User Guide

Wireless Access Point
WA840G

MOTOROLA
intelligence everywhere™

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

CAUTION: TO ENSURE REGULATORY COMPLIANCE, USE ONLY THE PROVIDED POWER AND INTERFACE CABLES.

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

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.

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

Do not overload outlets or extension cords, as this can result in a risk of fire or electric shock. Overloaded AC outlets, extension cords, frayed power cords, damaged or cracked wire insulation, and broken plugs are dangerous. They may result in a shock or fire hazard.

Route power supply cords so that they are not likely to be walked on or pinched by items placed upon or against them. Pay particular attention to cords where they are attached to plugs and convenience receptacles, and examine the point where they exit from the product.

Place this equipment in a location that is close enough to an electrical outlet to accommodate the length of the power cord.

Place this equipment on a stable surface.

When using this device, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

- Read all of the instructions {listed here and/or in the user manual} before you operate this equipment. Give particular attention to all safety precautions. Retain the instructions for future reference.
- Comply with all warning and caution statements in the instructions. Observe all warning and caution symbols that are affixed to this equipment.
- Comply with all instructions that accompany this equipment.
- Avoid using this product during an electrical storm. There may be a risk of electric shock from lightning. For added protection for this product during a lightning storm, or when it is left unattended and unused for long periods of time, unplug it from the wall outlet, and disconnect the cable system. This will prevent damage to the product due to lightning and power surges.
- Operate this product only from the type of power source indicated on the product's marking label. If you are not sure of the type of power supplied to your home, consult your dealer or local power company.
- Upon completion of any service or repairs to this product, ask the service technician to perform safety checks to determine that the product is in safe operating condition.

It is recommended that the customer install an AC surge protector in the AC outlet to which this device is connected. This is to avoid damaging the equipment by local lightning strikes and other electrical surges.

Different types of cord sets may be used for connections to the main supply circuit. Use only a main line cord that complies with all applicable product safety requirements of the country of use.

Installation of this product must be in accordance with national wiring codes.

Place unit to allow for easy access when disconnecting the power cord/adapter of the device from the AC wall outlet.

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

This product was qualified under test conditions that included the use of the supplied cables between system components. To be in compliance with regulations, the user must use these cables and install them properly. Connect the unit to a grounding type AC wall outlet using the power adapter supplied with the unit.

Do not cover the device, or block the airflow to the device with any other objects. Keep the device away from excessive heat and humidity and keep the device free from vibration and dust.

Installation must at all times conform to local regulations.

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.

MOTOROLA INC. declares that WA840Gv2 (FCC ID: ACQWA840GV2) is limited in CH1~CH11 by specified firmware controlled in U.S.A.

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 WR850G, WE800G, WA840G, WN825G, WPCI810G, and BR700 compile 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 Information

The WR850G, WE800G, WA840G, WN825G, and WPCI810G Wireless LAN products are wireless network products that uses Direct Sequence Spread Spectrum (DSSS) radio technology. This product is designed to be inter-operable with any other wireless DSSS type product that complies with:

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

Wireless LAN and your Health

The WR850G, WE800G, WA840G, WN825G, and WPCI810G, like other radio devices, emits radio frequency electromagnetic energy, but operates within the guidelines found in radio frequency safety standards and recommendations.

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 WR850G, WE800G, WA840G, WN825G, and WPCI810G contains a radio transmitter and accordingly has been certified as compliant with 47 CFR Part 15 of the FCC Rules for intentional radiators. Products that contain a radio transmitter are labeled with FCC ID and the FCC logo.

Caution: Exposure to Radio Frequency Radiation. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

Canada - Industry Canada (IC)

The wireless radio of this device complies with RSS 210 ans 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

Copyright © 2003 by Motorola, Inc.

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

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

MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. Microsoft Windows screen shots are used by permission of Microsoft Corporation. All other product or service names are the property of their respective owners. © Motorola, Inc. 2003

Contents

Section 1:Overview 1-1

Features **1-2**
Understanding Your User Guide **1-3**
Box Contents **1-4**
Wireless Connections **1-4**
Access Point 1-4
TCP/IP 1-4
Static IP Address *1-5*
Dynamic IP Address *1-5*
Understanding Wireless *1-5*
Wireless Range 1-6
Recommended Wireless Environment 1-6
Type of Networks **1-7**
Access Point Mode 1-7
WDS Access Point Mode 1-7
Access Point Physical Description **1-8**
Back of Access Point 1-8
Front of Access Point 1-9
LED Description 1-10

Section 2:Installation 2-1

Hardware Setup **2-1**
Antenna Installation 2-1
Access Point Physical Installation 2-2
Horizontal Installation *2-2*
Vertical Installation *2-3*
Wall Mount Installation *2-3*
Electrical Connection to Access Point 2-6
Easy Software Setup **2-6**
Manual Software Setup **2-6**
Wired Connection to Access Point 2-7
Wireless Connection to Access Point 2-8
Configure Your Computers **2-9**
Configuring Windows 98SE and ME 2-10
Configuring Windows 2000 2-12
Configuring Windows XP 2-15
Configure Your Wireless Security Settings **2-19**
Logging In 2-19
Wireless Security Setup 2-20

Section 3:Configuration 3-1

Using the Web-Based Configuration Utility 3-1
Logging In 3-1
Navigation 3-2
Help, Restart, and Logout 3-2
Configuring Wireless Network Settings 3-3
Wireless - Basic 3-3
Wireless - Security 3-5
Wireless - Site Monitor 3-11
Wireless - Advanced 3-13
Configuring Control Panel Settings.....3-16
Control Panel - Network Access.....3-16
Control Panel - Device Security 3-18
Control Panel - Firmware Update.....3-18
Control Panel - Configuration Data 3-19

Section 4:Troubleshooting 4-1

Contact.....4-1
Hardware Solutions.....4-1
My computer is experiencing difficulty in connecting to the AP.....4-2
Software Solutions.....4-3
I would like to see if my Internet connection is alive.....4-3
I cannot access the Web-Based Configuration Utility for the AP.....4-4

Section 5:Glossary 5-1

Section 1:Overview

Congratulations on purchasing the Motorola Wireless Access Point WA840G. With this unit, you have entered the world of freedom and independence – freedom from wires and the independence to communicate wherever YOU choose.

Because the Access Point (AP) is built with both the popular 802.11b wireless standard and the new nearly 5-times-faster 802.11g standard, your unit provides you the ultimate in flexibility and speed. With Wi-Fi® Protected Access (WPA) included, your wireless connections are robust and secure, giving you the security to communicate without fear that your signal might be compromised.

Upgradeable firmware keeps the AP's control software up-to-date. The WA840G captures the latest technology in a package that will stay current for many years, protect your home network, and provide you easy home network management.

Wireless Access Point WA840G

Your wireless access point offers these great features:

Wireless Connectivity

Connects your PC to your wireless network and allows you to communicate unfettered. Using the 802.11g and 802.11b wireless standards will ensure compliance with the now and the future.

Secure Transmission

Protection against Internet intruders is crucial. Of course the product supports single session encryption when communicating with just the client, but it also supports network encryption, when communicating with larger surrounding wireless networks.

Supports Wi-Fi Protected Access (WPA) and Media Access Control (MAC) filtering protocols, giving you the choice to share your Internet connection with only those whom you designate.

Your Motorola Wireless Access Point WA840G connects and protects you. Built-in security coupled with upgradeable firmware ensures your Access Point will work for you for years to come.

Features

- CD-ROM based Installation Assistant for easy installation
- Web-based configuration of features using any web browser
- Compatibility with both 802.11g and 802.11b standards
- Wireless security using WPA, 802.1X Authentication, and Advanced Encryption Standard (AES)
- Wireless Distribution System (WDS) mode supporting peer-to-peer communication with other WA840G or WR850G units
- Firmware upgrade to stay current with latest specification
- Easily extend your home network, in the office, or even at tradeshows

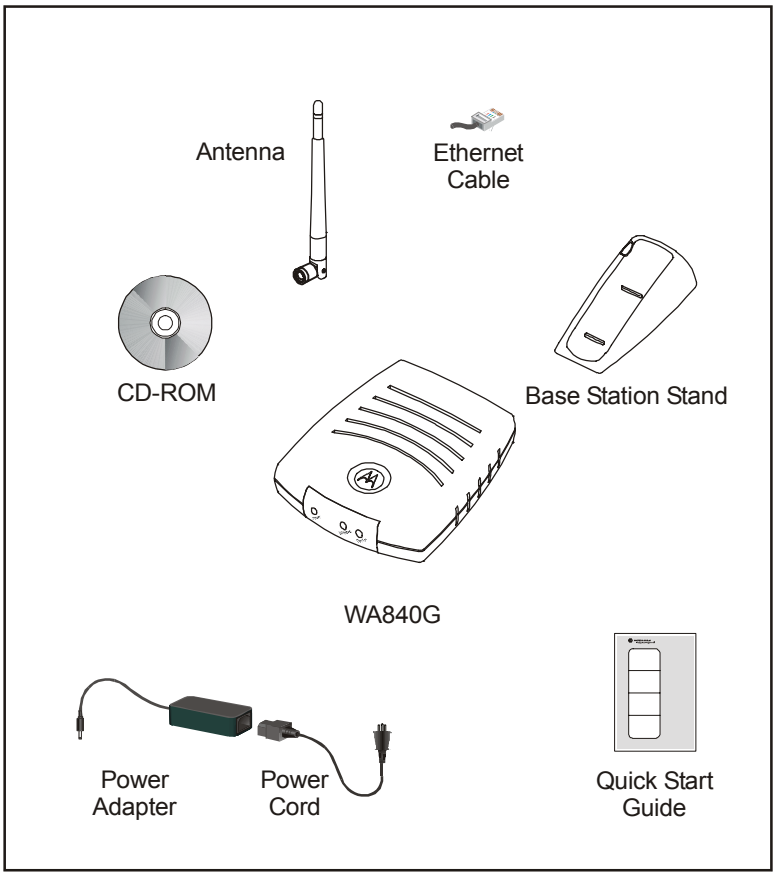
Understanding Your User Guide

The User Guide is subdivided into the following sections:

Overview	Provides a general introduction for using your product, the type of technology used, and recommended practices for using it.
Installation	It is assumed that you will use the Installation Assistant on the CD-ROM to setup your unit. If not, then refer to this section for details on getting your unit up and running. Once you have completed this section, your unit will be active and ready to work.
Configuration	Provides descriptive details for using the Configuration Utility to manage your unit.
Glossary	Defines the terms and acronyms.

Box Contents

Your box contains the following:



Wireless Connections

The various technologies and features utilized by your wireless access point require some conceptual explanation so that you can make the correct choices in configuring your wireless access point.

Access Point

Access Points (AP) wirelessly connect networks together, such as your network with the Internet (which can be thought of as a very large network). Or, by configuring multiple clients such as laptops, each using their own AP, you are able to create your own private wireless Ad-Hoc network.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) comprises the backbone of the Internet. IP moves packets of data between nodes while TCP verifies delivery from client to server. The device

you hook up to your wireless access point will identify itself with an IP address so that the network will know where to retrieve and deposit requested information.

Static IP Address

A static IP address is a fixed address that is assigned manually to a device on the network. Static IP addresses must be unique and cannot be shared, therefore they are used in situations where the address should never change, like print servers or PC servers.

Dynamic IP Address

A dynamic IP address is a temporary IP number, dynamically or randomly generated by a DHCP server. The address lasts only as long as the server allots, usually in the space of a day or two. When the IP address expires, the client is automatically reassigned a new IP address, ensuring smooth communication.

Understanding Wireless

Your wireless AP uses a radio transmission technology defined by the Institute of Electrical and Electronics Engineers (IEEE) called 802.11 or Wi-Fi (Wireless Fidelity). 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 AP supports both the ‘b’ and ‘g’ specifications. The 802.11b specification transmits data rates up to 11 Mbps while the 802.11g specifications transmits data rates up to 54 Mbps. These are theoretical speeds so your performance may vary. The radio waves radiate out in a donut-shaped pattern. The waves travel through walls and floors, but transmission power and distance are affected. The theoretical distance limit is 1,000 feet (305 meters), but actual throughput and distance varies.

Both standards operate in the 2.4 GHz range, meaning other electrical appliance also might interfere with the AP – televisions, radios, microwave ovens, and 2.4 GHz cordless telephones. Thus positioning your AP where it encounters the least interference gains the greatest benefit to maintaining a quality connection.

Wireless Range

The following describes different scenarios for the expected range of the coverage area of the unit. This table is only a guide and coverage varies due to local conditions.

Data Rate	Open Area	Closed Area
54 Mbps	Up to 100 ft (30m)	Up to 60 ft (18m)
11 Mbps	Up to 900 feet (275 m)	Up to 160 feet (49 m)
5.5 Mbps	Up to 1300 feet (396 m)	Up to 200 feet (61 m)
2 or 1 Mbps	Up to 1500 feet (457 m)	Up to 300 feet (91 m)

Recommended Wireless Environment

The following information helps you to achieve the best wireless performance:

- Placing your base station in the physical center of your network is the premium location because the antenna radiates out the signal in all directions.
- Placing the unit in a higher location, such as atop a cabinet, helps to disperse the signal cleanly, especially to receiving locations on upper stories.
- Direct line of sight achieves better performance, but obviously is not always achievable.
- Try to avoid placing the unit next to large solid objects like computer cases, monitors, walls, fireplaces, etc. This helps the signal penetrate more cleanly.
- Other wireless devices like televisions, radios, microwaves and 2.4 GHz cordless telephones can interfere with the signal. Keep devices away from the unit.
- Mirrors, especially silver-coated, negatively affect transmission performance.

Type of Networks

Your AP supports several different usage scenarios and the following examples illustrate the flexibility of your WA840G. Some scenarios require additional hardware that can be purchased.

Access Point Mode

In this mode, the WA840G connects wireless clients to a wired Ethernet network. This is the most likely scenario you will use, as it shares an Internet connection with your laptop or other wireless client.

WDS Access Point Mode

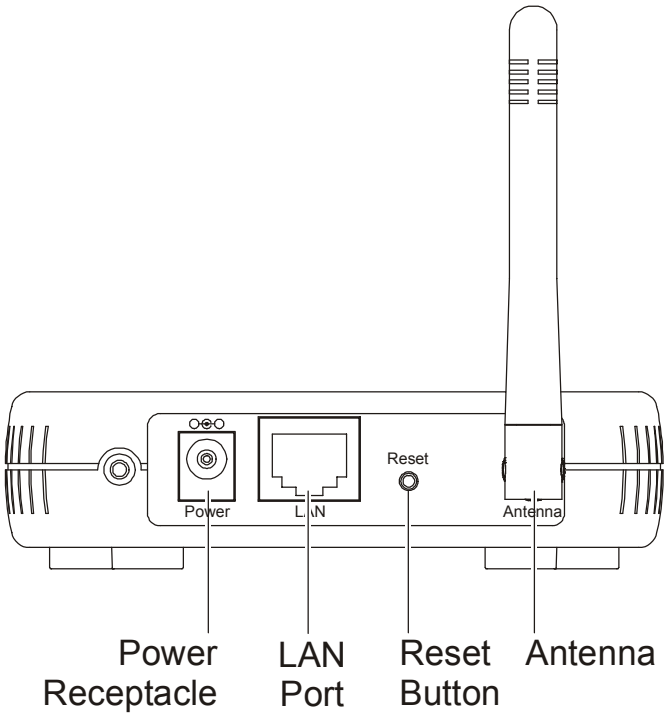
In this mode, the WA840G connects its wireless clients to other Access Points wirelessly.

Access Point Physical Description

The following sections describe the physical characteristics of the unit.

Back of Access Point

The following illustration shows the WA840G back panel:

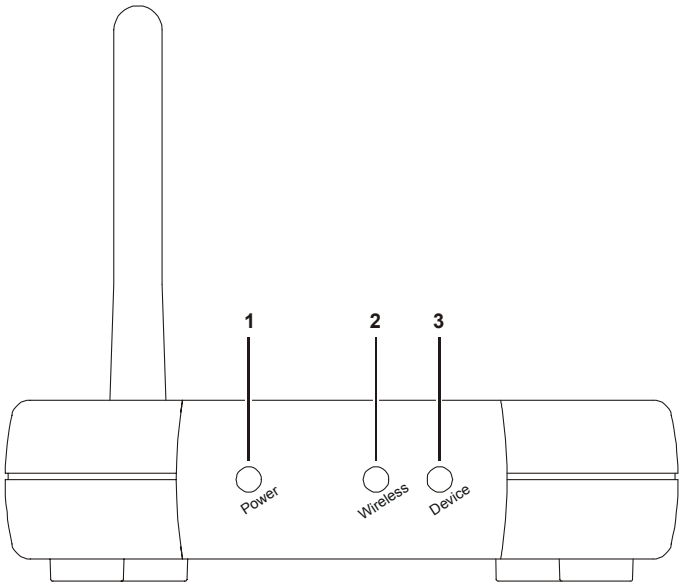


Feature	Description
Power	The power adapter receptacle.
LAN Port	This port connects to the Internet, your LAN network, or PC with an Ethernet cable. This enables communication between the devices. The LAN port supports either 10BASE-T or 100BASE-T transmission speeds as well as straight-through and Crossover Ethernet cables.

Feature	Description
Reset Button	A dual-function button. It either resets your unit or resets the unit to the default login settings. If the AP is experiencing trouble connecting to the Internet, briefly press and release the Reset button to reset the AP. This retains its configuration information. To reset the unit to the factory defaults, while the unit is powered, press and hold the Reset button for more than 5 seconds. This clears the AP's user settings, including User ID, Password, IP Address, and Subnet Mask. Refer to the *Configuration* section for re-configuring the AP.
Antenna	The antenna used for wireless connections. You are able to rotate and tilt the antenna to gain the best signal reception.

Front of Access Point

The following illustration shows the front of the unit.



The LEDs of the access point indicate operational information of its status.

LED Description

The underlined items represent network activity.

	LED	Condition	Color	Status
1	Power	ON	**Green**	The device is powered on and operating normally.
		Blinking	**Green**	Firmware update is in progress.
		Blinking/ON	**Red**	The power LED turns RED as soon as the reset button is depressed. If the reset button is held down for more than 5 seconds, the LED starts to blink during which the access point's default user name, password and IP address will be restored. The LED then turns OFF until the reset button is released. The power LED keeps blinking RED if the firmware is corrupted indicating the firmware needs to be restored.
2	Wireless	OFF	**None**	No mobile station or AP has associated with this device.
		ON	**Red**	The wireless interface has been disabled by the firmware.
		ON/Blinking	**Green**	802.11b/802.11g connection exists in this wireless domain/active traffic present.
3	Device	OFF	**None**	No external Ethernet device has been attached and detected. The Ethernet link is down.
		ON/Blinking	**Amber**	10BaseT link detected/active traffic present.
		ON/Blinking	**Green**	100BaseT link detected/active traffic present.

Section 2:Installation

To get your network up and running:

- Setup your hardware.
- Insert the CD-ROM for Software Setup. Follow the prompts.

If you prefer to setup the Access Point's (AP) software manually, refer to the Manual Software Setup found in this section.

The following sections provide detailed instructions for completing these tasks.

Hardware Setup

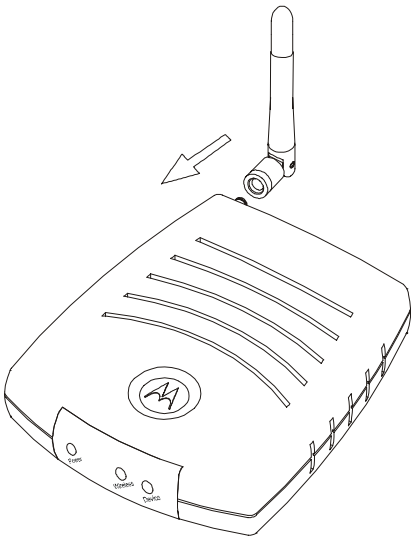
Hardware setup includes:

- Antenna Installation: verifying the antenna is connected to the unit.
- Physical Installation: where you physically place your unit.
- Electrical Connection: how to power your unit.

Antenna Installation

When shipped, the antenna is already installed on the main unit. If you have to detach and reattach the antenna to the main unit:

1. Take the bottom of the antenna and locate, on the right backside of the AP, the threaded knob.
2. Screw the antenna connector clockwise on to the threaded knob until firmly seated. Do not overtighten.



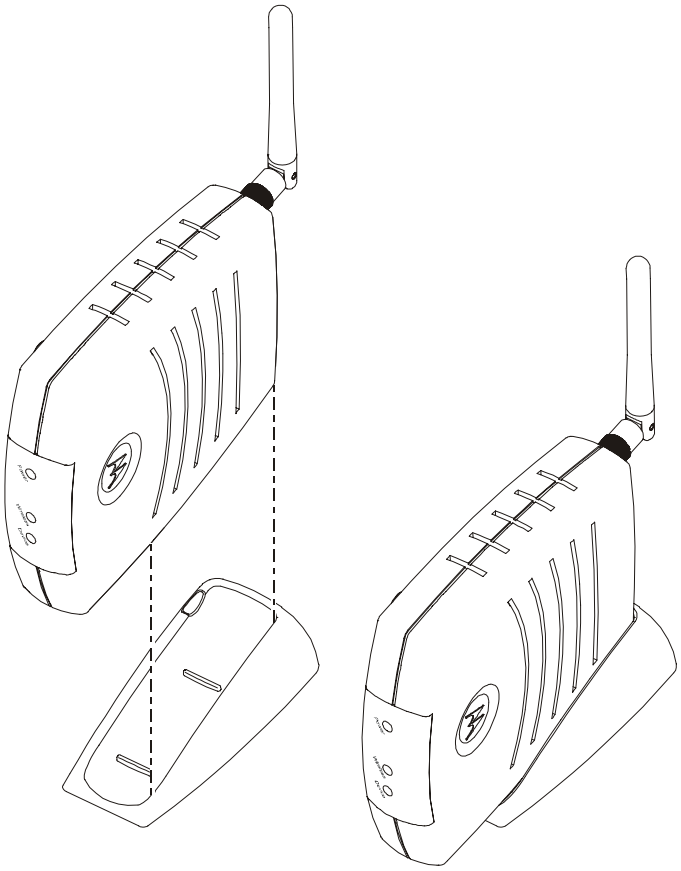
Access Point Physical Installation

You can install the AP in various different physical orientations – horizontally, vertically, or hung on the wall. Your own needs determine the best placement.

Horizontal Installation

1 Place the AP in the desired location and follow the procedures below for connecting and configuring the unit.

Vertical Installation



1. To use the AP in a vertical position, insert it into the supplied base. Ensure that the antenna's location is on top, as it does not allow the unit to nestle into the base. The AP's foot slides snugly into the base to keep the unit stable.
2. Follow the installation procedures for connecting and configuring the unit.

Wall Mount Installation

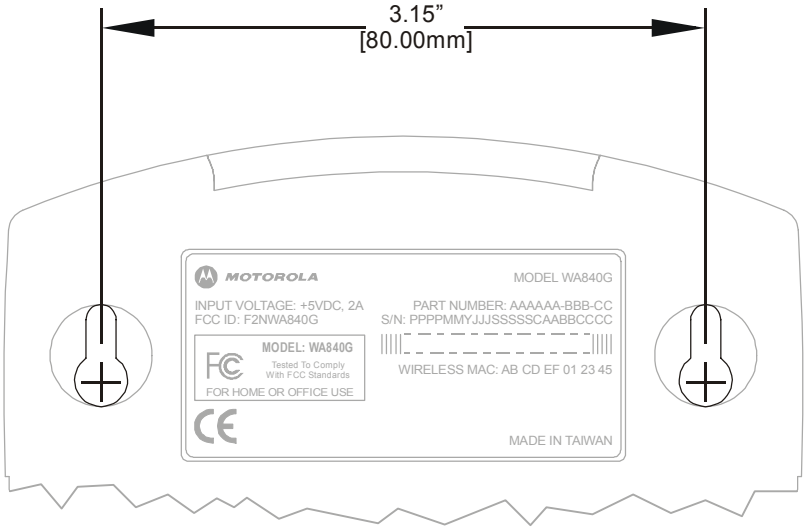
If you mount the AP on the wall, you must:

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

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

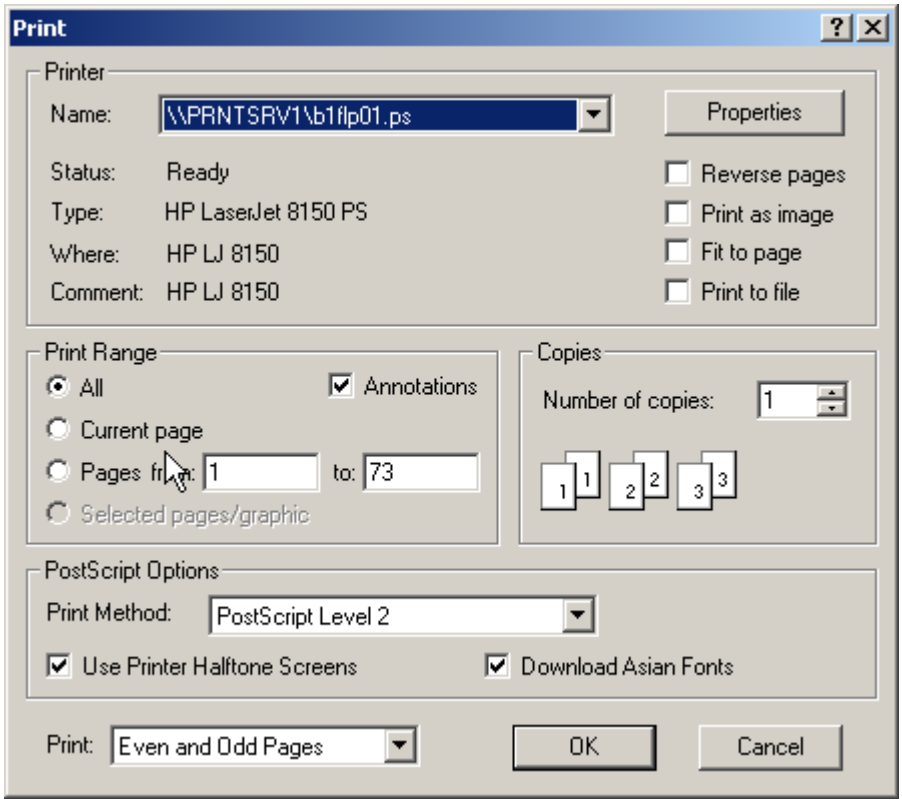
To mount your AP on the wall:

1 Print the Wall Mounting Template.



The illustration is drawn at a one-to-one scale, which means that when printed, it provides the exact dimensions required to mount the unit.

2 Click the **Print** icon or choose Print from the File menu to display the Print dialog box. (A sample print dialog follows.)



Be sure you print the template at 100% scale and that Fit to page is not checked in the Print dialog box.

3 Click **OK** to print the template.

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

5 Use a center punch to mark the center of the holes on the wall.

6 On the wall, locate the marks for the mounting holes you just made.

WARNING!

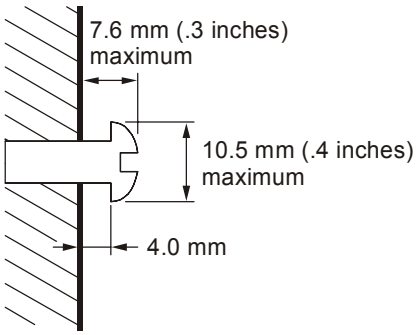
Before drilling holes, check the structure for potential damage to water, gas, or electric lines.

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

8 If necessary, seat an anchor in each hole. Use M5 x 38 mm (#10-16 x 1½ inch) screws with a flat underside and maximum screw head diameter of 10.5 mm to mount the unit.

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

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



10 Remove the front two plastic feet, nearest to the LED panel, from the bottom of the unit to uncover the keyholes.

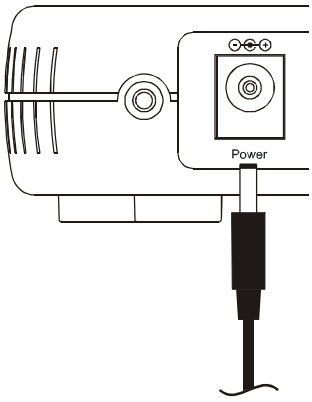
11 Place the unit so the keyholes are above the mounting screws.

12 Slide the AP down until it stops against the top of the keyhole opening.

13 Follow the installation procedures for connecting and configuring the unit.

Electrical Connection to Access Point

Your AP does not have an On/Off power switch and therefore will only be powered on by plugging in the power adapter. Use only the original power adapter supplied with your unit.



To power supply

1. Connect the power adapter to the AP's Power port, found on the back of the unit.
2. Then plug the power adapter into a grounded and surge protected power outlet.
   - The Power LED on the front panel lights green when connected properly.

Easy Software Setup

Run the Installation Wizard program from the supplied CD-ROM to quickly setup your network. Once your network is up and running, refer to *Section 3:Configuration* for advanced configuration.

Manual Software Setup

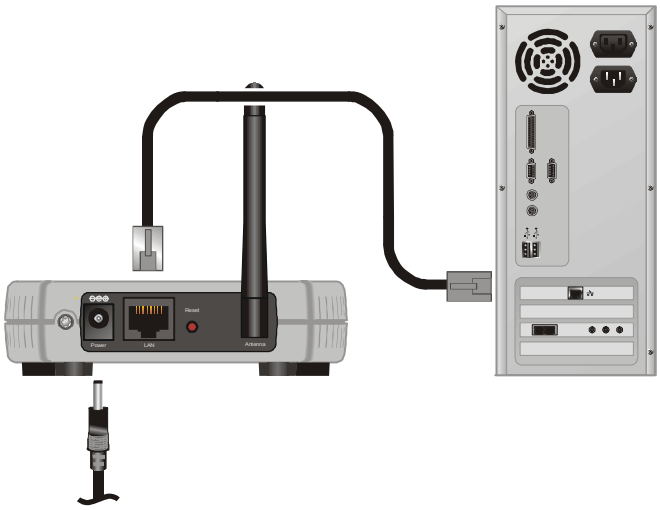
If you'd prefer to manually setup your network, use this section to configure it. This section details the physical connection of the AP to your network as well as the configuration needed by your PC.

To set up your wireless network:

- Physically connect and power on the Access Point
- Configure your PCs
- Enter Wireless Security settings

If you don't want to use the Installation Wizard from the CD-ROM, follow the instructions below. For advanced configurations, refer to *Section 3:Configuration*.

Wired Connection to Access Point



This section applies if you are connecting your PC with an Ethernet cable to the Access Point. Your PC must be installed first with an Ethernet adapter.

You need one Ethernet cable for this procedure, to connect the PC to the Access Point.

1. Using the supplied Ethernet cable, connect one end of the cable to your PC's Ethernet adapter and the other end to the LAN port on the Access Point. You are now able to configure the Access Point.
2. To configure the initial settings of the Access Point, please see Configure your Computers.

Wireless Connection to Access Point

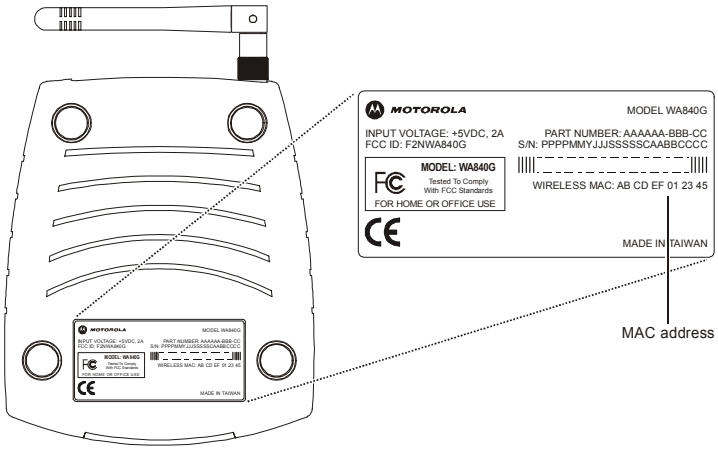
WARNING!

Initial configuration of the Access Point with a wireless connection is NOT secure and is not recommended by Motorola. If at all possible, for an initial configuration, use an Ethernet cable to connect to the AP.

If you are connecting your client (most likely a PC) wirelessly to the AP, you can use the Motorola WPCI810G, a wireless PCI card for your desktop PC. If you have a laptop, the Motorola WN825G wireless PC card provides access.

The WN825G and WPCI810G are not supported under Windows 95, 98, nor NT. Windows 98SE, ME, 2000, and XP are supported.

1. To connect the PC to the AP through a wireless connection, ensure the PC's wireless adapter SSID (Service Set Identifier) is set to the AP's default setting of **motorola** appended with the last 3 characters of the Wireless MAC address (an example SSID: **motorola 345**) and that no encryption is enabled.



2 To configure the initial settings of the AP, please see Configure your Computers.

Configure Your Computers

For initial configuration, you need to initially configure the PC's network setting to specify a static IP address for the computer that is going to "talk" to the Ethernet Bridge.

After initial configuration:

If using DHCP	Reconfigure the PC's settings to ***Obtain An IP Address Automatically***.
If not using DHCP	Continue to use the Static IP settings.

This section includes information on configuring computers with the following operating systems:

- Windows 98SE
- Windows ME
- Windows 2000
- Windows XP

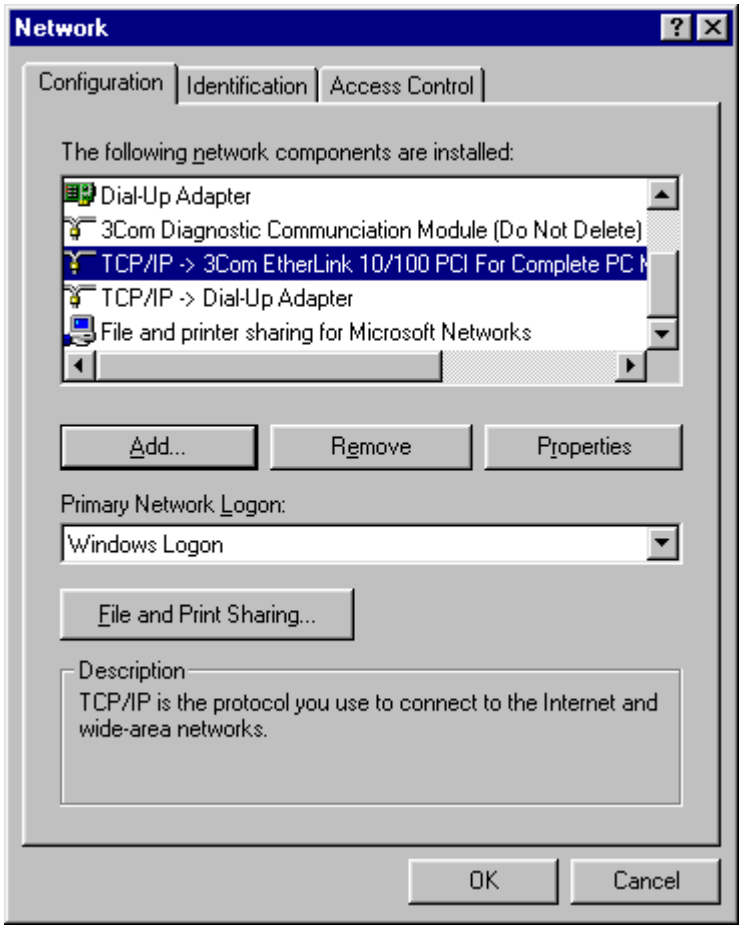
Determine the operating system for each computer you are including in your wireless network and follow the steps to configure the network settings for that PC.

Configuring Windows 98SE and ME

1 Click **Start**.

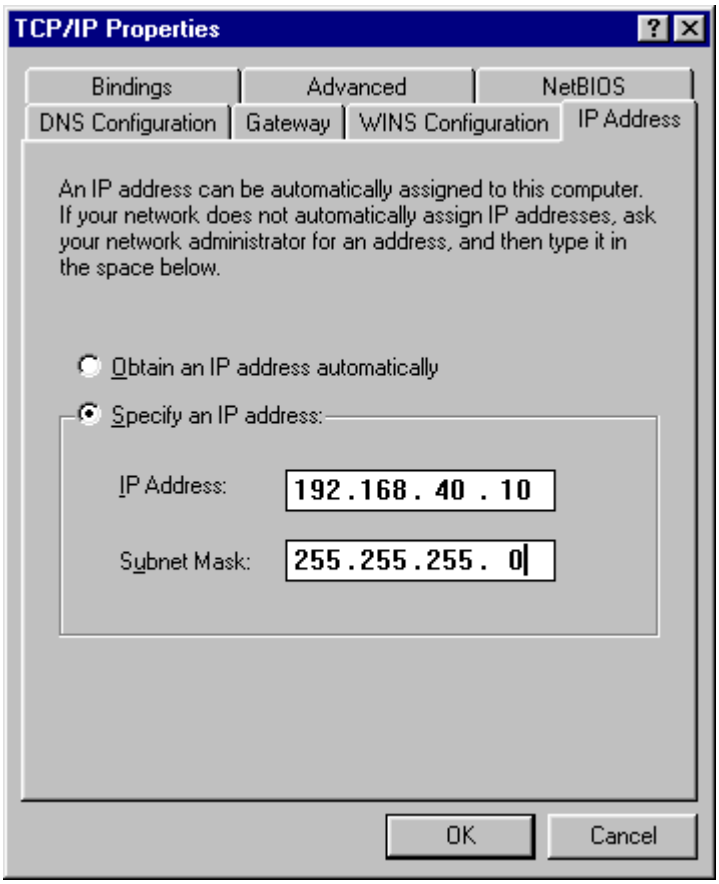
2 Select Settings > Control Panel.

3 Double-click **Network**. The Network window is displayed:



4 On the configuration tab, select the ***TCP/IP*** line the for the appropriate Ethernet adapter. There might be multiple adapters installed – choose only the one that is configured for your adapter. In the example above, a 3Com Ethernet adapter card is installed and is the appropriate choice for this example.

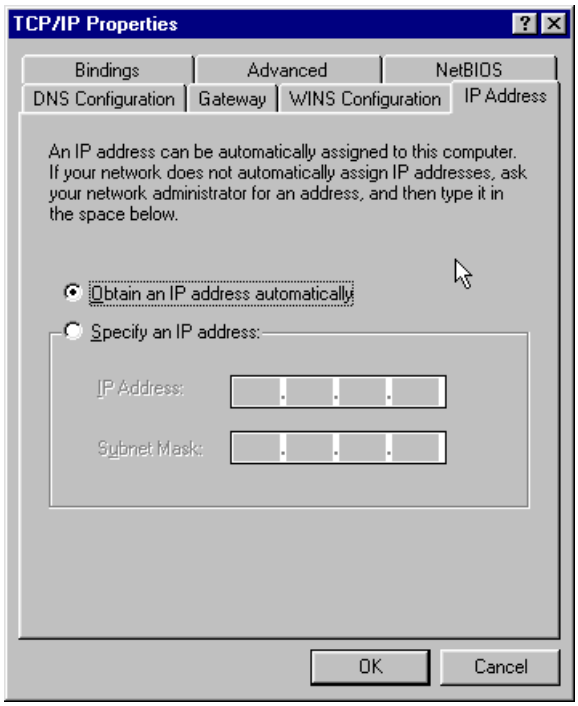
5 Click **Properties**. The TCP/IP Properties window is displayed:



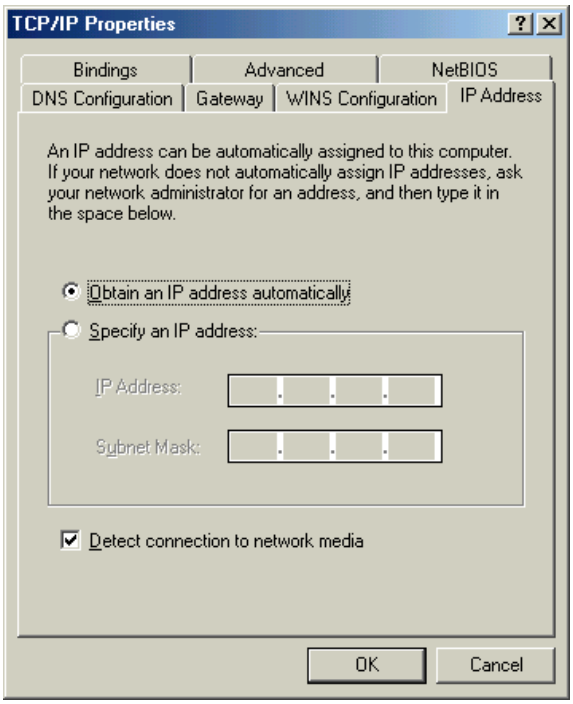
6 Click the **IP address** tab.

7 Enter **192.168.40.1** into the IP Address field.

8 Enter **255.255.255.0** into the Subnet Mask field.



Windows 98SE



Windows ME

9 (If using a DHCP after initial configuration, select ***Obtain An IP Address Automatically***.)

10 Click **OK**.

11 Click the **Gateway** tab and check to make sure that the *Installed Gateway* field is blank.

12 Click **OK** twice. Windows might ask for the Windows installation disk. First check to see if the installation files are installed at c:\windows\options\cabs. Otherwise, install your Windows CD and follow the prompts.

13 Restart your computer to save your settings.

14 Proceed to the *Configure Your Wireless Settings* section to set up the security settings.

Configuring Windows 2000

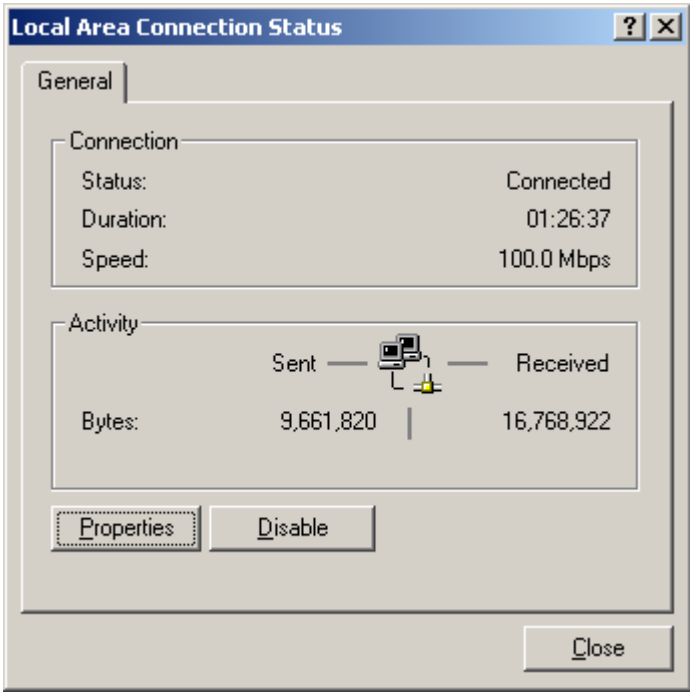
1 Click **Start**.

2 Select **Settings**.

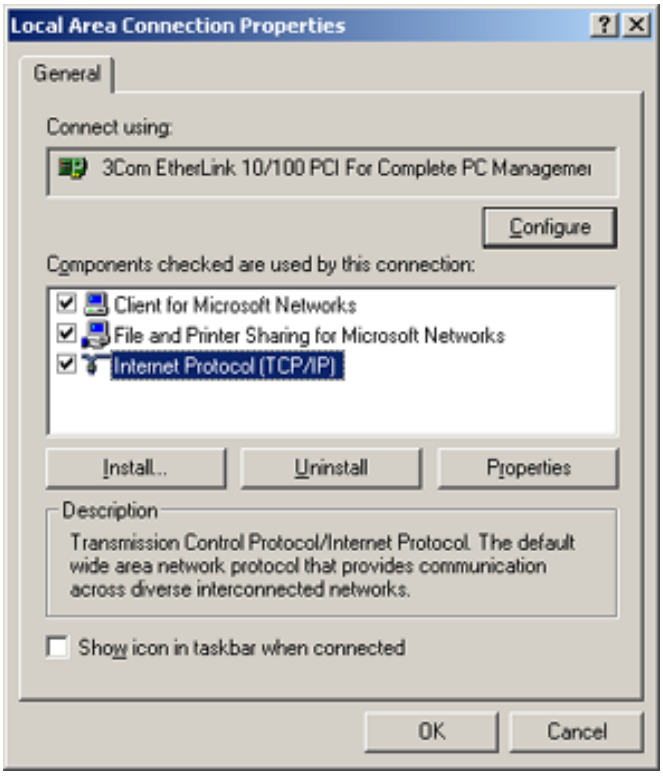
3 Select **Control Panel**.

4 Double-click **Network and Dial-Up Connections**.

5 Double-click **Local Area Connection**.

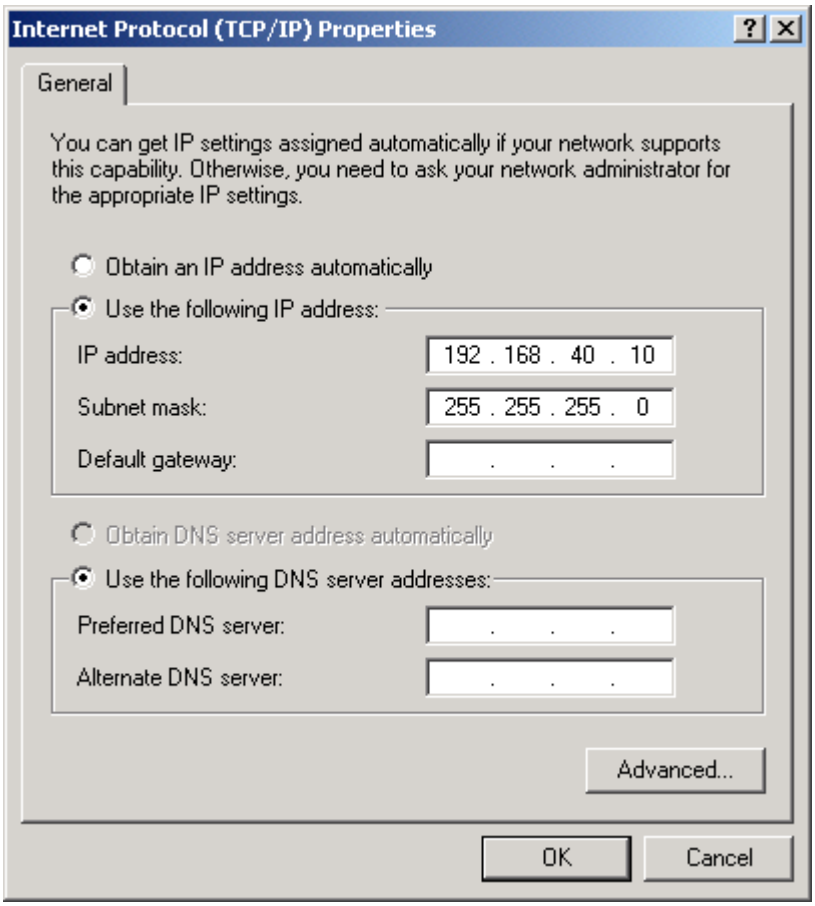


6 Click the **Properties** button.



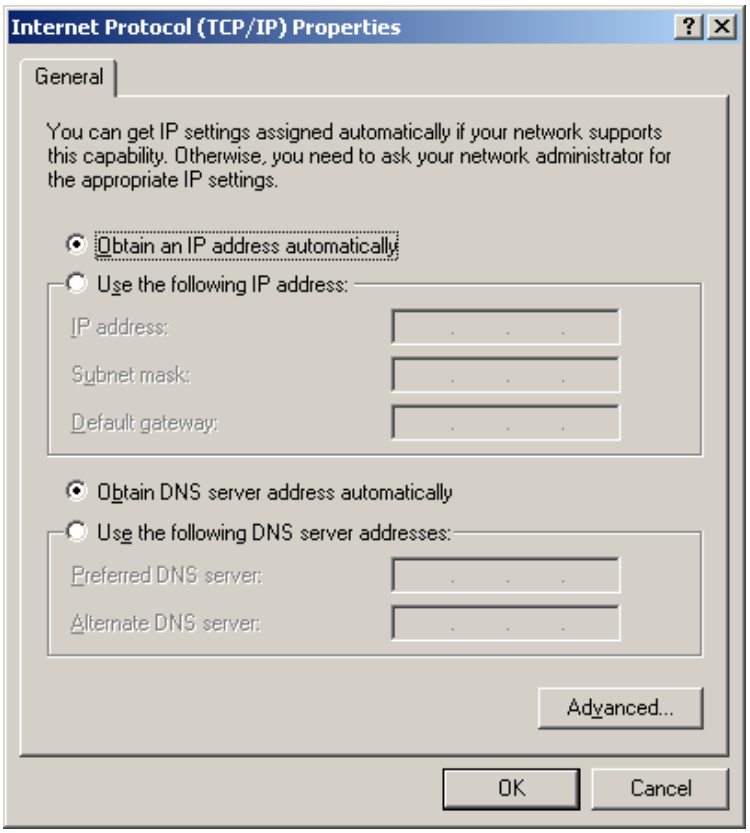
7 Ensure the box next to ***Internet Protocol (TCP/IP)*** is selected.

8 Click to highlight **Internet Protocol (TCP/IP)** and click the **Properties** button.



9 Enter **192.168.40.10** into the IP Address field.

10 Enter **255.255.255.0** into the Subnet Mask field.



11 (If using a DHCP after initial configuration, select ***Obtain An IP Address Automatically***.)

12 Click **OK** twice to exit and save your settings.

13 Restart your computer to save your settings.

14 Proceed to the *Configure Your Wireless Settings* section to set up the security settings.

Configuring Windows XP

This configuration assumes you have retained the default interface for Windows XP. If you are running the 'Classic' interface, please follow the instructions for Windows 2000.

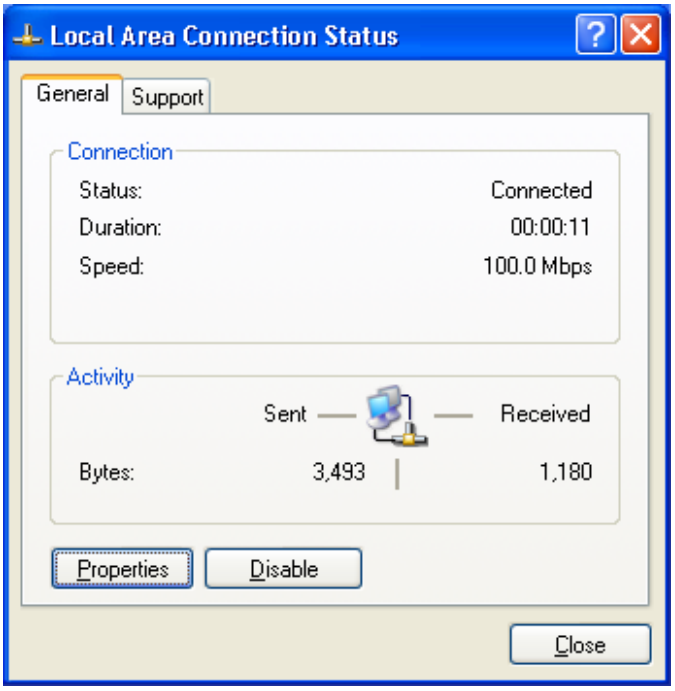
1 Click **Start**.

2 Select **Settings**.

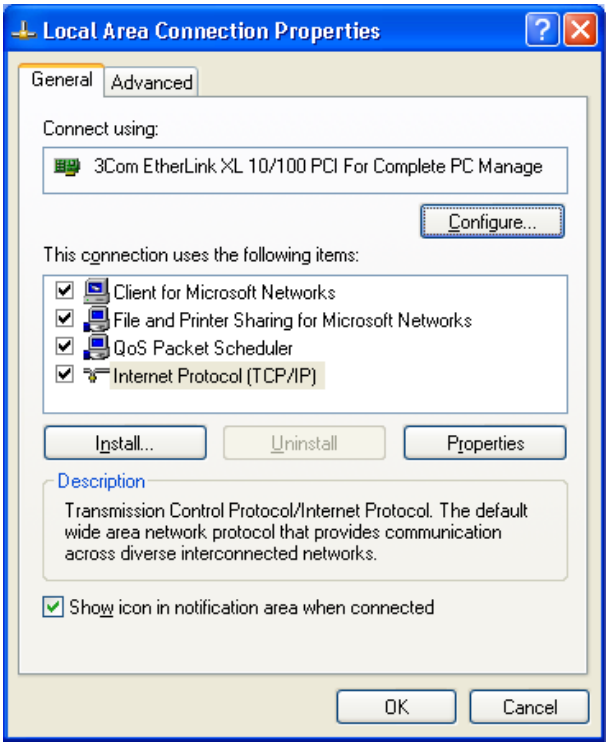
3 Select **Control Panel**.

4 Double-click **Network and Dial-Up Connections**.

5 Double-click **Local Area Connection**. The Local Area Connection Status window appears.

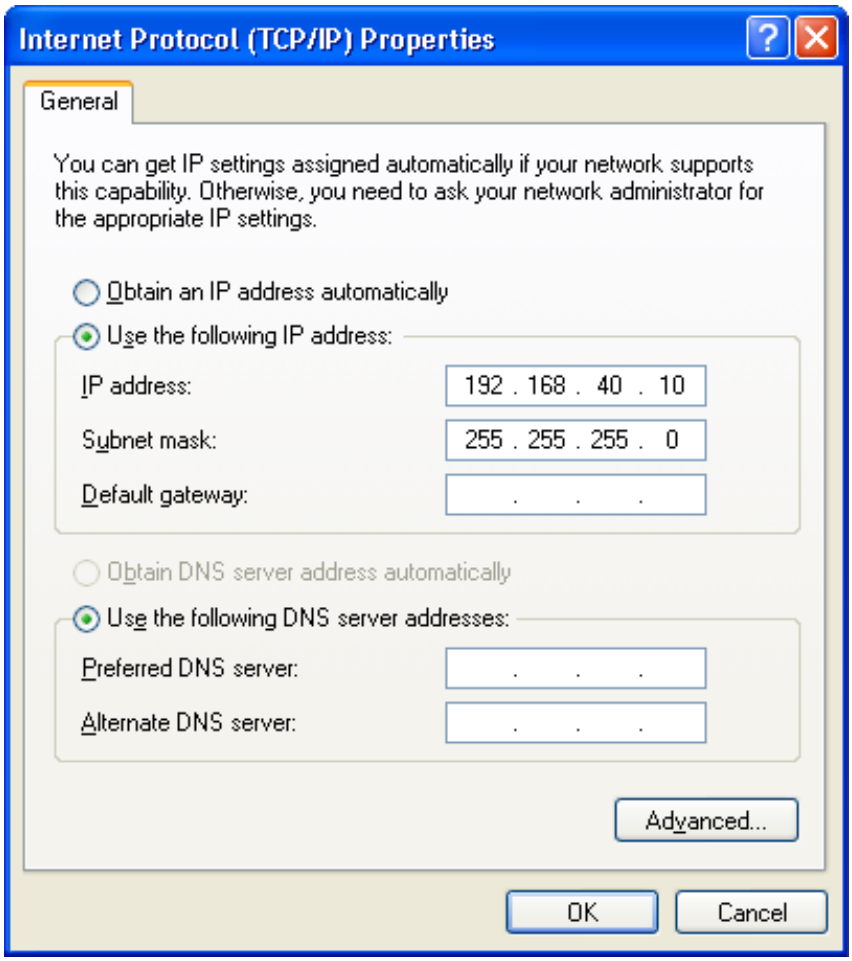


6 Click the **Properties** button.



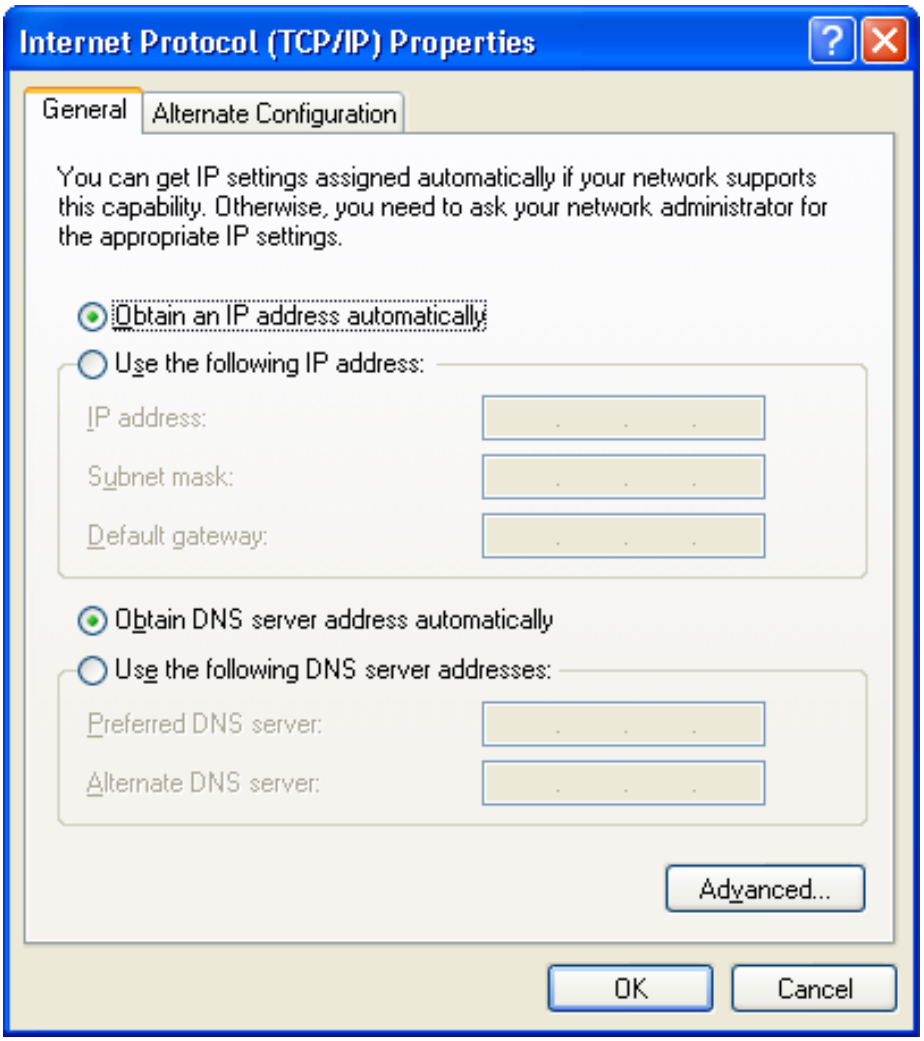
7 Ensure the box next to *Internet Protocol (TCP/IP)* is selected.

8 Click to highlight **Internet Protocol (TCP/IP)** and click the **Properties** button.



9 Enter **192.168.40.10** into the IP Address field.

10 Enter **255.255.255.0** into the Subnet Mask field.



11 (If using a DHCP after initial configuration, select ***Obtain An IP Address Automatically***.)

12 Click **OK** twice to exit and save your settings.

13 Proceed to the *Configure Your Wireless Settings* section to set up the security settings.

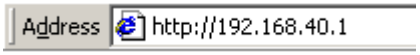
Configure Your Wireless Security Settings

Due to the limitation of the Wi-Fi WPA Test Plan, your AP's factory default settings are not set at their maximum security level. Adjustments are **strongly recommended** to ensure that you communicate securely on your wireless network at maximum strength. Failure to configure these settings properly could compromise your network to wireless hackers.

Logging In

If at all possible, connect your computer with an Ethernet cable to the AP and not wirelessly. If you log into the AP wirelessly for the first time, someone could be snooping and see the changes you make to passwords, thereby compromising your security from the very start. After you have configured the security settings, then wirelessly connecting to your AP is safe.

1 Once the AP is connected, open your web browser. Enter into the URL field **http://192.168.40.1** (the AP's default IP address) and press **Enter**.



The login screen will appear.

2 Enter the ***User ID***. The default factory setting is “admin”, without the quotation marks.

3 Enter the ***Password***. The default factory setting is “motorola”, without the quotation marks.

Once you have logged in, for security reasons, you should change the User ID and Password. See Wireless Security Setup.

4 Click the **Log In** button to enter the AP’s Web-based Configuration Utility.

Wireless Security Setup

Follow these procedures to setup the correct security protocols for your AP.

1 Select **Control Panel** > **Device Security**.

2 In the Change User ID field, enter in the desired ***Login User ID***. For strong security, select an ID that contains multiple of case-sensitive characters as well as numbers. It cannot be longer than 64 characters.

3 In the Change User Password field, enter in the desired ***Login Password***. For strong security, select a password that contains multiple of case-sensitive characters as well as numbers and symbols like “**_ +)**”. It cannot be longer than 64 characters.

4 Re-enter the same Password.

5 Click **Apply**.

6 Once the settings have been accepted, click **Restart** and log back into the *Configuration Utility* using your new User ID and Password.

7 Navigate to **Wireless** > **Basic.**

8 Change the ***SSID*** to a user-friendly name and click **Apply**.

9 Navigate to **Wireless** > **Security**.

10 Select **WPA-PSK** from the drop down list of ESS Authentication.

11 Select **AES** from the drop down list of Encryption Status.

12 Enter a new **Pass Phrase** and again in **Pass Phrase Confirm**. Remember this Pass Phrase so that you can enter the same phrase for the Motorola client devices on your wireless LAN. Pass Phrase must be between 8 and 63 characters.

13 Click **Apply** and then **Restart**. Your wireless configuration is now complete.

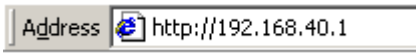
Section 3:Configuration

You can use the information in this section to modify the Access Point's (AP) settings. For example you can customize features for your home network, change settings such as your user name or password, view the status of the network, and more.

Using the Web-Based Configuration Utility

Logging In

1 Once the AP is connected, open your web browser. Enter into the URL field **http://192.168.40.1** (the AP's default IP address) and press the **Enter** key.



The login screen appears.

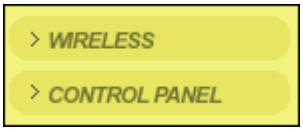
2 Enter the ***User ID***. The default factory setting is "admin", without the quotation marks.

3 Enter the ***Password***. The default factory setting is "motorola", without the quotation marks.

4 Click **Log In** to enter the AP's **Web-based Configuration Utility**.

Navigation

Each of the following subsections provides descriptions for the components of the AP's *Configuration Utility* – accessible from a web browser. These sections include:



- Wireless
- Control Panel

To navigate, click on a major section and then the associated subsection. For example, to adjust the **User Login ID**, click **CONTROL PANEL** on the left, then **DEVICE SECURITY** tab at top on the right. The Web-based Configuration Utility uses Javascript. Your web browser's Javascript needs to be enabled.

Help, Restart, and Logout

Click on the appropriate command to execute the action.

Help	If assistance is required in using the AP, click Help.
Restart	To restart your session with the Configuration Utility, click Restart. If you see Restart flashing, the change you have made requires that you restart the unit. **For convenience, it is recommended that you finish all of your configuration changes and then restart the unit.**
Logout	To logout out of the AP's Configuration Utility, click Logout.

Configuring Wireless Network Settings

The Wireless Network screens enable you to adjust settings for your wireless connection. Refer to each subsection for further descriptions. These include:

- Basic
- Security
- Site Monitor
- Advanced

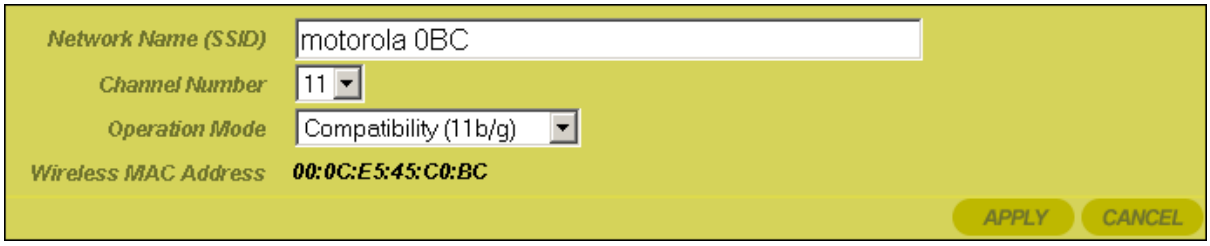
Wireless - Basic

This screen enables you to setup your Service Set Identifier (SSID) parameters for your network. The SSID is the name of your network that is shared among all the devices in a wireless network. The SSID must be identical on all of the devices in your wireless network. The SSID is case-sensitive and must not exceed 32 alphanumeric characters.

The default SSID is *motorola* appended with the last three characters of the unit's MAC address. It is recommended that you change this to a name easy for you to remember.

To access the screen, click **Wireless** > **Basic**.

Click **APPLY** to save your settings or **CANCEL** to cancel changes.



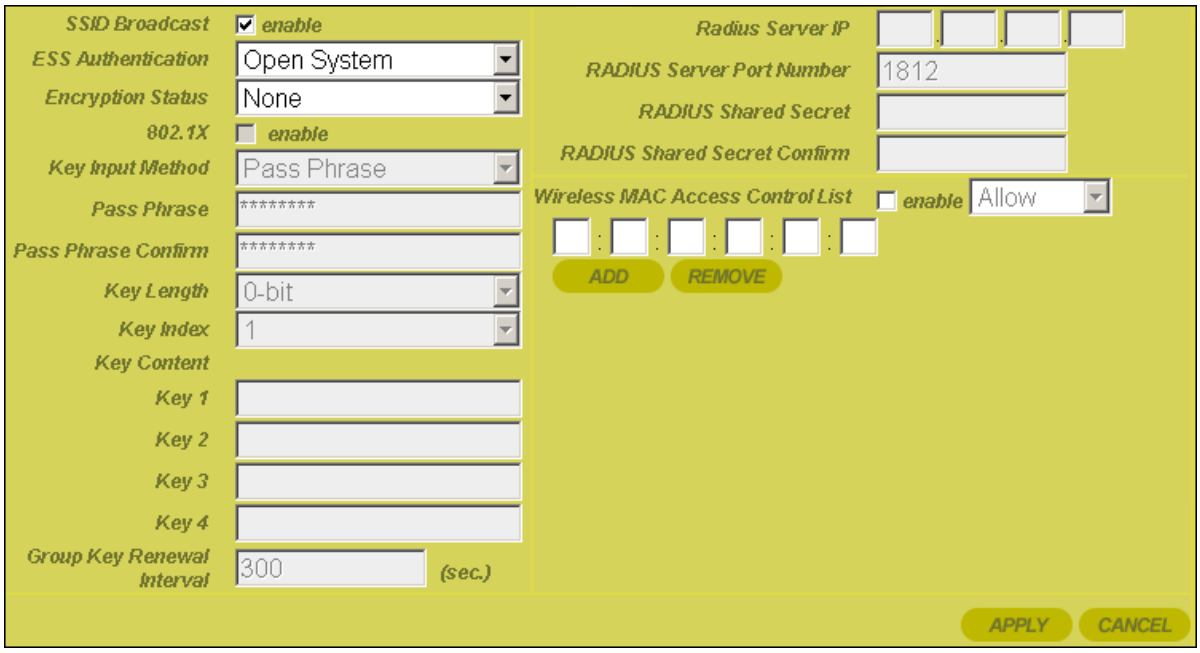
Field or Button	Description
Network Name (SSID)	Enter a Network Name (SSID) of no more than 32 alphanumeric characters. This SSID has to be entered on every wireless device on your wireless network. The default SSID is "motorola" along with the last three characters the unit's MAC address.

Field or Button	Description
Channel Number	Identifies the channel on which the AP communicates. Each wireless client must use the same channel to enable communication. This can only be altered from a PC that is wired directly to the AP, not wirelessly. For an Ad-hoc network, select a channel to broadcast. The default is Channel 11.
Operation Mode	Enables you to select the type of transmission protocol your wireless network uses. The default is 802.11b/g The options are: ▪ Compatibility (802.11b/g) ▪ Performance (802.11g only) ▪ Legacy (802.11b only)
Wireless MAC Address	Displays the MAC address of the unit.

Wireless - Security

This screen enables wireless security settings. Some fields activate other options. Refer to the descriptions for details. To access the screen, click **Wireless** > **Security**.

Click **APPLY** to save your settings or **CANCEL** to cancel changes.



Field	Description
SSID Broadcast	*Service Set Identifier (SSID)*. Broadcasts the SSID of the AP to devices on your network. This enables wireless clients, like a laptop, to receive the AP's SSID. If you don't want the SSID to be broadcast, disable this feature. The default is enabled.

Field	Description
ESS Authentication	*Extended Service Set (ESS*). Authentication differs from Encryption in that you are establishing either an open or secure verification of communication with an AP. This setting does not encrypt your transmission. The options are: Open System — The Open System Authentication method is used, meaning no authentication is used. Pre-Shared Key (PSK) — The Pre-Shared Key (PSK) 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. Select the option that best meets your needs. For home users, WPA-PSK is the best choice as it provides the strongest security without a RADIUS server. The default is Open System.

Field	Description
Encryption Status	Determines the type of security encryption algorithms for the Key Index. This security setting encrypts your wireless transmission. ▪ None, WEP64, and WEP128 are available only when Open System or Pre-Shared KEY (PSK) is selected. ▪ TKIP and AES are available only when WPA and WPA-PSK are selected. The options are: None — No security WEP64 — Wired Equivalent Privacy - 64-bit strength (provides 4 Keys) WEP128 — Wired Equivalent Privacy - 128-bit strength (provides 2 Keys) TKIP — Temporal Key Integrity Protocol - changes the temporal key often (provides 1 Key) AES — Advanced Encryption Standard (provides 1 Key) Select the option that best matches your needs. Motorola recommends using AES (which requires WPA or WPA-PSK selected) because it provides a stronger security algorithm. The default is None.
802.1X mode	Can only be enabled when the ESS Authorization is set to Open or PSK and either WEP64 or WEP128 is selected (see the Encryption Status field). During the Authentication process, the server verifies the identity of the client attempting to connect to the network. When WPA-PSK is selected in the ESS Authentication field, this option is automatically selected. If not already enabled, select to activate this feature. When enabled, Dynamic Key generation occurs. That is, when the client requests a key, this function dynamically generates one. The default is disabled.

Field	Description
Key Input Method	Unavailable if WPA is selected. The options are: ▪ Pass Phrase ▪ Hexadecimal ▪ ASCII If you select either Pass Phrase or Hexadecimal, in Key Content, the format of the Key appears in a hexadecimal format. *If you are using other non-Motorola wireless products and a security algorithm other than WPA-PSK, you must enter your WEP keys manually in hexadecimal format for the non-Motorola wireless products.* Select the option that best matches your needs. The default is Pass Phrase.
Pass Phrase	Enter the Pass Phrase to be used for Key encryption. Remember this Pass Phrase so that you can enter the same phrase for the Motorola client devices on your wireless LAN. You will use this Pass Phrase when using WPA security with your client devices. Pass Phrase must be between 8 and 63 characters.
Key Length	Only available when ESS Authentication is set PSK and the Encryption Status is set to None. The option selected determines the strength of the key. There are two options: ▪ 128-bit ▪ 64-bit. Select the option that best matches your needs.

Field	Description
Key Index	There are up to different 4 Keys (1, 2, 3, or 4) that can be selected, the amount determined by what is selected in the Encryption Authentication and Encryption Status field. You are selecting one of the Key Content fields below. The Key selected here must match between the AP and the client. For example, if you select Key 1 here you have to select Key 1 for the client. Select the option that best matches your needs. The default is 1.
Key Content Key 1 Key 2 Key 3 Key 4	There are up to four fields available (Key 1 – Key 4) that can be filled. The Key Content format is selected in the Password Input Format field. For the key content, the phrase is auto-generated by the password entered in the Pass Phrase field. For non-Motorola clients, you will use these Keys (and not Pass Phrase) when using WEP for security. If you have selected Hexadecimal or ASCII formatting (in the Key Input Method field), you can then enter your own Hexadecimal or ASCII keys. If entering keys manually, this also depends on whether WEP64 or WEP128 is selected in the Encryption Status field. ▪ For WEP64 keys, 5 case sensitive ASCII characters are allowed or 10 hexadecimal characters (using only characters 0-9 and A-F). ▪ For WEP128 keys, 13 case sensitive ASCII characters are allowed or 26 hexadecimal characters (using only characters 0-9 and A-F). *If entering a key manually, don't leave a key field blank or enter all 0's. These are not secure keys.*

Field	Description
Group Key Renewal Interval	Only available if ESS Authentication is set to WPA. This is the number of seconds that pass until your AP sends out a new group key. Enter in the option that best matches your needs. The default is 300 seconds.
RADIUS Server IP RADIUS Server Port Number	RADIUS is an authentication and accounting system used by many Internet Service Providers (ISPs), which verify users. Either of the conditions need to exist: ▪ Open System is selected, along with either WEP64 or WEP128, and 802.1X is enabled ▪ WPA is selected and TKIP or AES is selected. Enter the RADIUS Server IP and Port number. The default RADIUS Port Number is 1812.
RADIUS Shared Secret RADIUS Shared Secret Confirmation	A password that is entered twice for confirmation.

Field	Description
Wireless MAC Access Control List	Enables you to control which PC has access to your wireless network based upon their MAC address. The default is disabled. The options are:

Enable	Select to enable/disable the MAC Access Control List (ACL). When disabled, the MAC ACL is not active and any wireless station is allowed to communicate with the wireless AP.
Allow	Allows only the wireless devices in the ACL to communicate with the wireless AP.
Deny	Denies wireless devices in the ACL from communicating with the wireless AP.

To add a MAC address:

1. Check **enable**.
2. Select **Allow** or **Deny**.
3. Enter a ***MAC Address*** and click **ADD** to enter the Address into the ACL.

To edit a MAC address:

1. Remove and replace with the updated address.
2. Click **APPLY** to save.

To delete a MAC address:

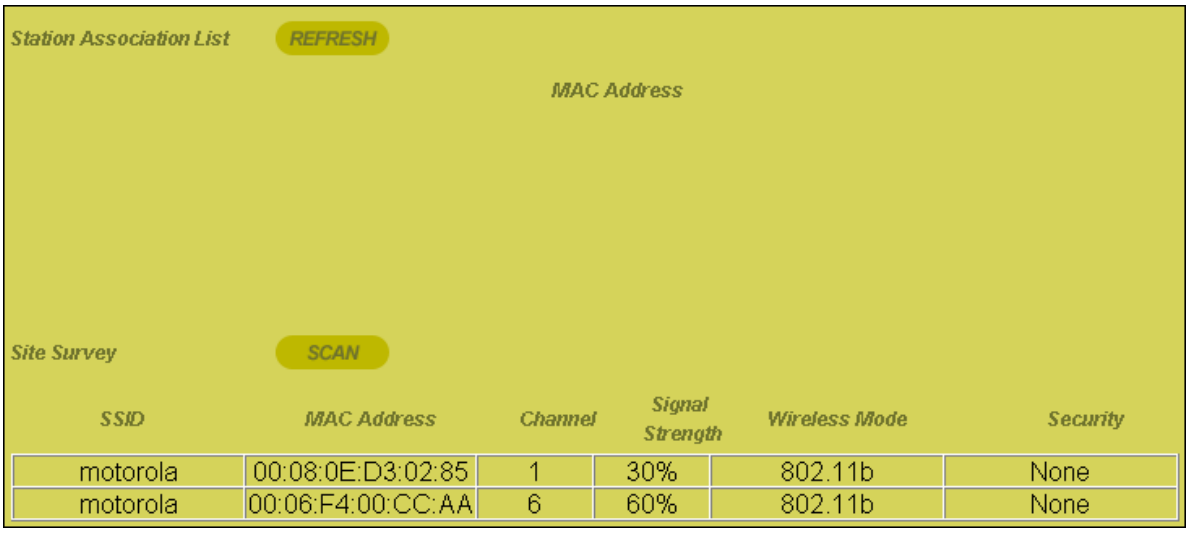
1. Click into the MAC address you wish to delete. Once activated, the field will change color.
2. Click **REMOVE** to clear the address.
3. Click **APPLY** to save.

Wireless - Site Monitor

This screen displays information about wireless Access Points (AP) and stations, and their associated information:

Station Association List	Identifies only those stations that are connected your wireless AP.
Site Survey	Reveals information of other APs in the area.

To access the screen, click **Wireless** > **Site Monitor**.

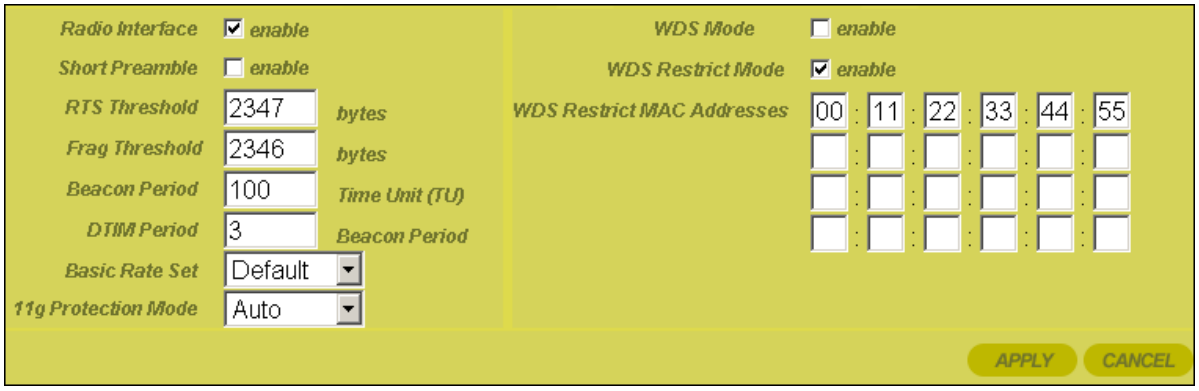


Field	Description
Station Association List	
MAC	Displays the MAC address of the client.
Host Name	Displays the name of the device attached.
Site Survey	
Scan	Click to search for more APs or clients.
SSID	Displays the SSID of the device found.
MAC Address	Displays the MAC address of the device found.
Channel	Displays the channel upon which the device is broadcasting.
Signal Strength	Displays the Signal Strength of the device found.
Wireless Mode	Displays which protocol is used, 802.11b or 802.11g.
Security	Displays the security protocol used.

Wireless - Advanced

This section enables you to turn on and off your wireless network and adjust wireless parameters. Generally, the settings here should remain at their default values.

To access screen, click **Wireless** > **Advanced**. Click **APPLY** to save your settings or **CANCEL** to cancel changes.



Field	Description
Radio Interface	Enables you to turn on and off the wireless feature. The default is enabled.
Short Preamble	Improves the efficiency of a network's throughput when transmitting special data such as voice, VoIP (Voice-over IP) and streaming video. The default is disabled.
RTS Threshold	The packet size at which an AP issues a request to send (RTS). The range is 0 to 2347 bytes. The default is 2347. If you encounter inconsistent data flow, only minor modifications are recommended. If needed, enter a new value.
Fragmentation Threshold	The size at which packets are fragmented and transmitted a piece at a time instead of all at once. The setting must be within the range of 256 to 2346 bytes. The default is 2346. If needed, enter a new value.

Field	Description
Beacon Period	The Beacon Period and Delivery Traffic Indicator Maps (DTIM) work together to keep power management in check. For example, if a client does not receive a beacon within a certain time period, it goes to sleep. This is why lowering the beacon period and DTIM period settings may keep sleepy clients awake. However, DTIM and Beacon settings do use additional bandwidth. So, setting them too low can have an effect on WI-FI performance. On the other hand, if no wireless clients use power management, then increasing the DTIM and Beacon settings may improve overall throughput. Usually the default settings are fine. A beacon is a packet broadcast by the Access Point to keep the network synchronized. You are able to set the Beacon Period value from 1 to 65535 in Time Units (TU). The default is 100. If needed, enter a new value.
DTIM Period	You are able to set the Delivery Traffic Indicator Maps (DTIM) period value from 1 to 255 in multiples of Beacon Periods. The default is 3. If needed, enter a new value.
Basic Rate Set	The AP broadcasts different transmission rates so clients know which transmission rate to use to join the network. The default is Default. The options are: **1 to 2 Mbps** — The slowest speed available. **Default** — Ensures compatibility with 802.11b or 802.11g devices **All** — Ensures compatibility with all devices.

Field	Description
11g Protection Mode	Ensures that your wireless AP does not interfere with neighbor networks. 802.11b networks cannot hear 802.11g networks, but 802.11g networks can hear 802.11b networks. The Protection Mode improves performance when 802.11b and 802.11g stations coexist in the network. The default is Auto. The options are: **Disable** 802.11g Protection Mode is never used. **Auto** 802.11g Protection Mode is used if either an 802.11b client joins the network or the AP detects an 802.11b network on the same channel
WDS Mode	Wireless Distribution System (WDS) enables you to share and expand your network with other wireless Access Points (AP). The WDS fields, WDS Restrict Mode and WDS Restrict MAC address, become active once WDS is enabled. When enabled, any AP can connect if using your settings. The default is disabled.
WDS Restrict Mode	An activated WDS Restrict Mode enables you to protect your network by assigning access in the WDS Restrict MAC address field to only those APs you designate. The default is enabled.
WDS Restrict MAC address	**1** Enter up to four AP MAC addresses. **2** To edit an entry, highlight the number and change. **3** To delete a number, delete each field.

Configuring Control Panel Settings

The Control Panel screens enable administrative maintenance for your AP, such as changing your User Name/Password, updating your firmware, or backing up your configuration.

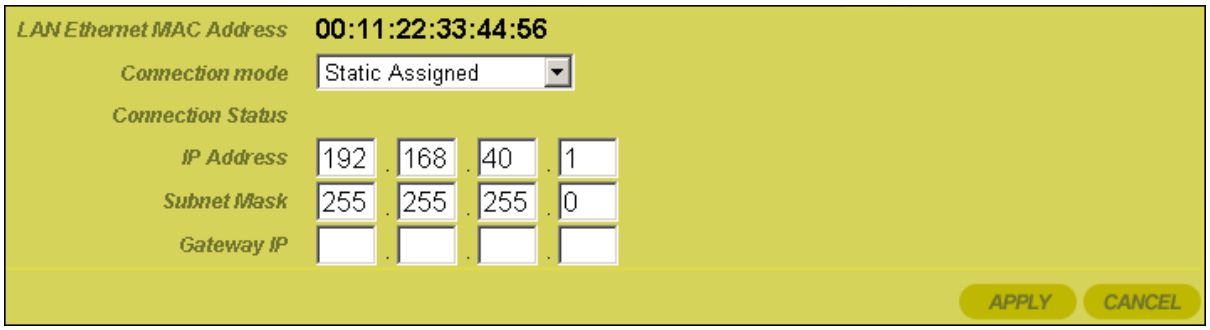
The following screens are available in Control Panel:

- Network Access
- Device Security
- Firmware Update
- Configuration Data

Control Panel - Network Access

This screen enables you to change your Connection Mode and IP settings.

To access the screen, click **Admin Control Panel** > **Network Access**. Click **APPLY** to save your settings or **CANCEL** to cancel changes.



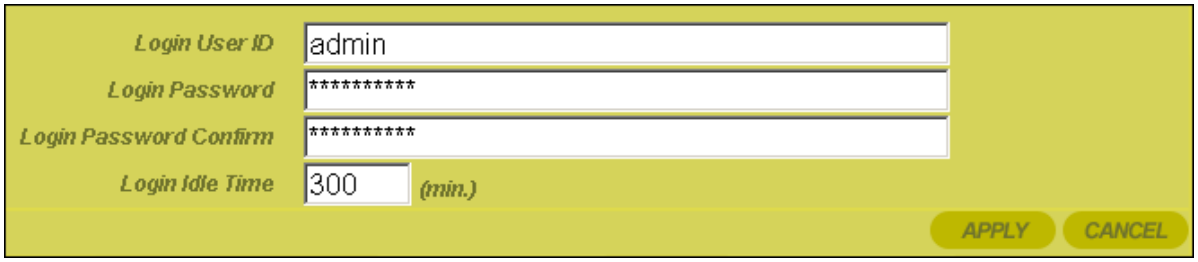
Field	Description
LAN Ethernet MAC Address	Displays the unit's MAC address.

Field	Description
Connection Mode	The AP supports two connection modes: ▪ Cable Modem (DHCP) ▪ Static Assigned Select the appropriate connection method for your ISP (Internet Service Provider). Based on which connection type you select, different areas are grayed out (become inaccessible), leaving you only the appropriate fields to fill in. For details on each Connection Mode type, refer to *Section 2:Installation*.
Connection Status	Provides current information about the connection status of the AP.
IP Address	The AP's IP Address used to connect to your ISP or router. It is either automatically displayed or manually entered from information provided by the provider. If DHCP is selected, this is the IP Address that your AP is currently using to access the Internet. If using Static Assigned, then you would enter the IP Address here.
Subnet Mask	Is either automatically displayed or manually entered from information provided by your ISP.
Gateway IP	Is either automatically displayed or manually entered from information provided by your ISP.

Control Panel - Device Security

This screen enables you to change your User ID and password and enables you to manage your AP remotely.

To access the screen, click **Admin Control Panel** > **Device Security**. Click **APPLY** to save your settings or **Clear** to cancel changes.



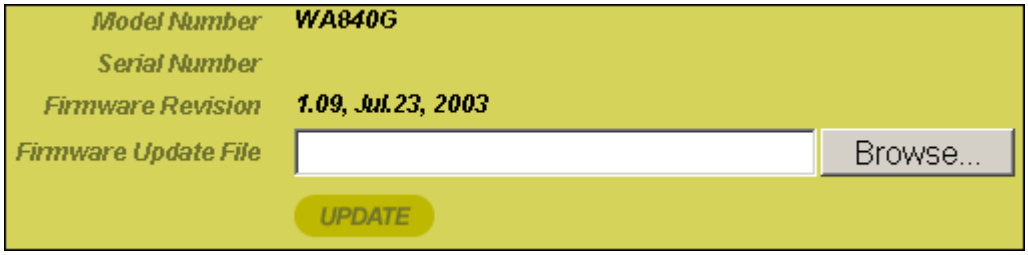
Field	Description
Login User ID	Changes the User ID used for logging into the AP's web-based utility. It cannot be longer than 63 bytes. A blank user name is not allowed. The default is "admin".
Login Password	Use this option to change the Password, used to log into the AP's web based utility. It cannot be longer than 63 bytes. A blank password is not allowed. The default is "motorola".
Login Password Confirm	Re-enter the User Password.
Login Idle Time	The amount of idle time (no actions occur) that elapses before the AP automatically logs you off. The default is 10 minutes.

Control Panel - Firmware Update

This screen enables you to update the firmware (AP's hardware control mechanism). Listed on this screen is the current version of the Model Number, Serial Number, and Firmware Number; enabling you to verify that you are running the most current version.

Access this website www.motorola.com/broadband/networking to check for a firmware update.

To access the screen, click **Admin Control Panel** > **Firmware UPDATE**.



To update the firmware:

1 Download the latest file to your computer.

2 To locate the file you downloaded, type the path to the file or click **Browse** and navigate to it.

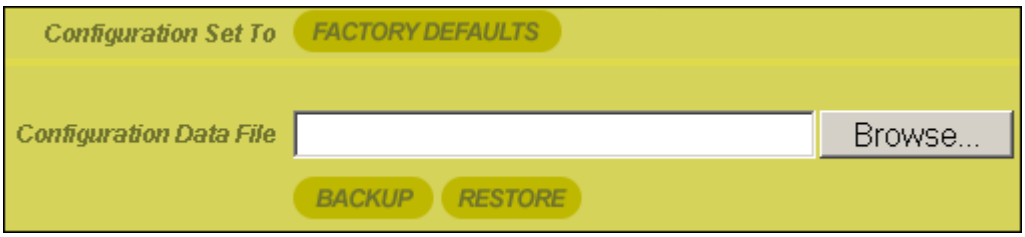
3 Click **UPDATE** to update the AP with the selected firmware file. The AP will inform you that you successfully updated the unit.

4 Follow the prompts for restarting.

Control Panel - Configuration Data

This screen enables you to save and restore your settings, that you have currently configured for your AP, to a file. You are also able to reset the AP to the factory default settings.

To access the screen, click **Admin Control Panel** > **Configuration Data**.



To reset the AP to its original configuration; click **FACTORY DEFAULTS**.

To backup your settings:

1 Click **BACKUP**.

2 From the pop up window, choose the destination for the file.

3 Enter a descriptive file name.

To restore your settings:

1 Locate the Configuration file on your computer by entering the path to the file or click **Browse** and navigate to it.

2 Click **RESTORE** to reapply the saved settings with the selected file.

Section 4:Troubleshooting

This section will detail possible solutions to common problems that might occur in using the Access Point (AP).

Contact

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.

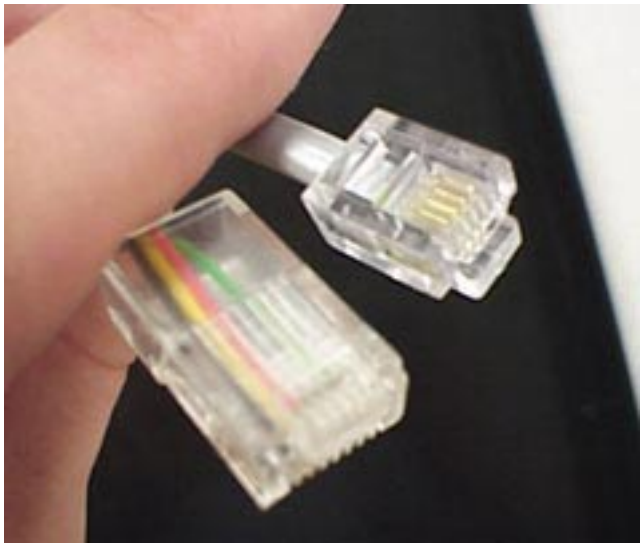
Hardware Solutions

My computer is experiencing difficulty connecting to the wireless network.

- Ensure that your Access Point (AP) is powered on and that the Wireless LED is lit.
- Ensure that your wireless adapter (PCI card, Notebook or Ethernet adapter) is installed correctly and is active.
- Ensure that your wireless adapter's radio signal is enabled. Review your adapter's documentation for further instructions.
- Ensure that your wireless adapter for your PC and the AP have the same security settings that will allow your computer to access the wireless network. Section 3: Wireless > Security details how to adjust security settings.
- Ensure that your AP is within range of your router or is not behind obstruction, for example metal structures will interfere with the signal, as will 2.4 GHz cordless phones, and microwaves.
- Ensure that your antenna is connected and that your router's antenna is also connected.

My computer is experiencing difficulty in connecting to the AP.

- Check that all of your cable connections are tight and secured. This includes the cables from the wall to your modem, between the router and modem, and, if available, from the AP to your PC. Ensure that your LEDs are not lit Red or not at all. For further information about LED descriptions, see Section 1: Overview.
- Ensure that you are using Ethernet cables and not telephone cables between the router and modem, router and PC, or if available, AP and PC. Ethernet cables use a wider RJ-45 style plug using 8 wires where telephone style plugs use the smaller RJ-11 style plug using 4 to 6 wires.



The plug on the left is RJ-45; the plug on the right is RJ-11 – use only RJ-45.

- Ensure that your Ethernet adapter is enabled. Check the System Tray at the bottom right of your display to see an icon that looks like a monitor. You can click on this to see the status of your Ethernet adaptor. Also in Control Panel > Network and Dial-Up Connections, you can examine the state of your Ethernet adaptor.

Software Solutions

I would like to see if my Internet connection is alive.

For this, you will use the *ping* command to test the connection. Before attempting, ensure that **Obtain an IP address automatically** has been selected in the computer's settings and that you have an IP address assigned. Refer to Section 2: Configuration > Configure Your Computers, for further details.

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

- 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**.

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

- You should see an IP address for your network adapter:

```
Ethernet Adapter Local Area Connection:

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

IP Address. . . . . : 192.168.40.3

Subnet Mask . . . . . : 255.255.255.0

Default Gateway . . . . . : 192.168.40.1
```

3 In the *Command* window, type **ping** followed by the ***AP's IP address*** and press **Enter**. For example type: **ping 192.168.40.3**.

There is a good possibility that the Default Gateway's IP address is the AP's IP address. You can verify the AP's IP address on the Control Panel > Network Access screen.

- If you receive a reply (the first word will be *Reply…*), then your computer is connected to the AP. Proceed to *Step 4*.
- If you do NOT receive a reply, try from a different computer to verify that the first PC is not the cause of the problem.

4 In the *Command* window, type **ping** and your ***ISP's default gateway*** and press **Enter**. For example type: **ping 192.168.40.1**.

- If you receive a reply (It might look something like this: *Reply from 216.109.125.72…*), then your connection to the Internet is alive and well. You can verify the ISP's IP address at the Gateway IP field on the Control Panel > Network Access screen.

- If you do NOT receive a reply, try from a different computer to verify that the first PC is not the cause of the problem.

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

I cannot access the Web-Based Configuration Utility for the AP.

- Verify your Ethernet connection to the AP.
- Verify that the IP address of the PC being used to configure the AP is on the same network as the AP's configuration IP address.
- The IP address of your network adapter must be on the same network and not a duplicate of any others on the network (for example: 192.168.40.3 and using a subnet mask of 255.255.255.0 can be used to login to the AP's default IP address of 192.168.40.1). Refer to Section 2: Configuration > Configure Your Computers on how to adjust the IP address for your PC.
- Verify that you can ping the AP on this IP address.
  - In the *Command* window, type **ping** and your AP's default ***IP address*** and press **Enter**. For example type: **ping 192.168.40.3**
  - If you have changed the factory configured default IP address of the AP, you will need to set your network adapter accordingly.
- Verify you are entering the correct URL in the browser. The default is http://192.168.40.1. If you think you have changed the IP address used to configure the AP and cannot remember it, you must reset the unit back to factory defaults. To do this, press and hold the reset button for more the 5 seconds. This clears the AP's user settings, including User ID, Password, IP Address, and Subnet mask.
- Once the AP is reset to factory default, re-verify the Ethernet connectivity and IP address issues.
- Verify you are using the latest version of IE or Netscape. IE 5.2 and below are not supported.

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

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.

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 64 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 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 a 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 to the router or AP 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 1.1 supports data transfer rates of 12 Mbps and plug-and-play installation. You can connect up to 127 devices to a single USB port. USB 2.0 supports data rates of 480 Mbps.

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 Public Switched Telephone Network (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.

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

494153-001
07/03

MGBI