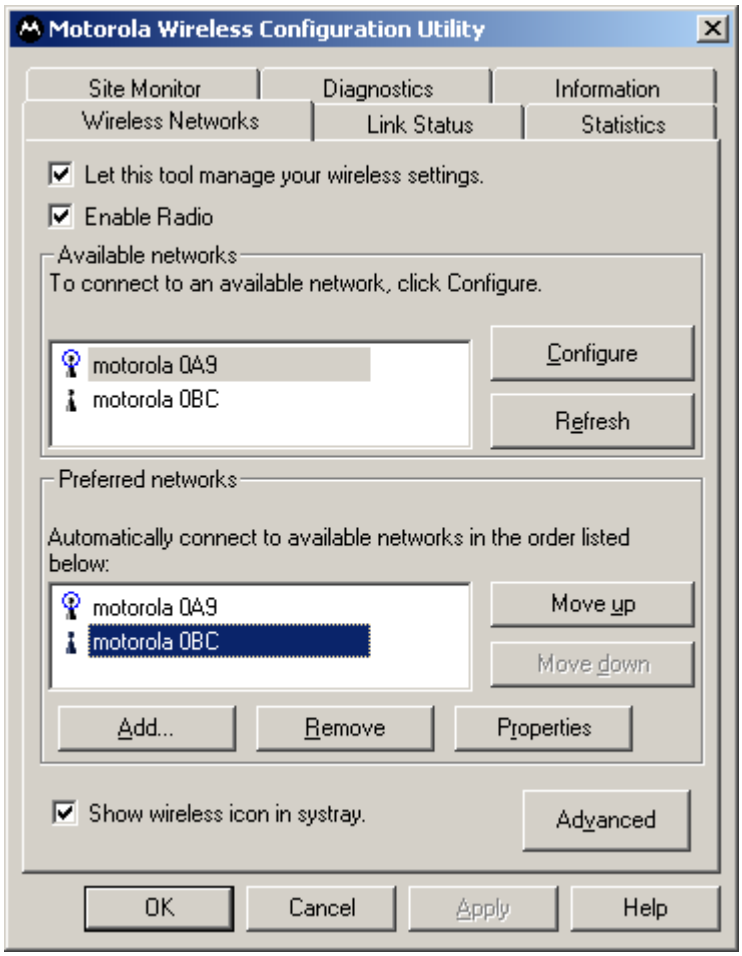
2 Choose one of the three ways to display and choose networks from the list. Choosing *Access point networks only* or *Computer-to-computer networks only* limits the number of networks in your preferred list.

3 Selecting *Automatically connect to non-preferred networks* allows you to connect to any network your utility can find. For example, this is useful if you are traveling with your computer and need to access wireless networks in hotels or airports.

Removing a Network from Your Preferred Network List

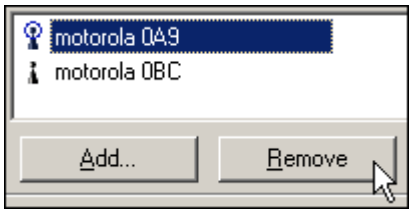
To remove a wireless network from your preferred network list:

1 Right-click the **antenna icon** in the system tray and select **Open Utility**. The Motorola Wireless Configuration Utility window displays.



2 In the Preferred networks list, highlight the ***network*** you want to remove.

3 Click **Remove**.



The network is removed from your preferred network list.

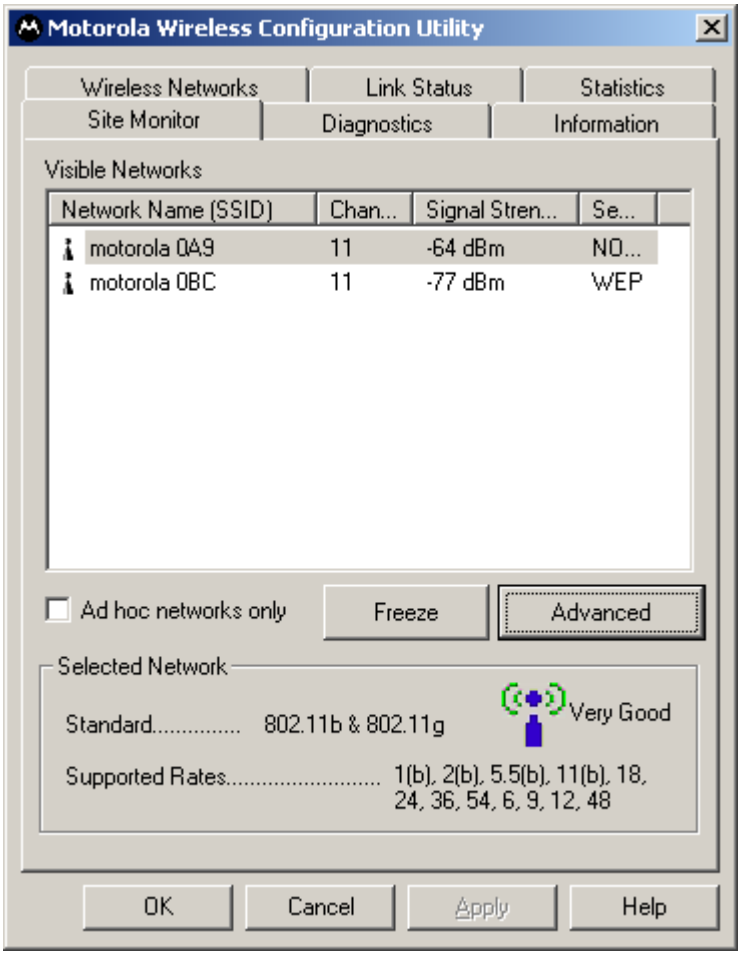
4 Click **Apply** or **OK** to save the change.

Viewing Site Monitor Information

To view site monitor information:

1 Right-click the **antenna icon** in the system tray and select **Open Utility**. The Motorola Wireless Configuration Utility window displays.

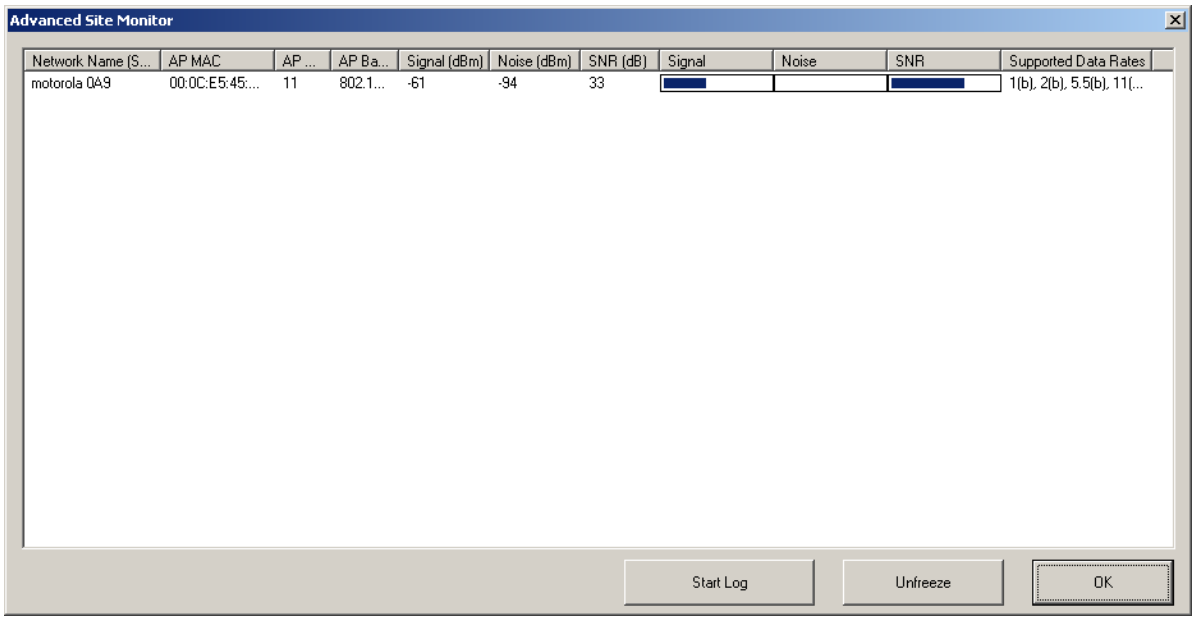
2 Click the **Site Monitor** tab.



The Visible Networks list provides information about all of the detected networks: the Network Name (SSID), Channel, Signal Strength, and Security.

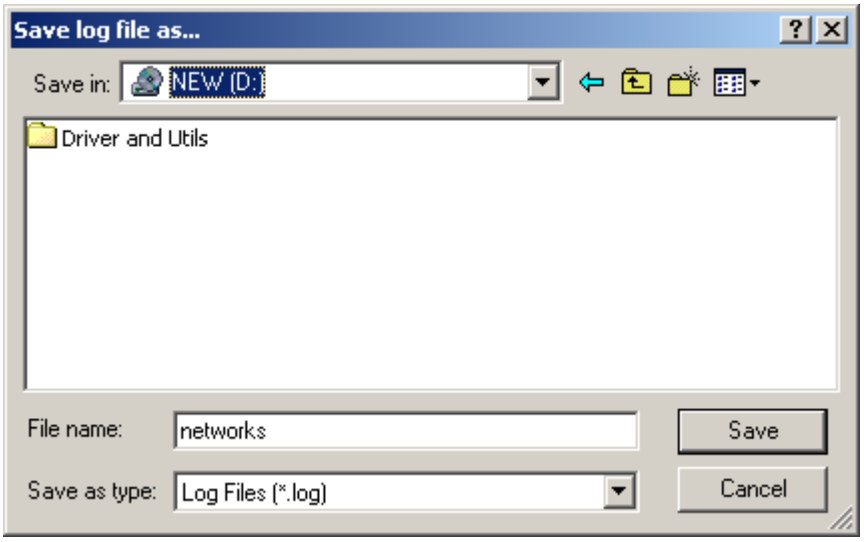
3 In the **Selected Network** area of the window, highlight a ***network*** to get more information about that network. This area provides information about which wireless transmission standard is used on the network, a graphic representation of the signal strength, and the supported transmission rates.

4 To obtain more information about a selected network, click **Advanced**. The Advanced Site Monitor window displays:



This window provides detailed information about the network selected.

5 To start a log of network activity, click **Start Log**. The Save log file as window displays:



6 Select a ***drive*** and ***directory*** to store the networks.log file.

7 Click **Save**.

The adapter saves a log of the information listed on the Advanced Site Monitor window to the networks.log file. The information is sent to the file approximately every six seconds. The log is a comma-delimited list that can be imported to a spreadsheet to enable you to view the activity on the network over a specific time period.

8 Click **Stop Log** to stop the log information from being sent to the networks.log file.

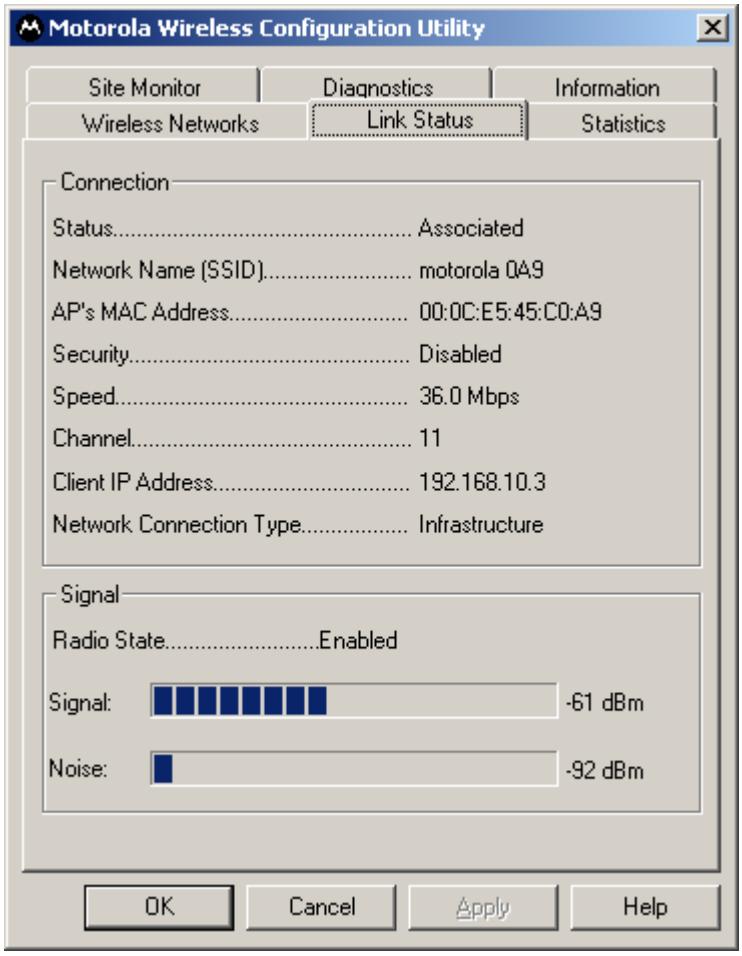
9 To freeze the display, click **Freeze**.

Viewing Link Status

To view link status:

1 Right-click the **antenna icon** in the system tray and select **Open Utility**. The Motorola Wireless Configuration Utility window displays.

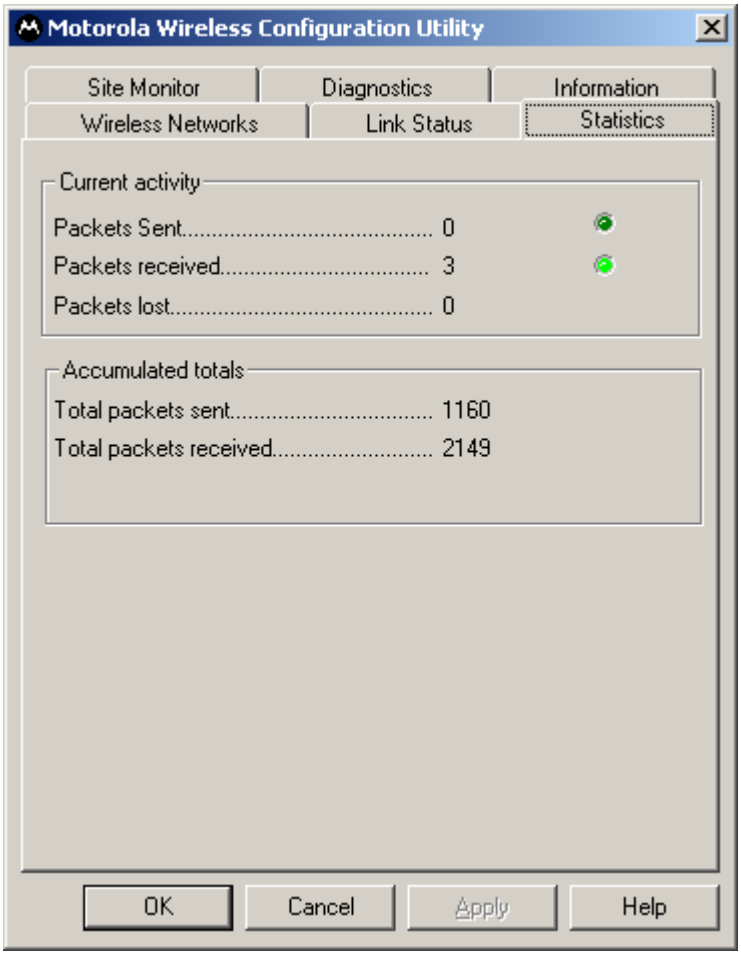
2 Click the **Link Status** tab. The Link Status tab provides information about the currently connected wireless network:



Viewing Network Statistics

To view statistics for the network you are connected to:

1. Right-click the **antenna icon** in the system tray and select **Open Utility**. The Motorola Wireless Configuration Utility window displays.
2. Click the **Statistics** tab. The Statistics tab provides information about the selected wireless network:

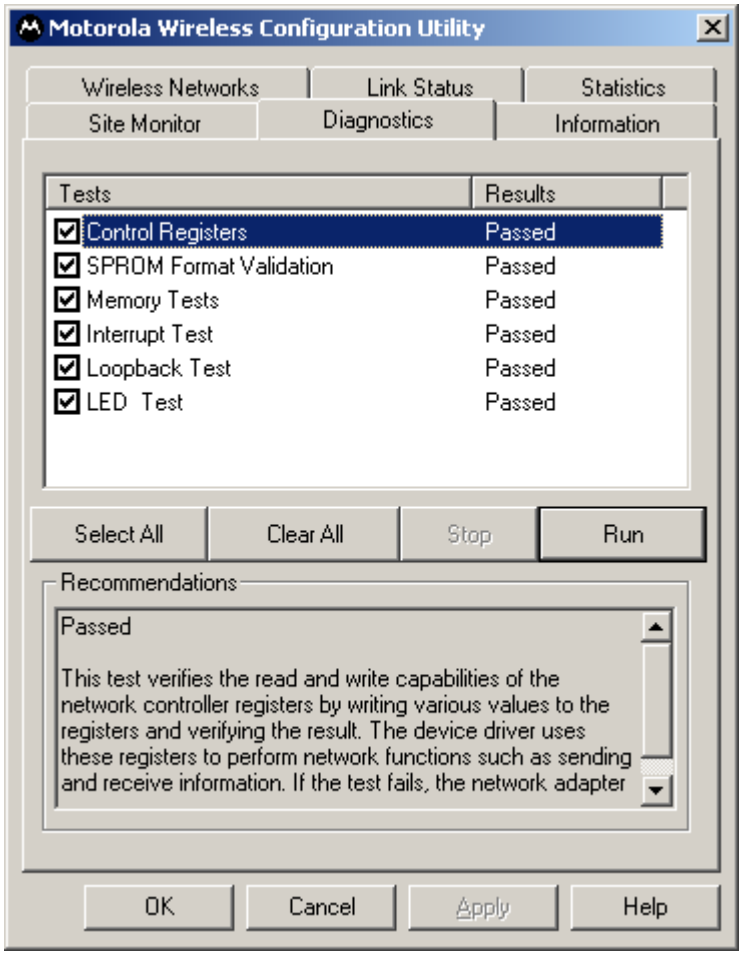


Diagnostics

This tab helps you to isolate problems that might be occurring with your adapter.

1 Right-click the **antenna icon** in the system tray and select **Open Utility**. The Motorola Wireless Configuration Utility window displays.

2 Click the **Diagnostics** tab.



3 Various diagnostic tests are available. Select a test to learn more about it.

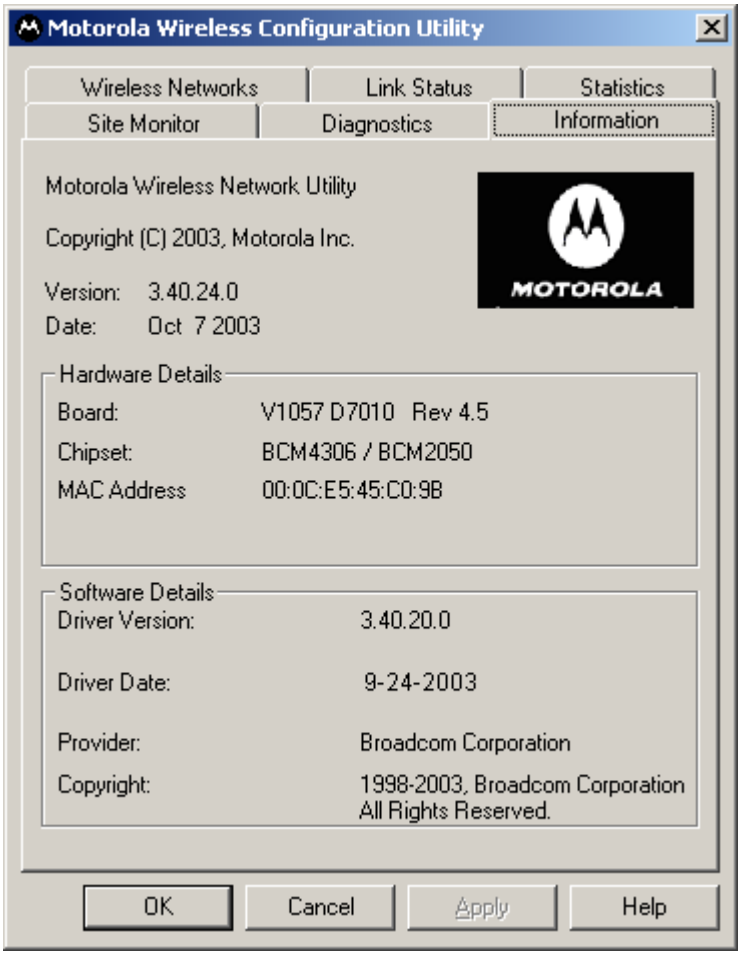
4 Click the ***desired test*** to enable and click **Run**. The results, Passed or Failed, are displayed in the next column.

5 Click the ***desired test*** to view individual results, which appear in the Recommendations field.

Viewing Utility and Driver Version Information

To view product information for the adapter installed in your PC:

1. Right-click the **antenna icon** in the system tray and select **Open Utility**. The Motorola Wireless Configuration Utility window displays.
2. Click the **Information** tab. The Information tab provides the firmware version number and hardware and software details about the adapter card:

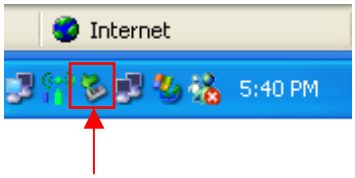


Removing the Wireless Adapter

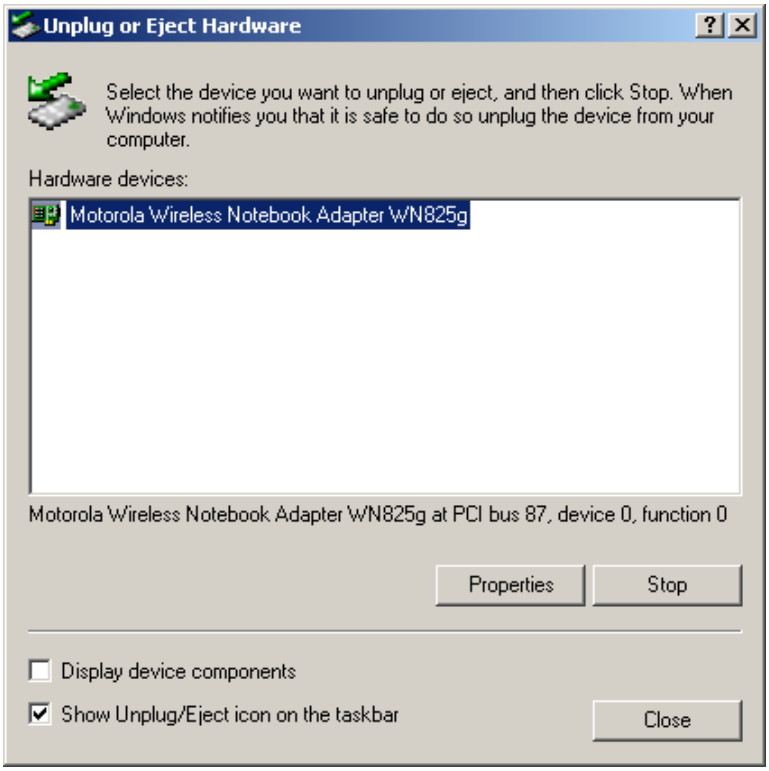
You can safely remove the Wireless Adapter while the PC is operating. If you encounter problems removing the device, then follow the steps below.

To remove the adapter:

1 Locate the **Device Eject icon** located in your system tray. In the illustration below, it is the third icon from the left – the picture of a card and a left-pointing arrow.

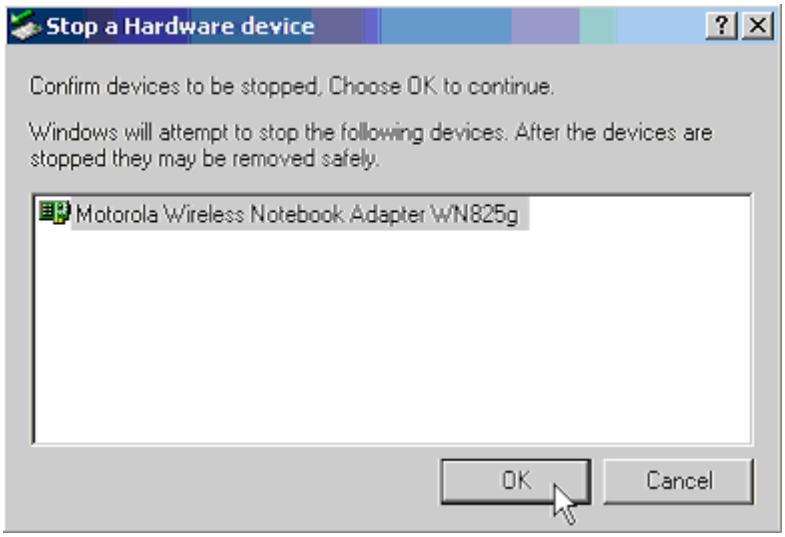


2 Double-click the **Device Eject icon**. The Unplug or Eject Hardware window displays:



3 Highlight the ***device*** you want to remove.

4 Click **Stop**. The Stop a Hardware device window is displayed. An example, illustrating the WN850G, is shown below:



5 Confirm that the device listed in the window is the device you want to stop.

6 Click **OK**. After you receive a message telling you the device is stopped, you can safely remove the Wireless Adapter.

Advanced Configuration of the Wireless Network Adapter

You can configure advanced features from this screen. Primarily you are concerned with the IBSS Channel Number, Location, and Frame Bursting areas.

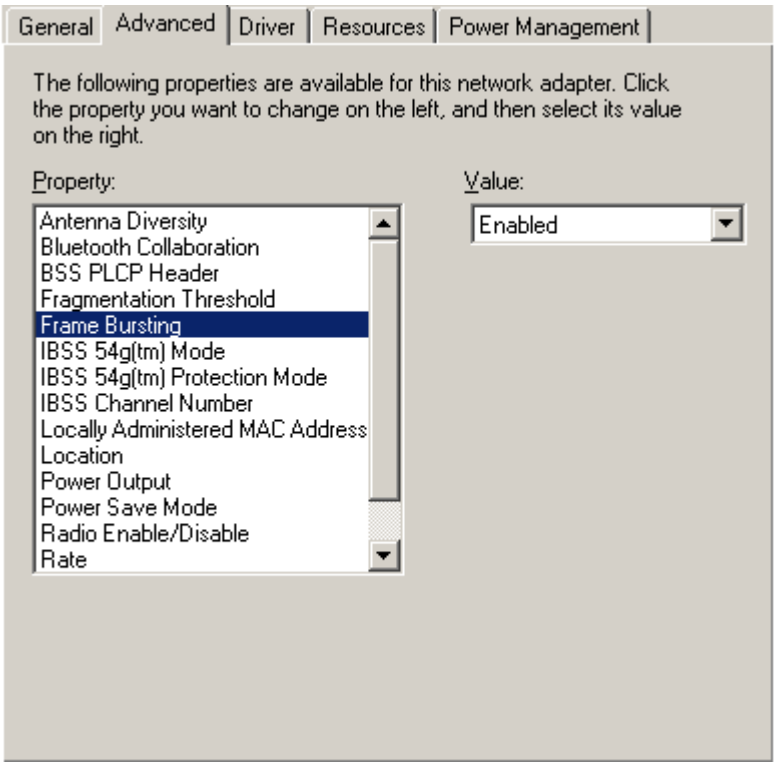
1 Click **Start**, click **Settings**, and then click **Control Panel**.

2 Click **System** and select the **Hardware** tab.

3 Click **Device Manager**.

4 Click **Network adapters**.

5 Click **Motorola Wireless Network Adapter WN825** and select the **Advanced** tab. An example of the Advanced tab is shown below (your screen may differ slightly):



6 To change the value for any of the listed properties, click the ***Property***.

7 Change the ***value*** in the Value box by either clicking the **Value** arrow and selecting a new value, or by typing a new value, as appropriate.

The default values for these properties are set for maximum performance.

Field	Description
IBSS Channel Number	This selects the channel number on which to operate. The WN825 comes preset for use on channels 1-11. These values are legal in most countries. Some countries allow use on more channels. If you travel to one of these countries, you may change the value for IBSS Channel Number to 12, 13, or 14.
Location	Allows you to match the regulatory permissions of the country in which you are using the Adapter. *Match the country in which you are using the adapter.*
Performance Enhancement ***WN825GP Only***	This toggles the feature on or off. The default is enabled. If Performance Enhancement is enabled, it is recommended that Frame Bursting also remain enabled.
Frame Bursting	Select this option if the network uses Frame Bursting. The default is enabled.

8 Click **OK** to save the changes and exit.

Section 4:Troubleshooting

This section details possible solutions to common problems that may occur in using the WN825.

Contact Us

If you are unable to locate a solution here, please access our website at www.motorola.com/broadband/networking for the latest information. You can also reach us 7 days a week, 24 hours a day at 1-877-466-8646.

Hardware Solutions

My computer is experiencing difficulty connecting to the wireless network.

- Ensure that your PC and wireless access point is powered on.
- Ensure that your wireless adapter is installed correctly and is active.
- Ensure that your wireless adapter and access point radio signal is enabled. Review your access point's documentation for further instructions.
- Ensure that your wireless adapter for your PC and the wireless access point have the same security settings that will allow your computer to access the wireless network. Refer to the Configuration section of the documentation that came with your access point.
- Verify that the Access Control List (ACL) is not configured to block your PC. Refer to the Configuration section of the documentation that came with your access point.
- Ensure that your wireless adapter is within range of your access point or is not behind and obstruction; for example, metal structures will interfere with the signal, as will 2.4 GHz cordless phones, and microwaves.
- Ensure that your access point antenna is connected.

I would like to test if my Internet connection is live.

Use the *ping* command to test the connection. Before attempting, determine the IP Address of your adapter.

1 Open a command prompt by clicking **Start** and **Run**.

2 For Windows 98 and ME, in the *Open* field, type **command** and press **Enter** or **OK**.

For Windows 2000 and XP, type **cmd**. Or, navigate using your **Start** button to **Programs**>**Accessories**>**Command Prompt**.

3 In the Command window, type **ipconfig**.

– You should see an IP address for your adapter, for example:

```
Ethernet Adapter Local Area Connection:

Connection-specific DNS Suffix. . : Example.example.example.com.

IP Address. . . . . . . . . . . . : 192.168.10.10

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 192.168.10.1
```

4 If using a router at home, in the Command window, type **ping** followed by the ***Router's IP address*** and press **Enter**. For example, type **ping 192.168.10.1**

The router's IP address is most likely the default gateway.

– If you receive a reply (the first word will be *Reply…*), then your computer is connected to the router. Proceed to Step 4.

– If you do NOT receive a reply, repeat steps 1 – 4 on a different computer to verify that the first computer is not the cause of the problem.

5 In the Command window, type **ping** and your ***ISP's default gateway IP Address*** and press **Enter**. You can determine your ISP's default gateway by examining your modem and or router. Refer to the instructions provided with your modem/router.

– If you receive a reply (For example, *Reply from 216.109.125.72…*), then your connection to the Internet is live.

– If you do NOT receive a reply, repeat steps 1 – 5 on a different computer to verify that the first computer is not the cause of the problem.

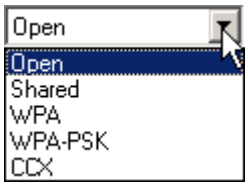
6 If you cannot determine your ISP's default gateway, ping www.yahoo.com or another known web location.

Software Solutions

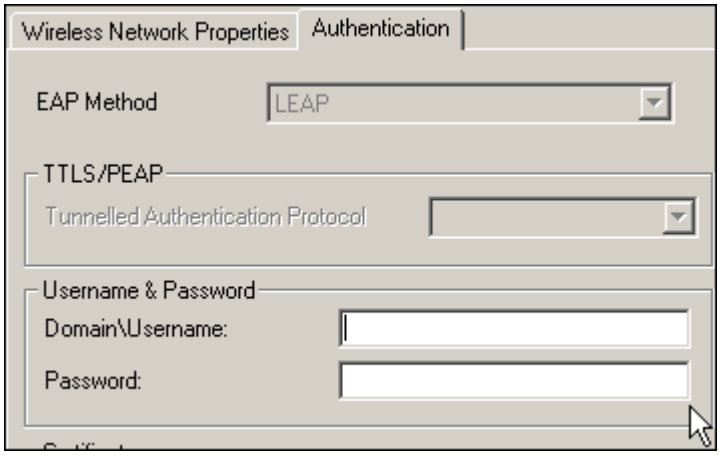
How do I enable LEAP for my corporate network?

Ask you system administrator for the ***Domain/Username*** and ***Password*** required.

1. Right-click the **antenna icon** in the system tray and select **Open Utility**. The Motorola Wireless Configuration Utility window displays.
2. Ensure that the Motorola Wireless Configuration utility is enabled, refer to Section 3 for further details.
3. Add a new network, refer to Section 3 for details.
4. In the Preferred networks area, highlight the ***network*** you want to configure.
5. In the Available networks area click **Configure,** or in the Preferred networks area click **Properties**.
6. Select the type of authentication required, in this case CCX. Match the authentication used by the access point.



7. Click the **Authentication** tab to enter further details.
   - Enter the ***Domain/Username*** and ***Password***.



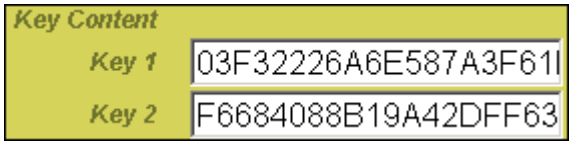
8. Click **OK** twice to save your changes.

I am unable to roam with WDS enabled.

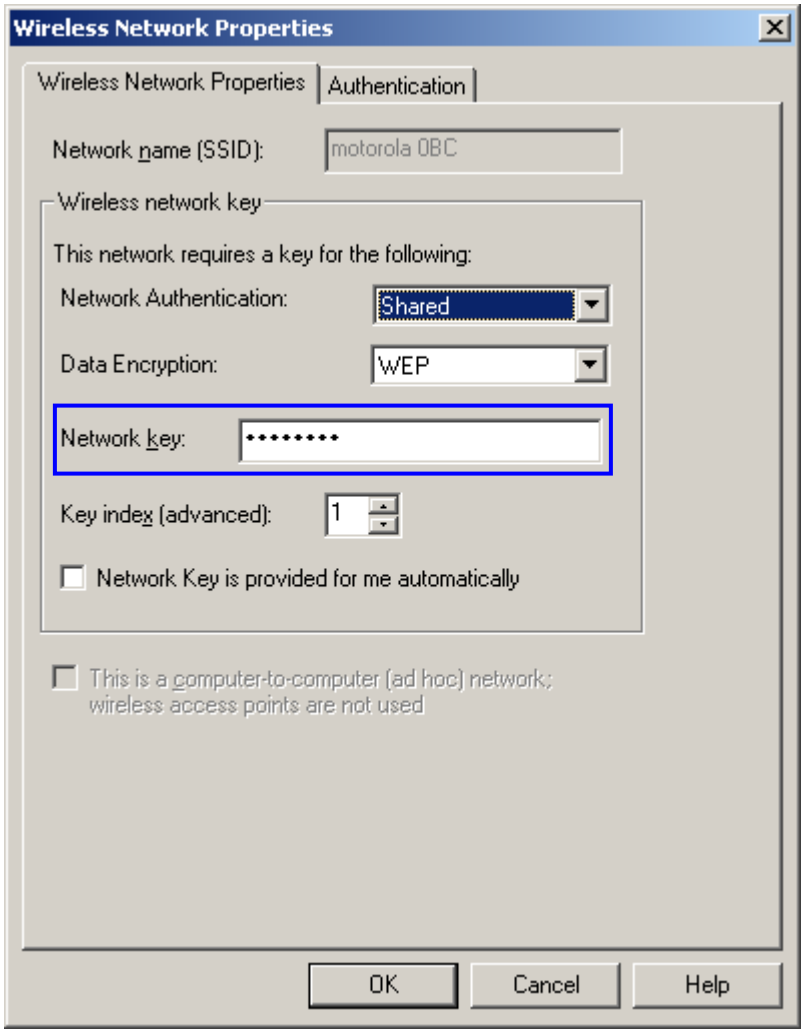
Currently WDS cannot work with WPA enabled. Use WEP for data encryption instead.

What if Pass Phrase isn't supported? What do I enter for my security?

Some wireless cards do not support Pass Phrase or Motorola's Pass Phrase algorithm, which means you have to enter the entire Key Content found in the appropriate Key field.



So, using the WEP example from above if using Key 1, you would enter 03F32226A…etc. into the **Network Key** field of the example Network Adapter, seen below. Ensure that the Key index matches what is selected on the wireless network.



Section 5:Glossary

A

Access Point (AP)

A device that provides wireless LAN connectivity to wireless clients (stations).

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 wireless LAN.

Address translation

See *NAT*.

Ad-Hoc Network

A temporary local area network connecting AP clients together, usually just for the duration of the communication session. The clients communicate directly to each other and not through an established, such as through a router. Also known as: IBSS (Independent Basic Service Set).

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.

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.

bps

Bits Per Second

Broadband

A communications medium that can transmit a relatively large amount of data in a given time period.

BSS

Basic Service Set. A configuration of Access Points that communicate with each other without resorting any infrastructure. Also known as Ad-Hoc networks. Also see *ESS*.

C

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. On an IEEE 802.11b/g wireless LAN, a client is any host that can communicate with the access point. Also called a CPE. A wireless client is also called a “station.” Also see *server.*

Coaxial Cable

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.

CPE

Customer Premise Equipment: typically computers, printers, etc, that are connected to the gateway at the subscriber location. CPE can be provided by the subscriber or the cable service provider. Also called a client.

Crossover Cable

A crossover cable is a cable that is used to interconnect two computers by "crossing over" (reversing) their respective pin contacts. A crossover cable is sometimes known as a null modem.

D

Default Gateway

A routing device that forwards traffic not destined to a station within the local subnet.

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.

DMZ

De**M**ilitarized **Z**one. This service opens one IP address to the Internet, usually for online gaming, and acts as a buffer between the Internet and your network.

DNS

The Domain Name System is the Internet system for converting domain names (like www.motorola.com) 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.

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. See *DNS.*

Download

To copy a file from one computer to another. You can use the Internet to download files from a server to a computer.

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. DSSS is a transmission technology used in WLAN transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission.

Dynamic IP Address

An IP address that is temporarily leased to a host by a DHCP server. The opposite of *Static IP Address*.

E

ESS

An Extended Service Set (ESS) is a set of two or more BSSs that form a single subnetwork. See also *BSS*.

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. Also see *MAC address*.

Event

A message generated by a device to inform an operator or the network management system that something has occurred.

F

Firewall

A security software system on some devices that enforces an access control policy between the Internet and the LAN for protection.

Firmware

Code written onto read-only memory (ROM) or programmable read-only memory (PROM). Once firmware has been written onto the ROM or PROM, it is retained even when the device is turned off. Firmware is upgradeable.

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.

G

Gateway

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

GUI

Graphical User Interface

H

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.

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

I

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.

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. 802.11b and 802.11g are examples of standards they have produced.

Internet

A worldwide collection of interconnected networks using TCP/IP.

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.

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.

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.”

ISDN

Integrated Services Digital Network

ISP

Internet Service Provider

L

LAN

Local Area Network. A local area network provides a full-time, high-bandwidth connection over a limited area such as a home, building, or campus. Ethernet is the most widely used LAN standard.

LEAP

Lightweight Extensible Authentication Protocol (LEAP) is an authentication implementation of 802.1X by Cisco, which provides a challenge-response authentication mechanism and dynamic WEP key assignment.

M

MAC Address

The Media Access Control address is a unique, 48-bit value permanently saved in the ROM at the factory to identify each Ethernet network device. It is expressed as a sequence of 12 hexadecimal digits printed on the unit’s label. You need to provide the MAC Address to the cable service 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.

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*.

N

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 LAN computers are invisible on the Internet.

Network

Two or more computers connected to communicate with each other. Networks have traditionally been connected using some kind of wiring.

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.

P

Packet

The unit of data that is routed between the sender and destination on the Internet or other packet-switched network.

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 or wireless connectivity.

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.”

Port Triggering

A mechanism that allows incoming communication with specified 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.

PPPoE

Point-to-Point Protocol over Ethernet. Used by many DSL Internet Service Providers for broadband connection.

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 LAN by the DHCP server for a specified lease time. Private IP addresses 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.

Public IP Address

The IP address assigned by the service provider. A public IP address is visible to devices on the Internet. See also *Private IP Address*.

R

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.

Roaming

The ability to transfer your wireless session from one AP to another AP seamlessly.

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.

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. Also see *client.*

Service Provider

A company providing Internet connection services to subscribers.

SMTP

Simple Mail Transfer Protocol is a standard Internet protocol for transferring e-mail.

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*.

Station

IEEE 802.11b term for wireless client.

Subscriber

A user who accesses television, data, or other services from a service provider.

Subnet Mask

A methodology that determines what the router will examine for the destination of an IP address. A router delivers packets using the network address.

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.

T

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.

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

U

UDP

User Datagram Protocol. A method used along with the IP to send data in the form of message units (datagram) between network devices over a LAN or WAN.

Unicast

A point-to-point data transmission sent from one sender to one receiver. This the normal way you access websites. See also *multicast*.

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.

V

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 (Public Switched Telephone Network) 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.

W

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*.

WEP

Wired Equivalent Privacy encryption protects the privacy of data transmitted over a wireless LAN. 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.

Wi-Fi®

Wireless fidelity (pronounced why'-fy) brand name applied to products supporting IEEE 802.11b/g.

WLAN

Wireless LAN.

WPA

Wi-Fi Protected Access. A security regimen developed by IEEE for protection of data on a WLAN.

WWW

World Wide Web. An interface to the Internet that you use to navigate and hyperlink to information.

Visit our website at:
www.motorola.com/broadband

516591-001
7/04

MGBI