User Guide

Wireless Ethernet Bridge

WE800G

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 WE800Gv2 (FCC ID: ACQWE800GV2) 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 **1-2**
Box Contents **1-3**
Understanding Functions **1-3**
Wireless Ethernet Bridge Connectivity 1-3
TCP/IP 1-4
Static IP Address *1-4*
Dynamic IP Address *1-4*
Understanding Wireless *1-4*
Wireless Range 1-5
Recommended Wireless Environment 1-5
Type of Networks **1-6**
Wireless Ethernet Bridge Infrastructure Mode 1-6
Wireless Ethernet Bridge Ad-Hoc Mode 1-7
Multiple Clients Mode 1-8
Wireless Ethernet Bridge Physical Description **1-9**
Back of Wireless Ethernet Bridge 1-9
Front of Wireless Ethernet Bridge 1-11
LED Description 1-12

Section 2:Installation 2-1

Hardware Setup **2-1**
Antenna Installation 2-1
Wireless Ethernet Bridge Physical Installation 2-2
Horizontal Installation *2-2*
Vertical Installation *2-3*
Wall Mount Installation *2-3*
Electrical Connection to Wireless Ethernet Bridge 2-6
Easy Software Setup **2-7**
Manual Software Setup **2-7**
Wired Connection to Wireless Ethernet Bridge 2-8
Configure Your Computers **2-9**
Configuring Windows 98SE and ME 2-10
Windows 98 and ME DHCP Server Configuration *2-12*
Configuring Windows 2000 2-12
Windows 2000 DHCP Server Configuration *2-15*
Configuring Windows XP 2-15
Windows XP DHCP Server Configuration *2-18*
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 Log Out 3-2
Active Profile and Site Monitor 3-3
Site Survey – Active Profile.....3-3
Site Survey – Site Monitor.....3-4
Configuring Wireless Profile 1 or 2.....3-5
Wireless – Basic.....3-5
Wireless – Security 3-6
Wireless – Advanced 3-10
Wireless – Professional.....3-11
Configuring Control Panel Settings.....3-13
Control Panel – Network Address 3-13
Control Panel – Device Security.....3-14
Control Panel – Firmware Update.....3-15
Control Panel – Configuration Data.....3-16

Section 4:Troubleshooting 4-1

Contact Us 4-1
Hardware Solutions.....4-1
Software Solutions.....4-3
I cannot access the Configuration Utility for the unit. 4-3
My WE800G cannot associate with the wireless access point/router 4-4
I would like to see if my Internet connection is alive.....4-4

Section 5:Glossary 5-1

Section 1:Overview

Congratulations on purchasing the Motorola Wireless Ethernet Bridge WE800G. With this unit, you have entered the world of freedom and independence – freedom from wires and the independence to communicate wherever YOU choose.

The WE800G is built with both the popular 802.11b wireless standard and the new nearly 5-times-faster 802.11g standard, providing you the ultimate in flexibility and speed. With Wired Equivalent Privacy (WEP) supported, 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 Wireless Ethernet Bridge control software up-to-date. The WE800G captures the latest technology in a package that stays current, connects multiple products to your home network, and provides you easy home network management.

Wireless Ethernet Bridge WE800G

Features

The WE800G has the following features:

- Wirelessly connects separate wireless networks together
- Connect any Ethernet equipped device to your wireless network; for example, a gaming console, a laptop or desktop computer, or a printer
- Compatibility with both 802.11g and 802.11b standards
- CD-ROM based Installation Wizard for easy installation
- Built-in Web interface for easy configuration
- Firmware upgrade to stay current with latest specification

Your Motorola WE800G Wireless Ethernet Bridge enables you to extend your wireless network and increase your productivity.

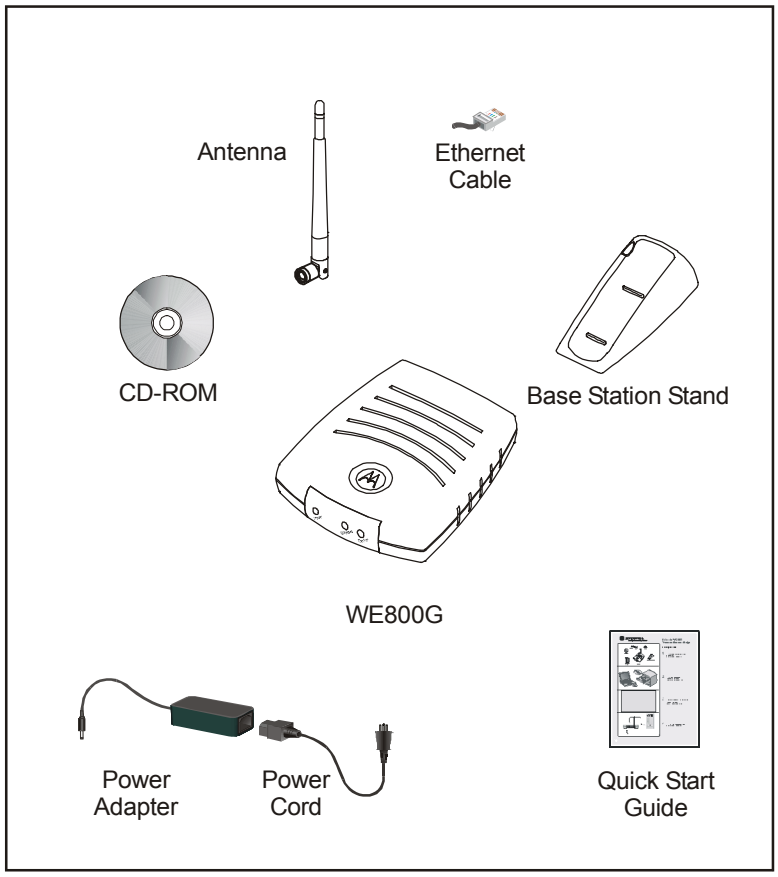
Understanding your User Guide

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 Wizard 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 web-based Configuration Utility to manage your unit.
Glossary	Defines the terms and acronyms.

Box Contents

Your box contains the following:



Understanding Functions

The various technologies and features used by your Wireless Ethernet Bridge require some conceptual explanation so that you can make the correct choices when configuring your unit.

Wireless Ethernet Bridge Connectivity

Your unit wirelessly connects:

- Networks or units to a network, Or
- By configuring multiple clients such as laptops, each using their own Wireless Ethernet Bridge, are you able to create your own private wireless Ad-Hoc network

The mechanics behind the connectivity are explained in the following subsections.

TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) comprises the backbone of the Internet. IP moves packets of data between nodes while TCP verifies delivery from client to server. Every device you hook up to your wireless router identifies itself with an IP address. You are able to assign devices on your network with either a static or dynamically assigned IP address.

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 address, dynamically or randomly generated by a DHCP server. The address lasts only as long as the server specifies, 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 Ethernet Bridge uses a radio transmission technology defined by the Institute of Electrical and Electronics Engineers (IEEE) called 802.11 or Wi-Fi (Wireless Fidelity). This 802.11 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 Wireless Ethernet Bridge supports both the ‘b’ and ‘g’ specifications. The 802.11b standard specifies transmission rates up to 11 Mbps while the 802.11g standard specifies transmission rates up to 54 Mbps. 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 the 802.11b and 802.11g standards operate in the 2.4 GHz range, meaning other electrical appliances also might interfere with the Wireless Ethernet Bridge – televisions, radios, microwave ovens, and 2.4 GHz cordless telephones. Therefore, positioning your Wireless Ethernet Bridge 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:

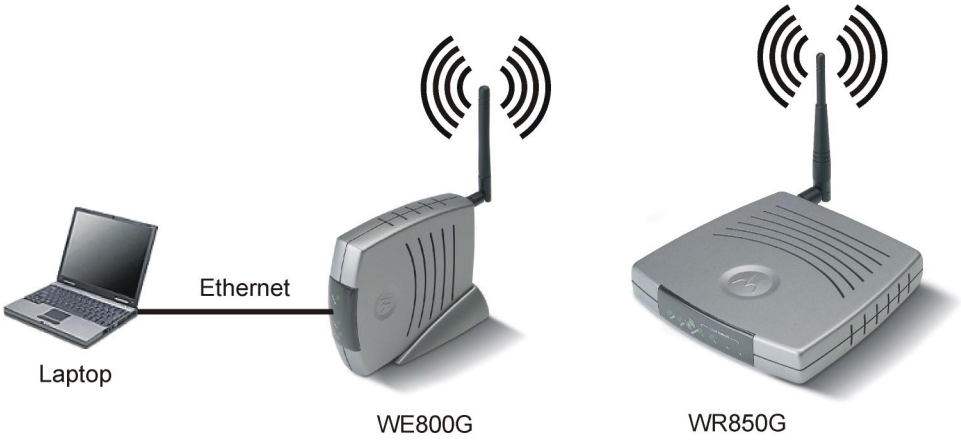
- Placing your Wireless Ethernet Bridge in the physical center of your network is the premium location because the antenna radiates out the signal in all directions.
- Placing the unit in a higher location, such as atop a cabinet, helps to disperse the signal cleanly, especially to receiving locations 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.

Type of Networks

Your Wireless Ethernet Bridge supports several different usage scenarios and the following examples illustrate the flexibility of your WE800G. Some scenarios require additional hardware.

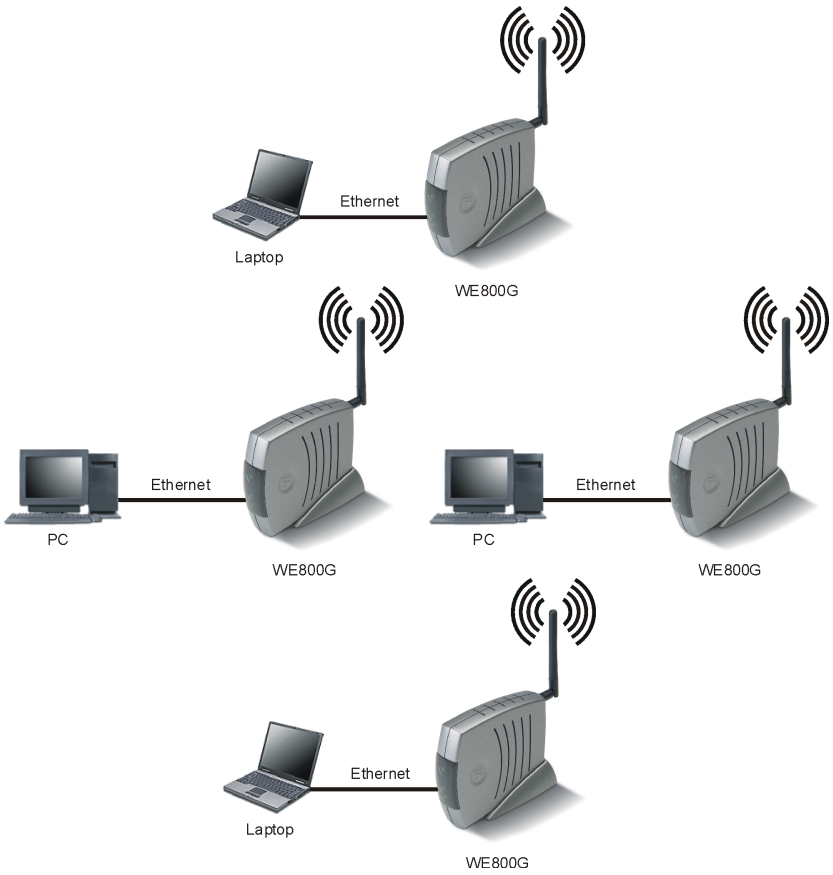
Wireless Ethernet Bridge Infrastructure Mode

In this mode, the WE800G functions like a bridge, connecting wired Ethernet clients to a wireless network. This is the most likely scenario you will use, because it shares an Internet connection with your laptop or other wireless client.



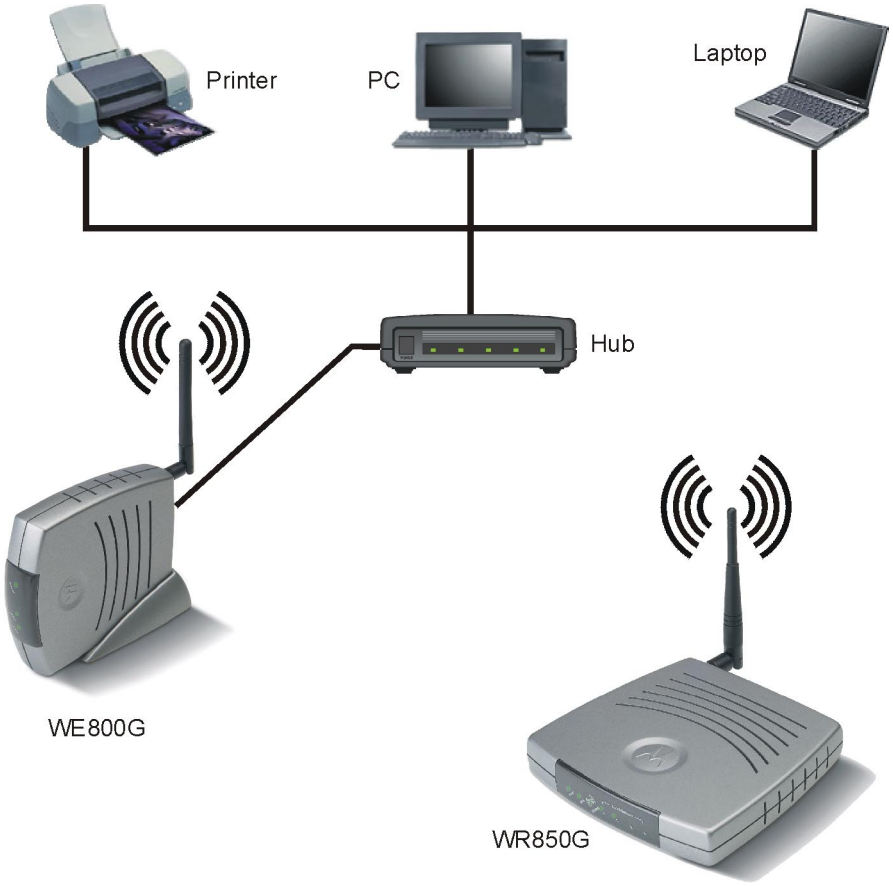
Wireless Ethernet Bridge Ad-Hoc Mode

This mode is very similar to the Wireless Ethernet Bridge Infrastructure mode, except the WE800G will connect to other client devices using Ad-Hoc mode. One inherent limitation of operating in this mode is that all client devices must be in wireless range of each other, as opposed to a network with an Access Point, where all wireless devices must be in range of the Access Point.



Multiple Clients Mode

In this mode, the WE800G connects multiple clients to your network wirelessly.

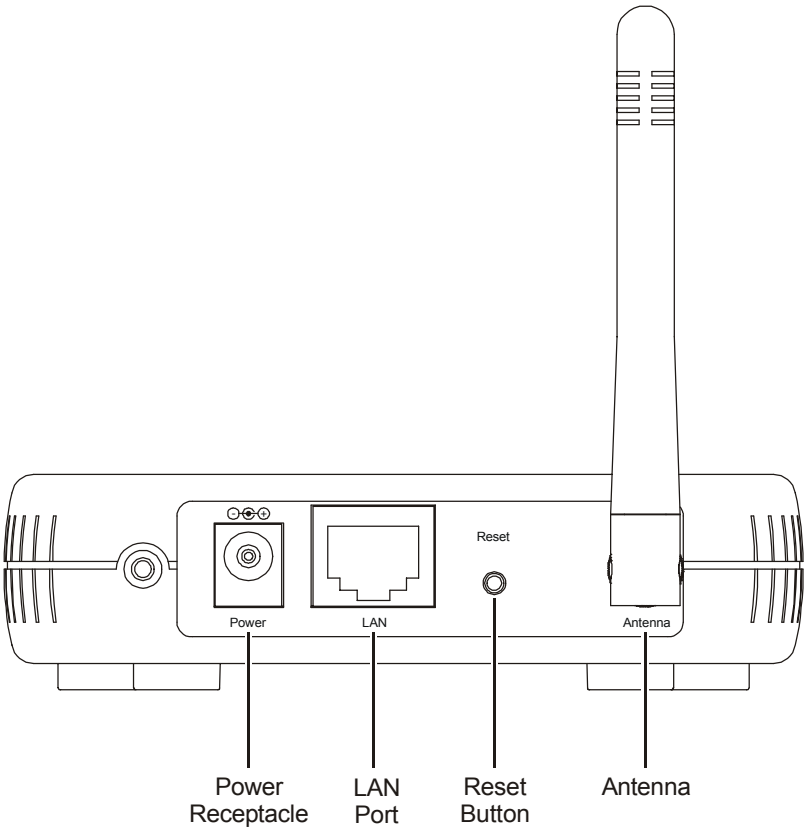


Wireless Ethernet Bridge Physical Description

The following sections describe the physical characteristics of the WE800G.

Back of Wireless Ethernet Bridge

The following illustration shows the WE800G back panel:

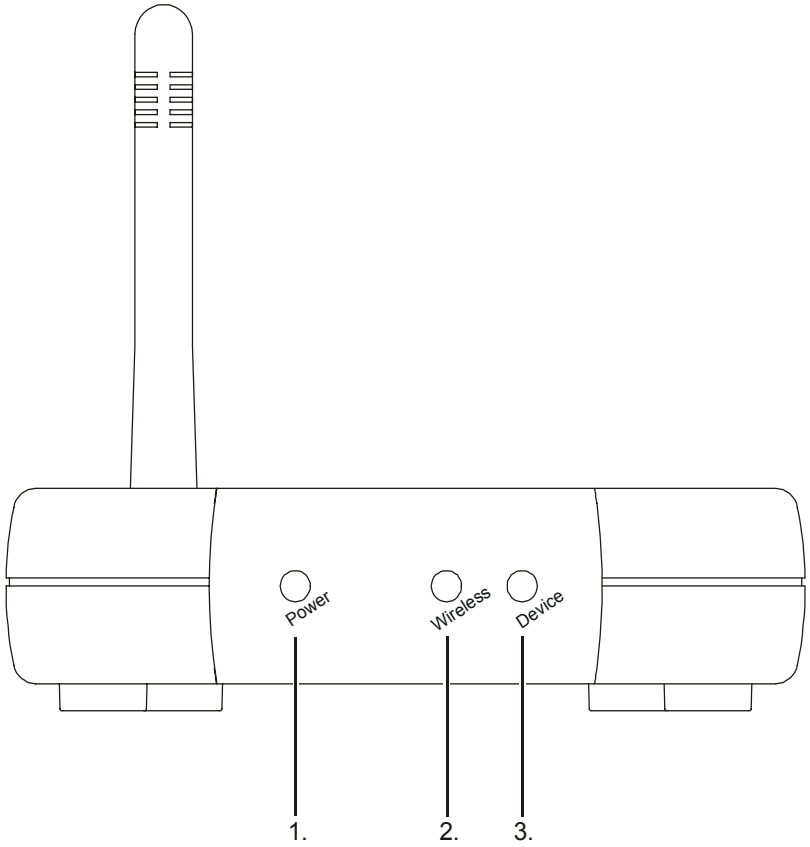


Feature	Description
Power Receptacle	The receptacle used to plug in the power adapter.
LAN Port	The receptacle used to plug in an Ethernet cable.

Feature	Description
Reset Button	A dual-function button. It either resets your unit or resets the unit to the default login settings. If the Wireless Ethernet Bridge is experiencing trouble connecting to the Internet, briefly press and release the Reset button to reset the router. This retains the router's configuration information. To reset the unit to the factory defaults while the unit is powered up, press and hold the Reset button for more than five seconds. This clears the Wireless Ethernet Bridge's user settings, including User ID, Password, IP Address, and Subnet mask. Refer to *Section 3: Configuration* to re-configure the unit.
Antenna	The antenna used for wireless connections. You are able to rotate and tilt the antenna to gain the best signal reception.

Front of Wireless Ethernet Bridge

The following illustration shows the WE800G front panel:



The LEDs of the unit indicate its operational 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 five seconds, the LED starts to blink, during which time the Wireless Ethernet Bridge'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**	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:

1 Setup your hardware.

CAUTION!

Use only the Motorola supplied WE800G power adapter.
This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

2 Insert the CD-ROM for Software Setup. Follow the prompts.

If you prefer to setup the Wireless Ethernet Bridge 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:

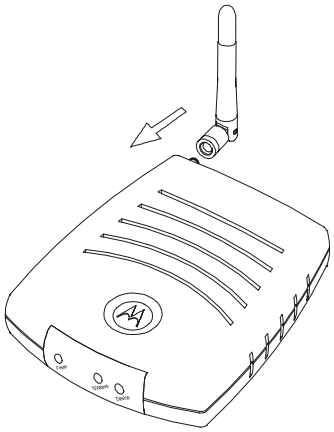
- Antenna Installation: connecting the antenna to the unit.
- Physical Installation: where you physically place your unit.
- Electrical Connection: how to power your unit.

Antenna Installation

When shipped, the antenna is already installed on the main unit. If, for some reason, you have to detach and than re-attach the antenna to the main unit:

1 Take the bottom of the antenna and locate, on the right backside of the Wireless Ethernet Bridge, the threaded knob.

2 Screw the antenna connector (counter-clockwise to remove, clockwise to attach) on to the threaded knob until firmly seated. When attaching, do not over-tighten.



Wireless Ethernet Bridge Physical Installation

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

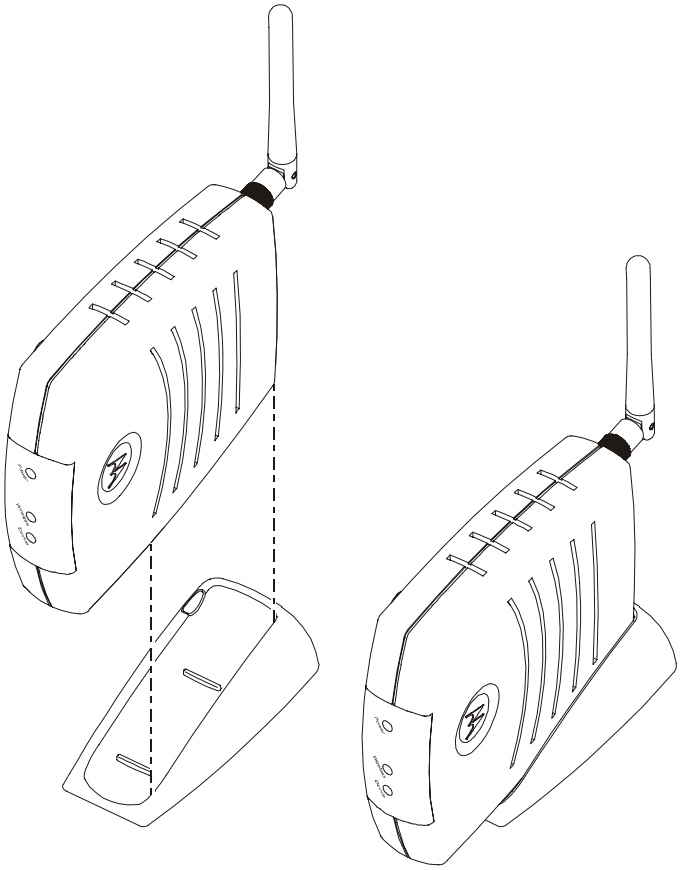
Horizontal Installation

To install the Wireless Ethernet Bridge horizontally, as shown in the illustration below:

1. Place the Wireless Ethernet Bridge in the desired location.
2. Follow the procedures in “Electrical Connection to Wireless Ethernet Bridge” located later in this section to connect the unit.

Vertical Installation

To install the Wireless Ethernet Bridge vertically, as shown in the illustration below:



1. Insert the Wireless Ethernet Bridge into the supplied base. Ensure that the antenna's location is on top, because the antenna prevents the unit from fitting into the base. The Wireless Ethernet Bridge's foot slides snugly into the base to keep the unit stable.
2. Follow the procedures in "Electrical Connection to Wireless Ethernet Bridge" located later in this section to connect the unit.

Wall Mount Installation

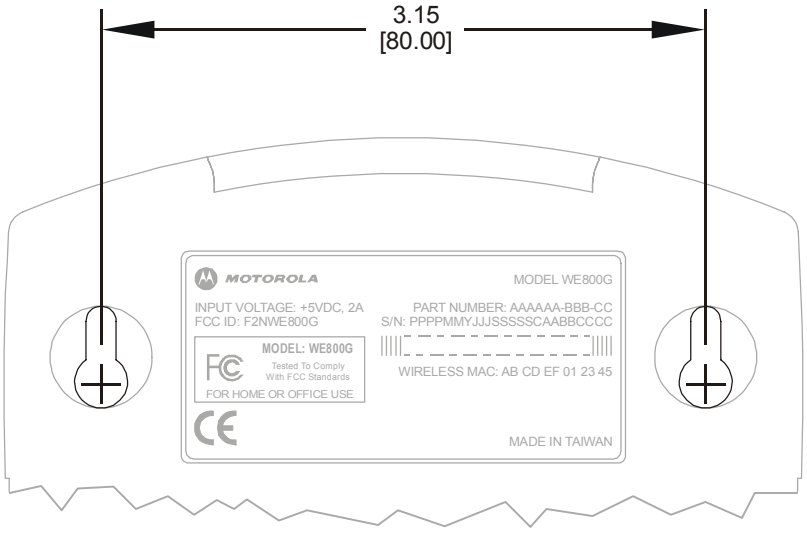
To mount the Wireless Ethernet Bridge on the wall, you must:

- 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 Wireless Ethernet Bridge to concrete, masonry, a wooden stud, or other 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.

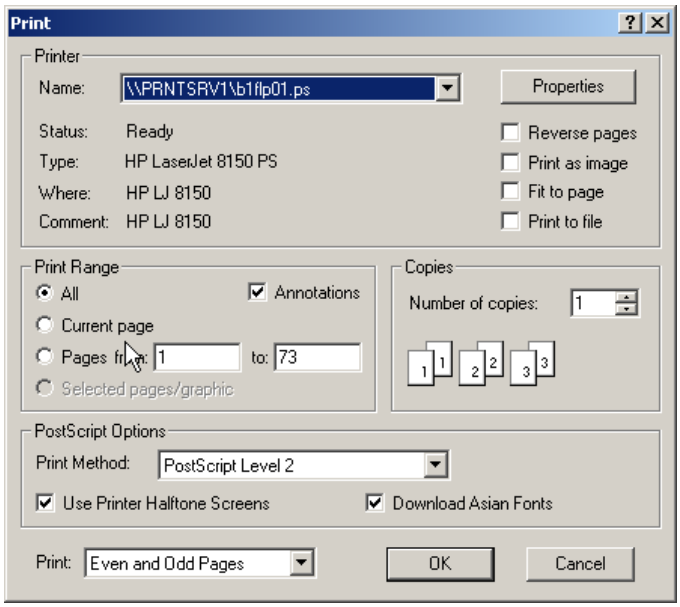
To mount your Wireless Ethernet Bridge on the wall:

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 appears below.)



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!

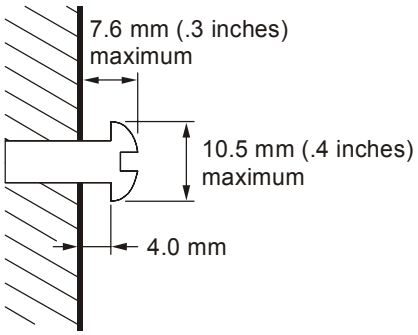
Before drilling holes, check the structure for potential damage to water, gas, or electric lines.

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 Wireless Ethernet Bridge down until it stops against the top of the keyhole opening.

13 Follow the procedures in “Electrical Connection to Wireless Ethernet Bridge” located later in this section to connect the unit.

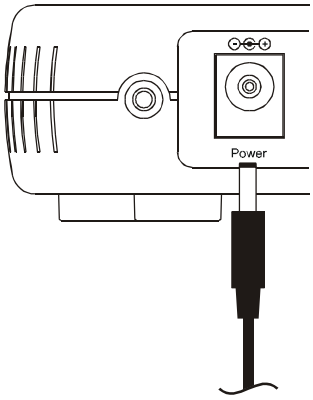
Electrical Connection to Wireless Ethernet Bridge

Your Wireless Ethernet Bridge does not have an On/Off power switch and will only be powered on by plugging in the power adapter. To make the electrical connection to the Wireless Ethernet Bridge:

CAUTION!

Use only the Motorola supplied WE800G power adapter.

1 Connect the power adapter to the Wireless Ethernet Bridge's Power port, found on the back of the unit:



To power supply (5V / 2A)

2 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 describes the physical connection of the Wireless Ethernet Bridge to your network as well as the configuration needed by your PC.

To set up your wireless network:

- Physically connect and power on the Wireless Ethernet Bridge
- Configure your PCs
- Enter Wireless Security settings

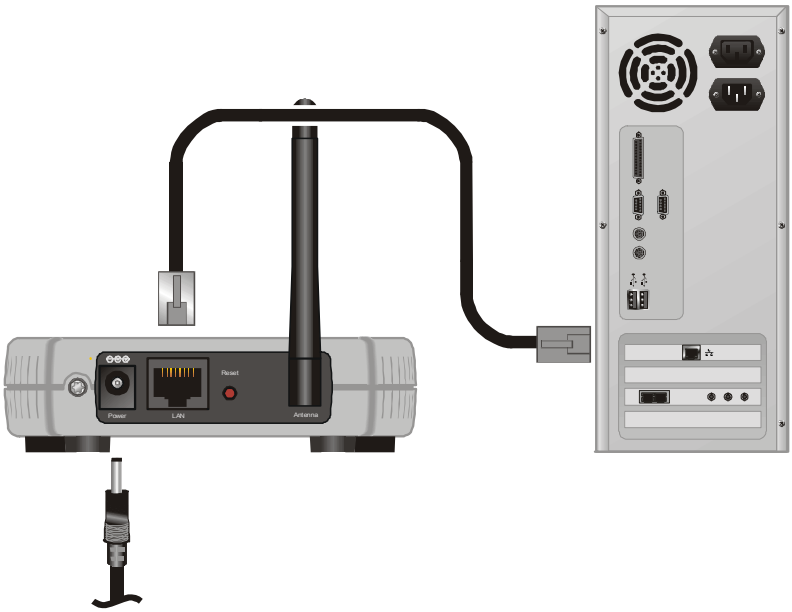
If you don't want to use the Installation Wizard from the CD-ROM, follow the instructions below. For advanced configurations, refer to *Section 3:Configuration*.

Wired Connection to Wireless Ethernet Bridge

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

You need the supplied Ethernet cable to connect the PC to the Wireless Ethernet Bridge.

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 Wireless Ethernet Bridge:



You are now able to configure the Wireless Ethernet Bridge.

2 To configure the Wireless Ethernet Bridge, please refer to *Section 3:Configuration*.

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

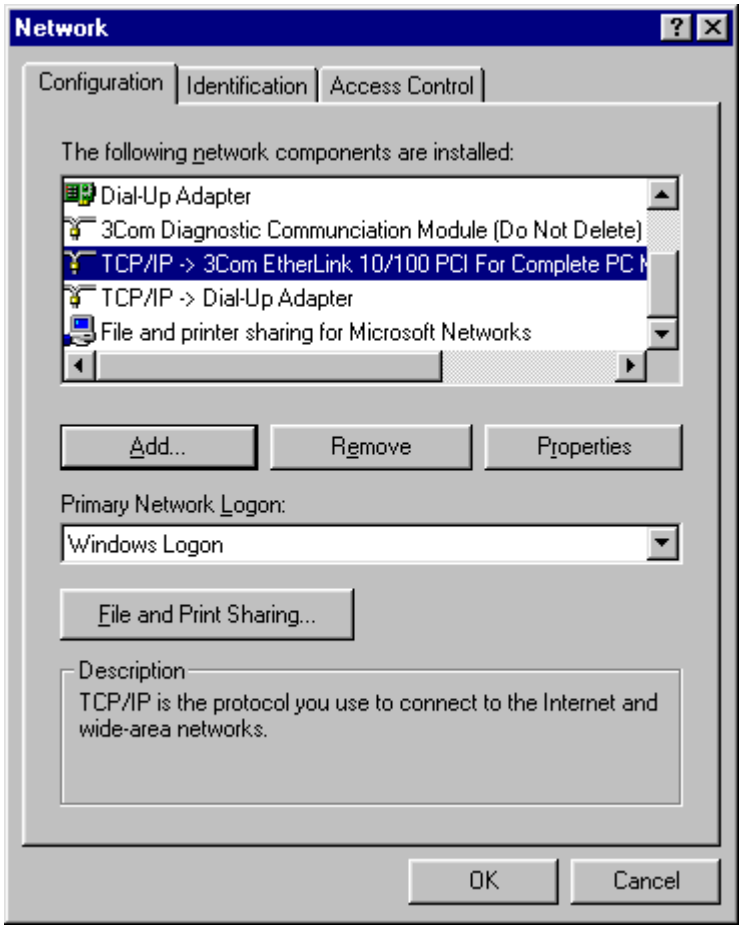
Determine the operating system for each computer you are including in your wireless network and follow the steps to configure the network settings for that PC.

Configuring Windows 98SE and ME

1 Click **Start**.

2 Select Settings > Control Panel.

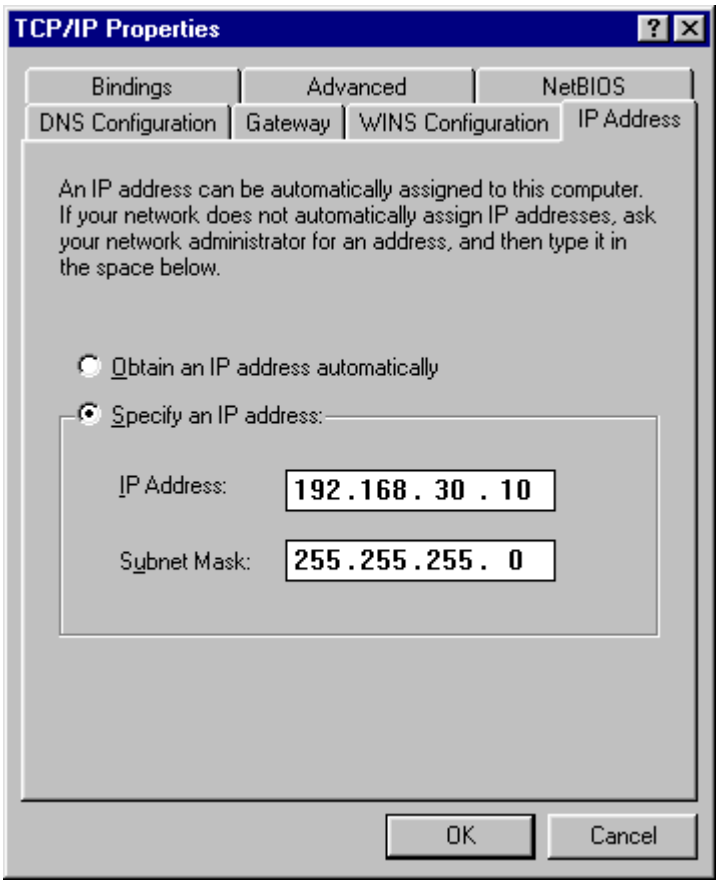
3 Double-click **Network**. The Network window is displayed:



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 **192.168.30.1** into the IP Address field.

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

9 Click **OK**.

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

11 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.

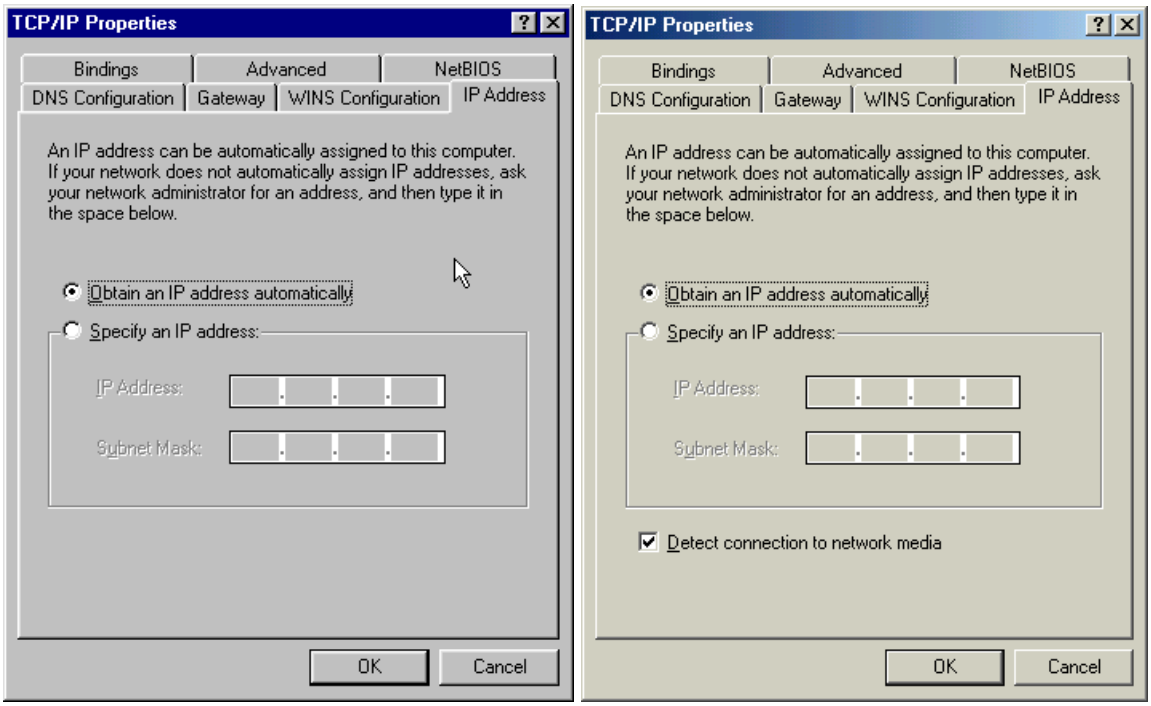
12 **Restart** your computer to save your settings.

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

Windows 98 and ME DHCP Server Configuration

After your initial configuration has been completed, you may need to setup your PC for using a DHCP server, using the procedure below.

1 Follow Steps 1 through 6 from above.



Windows 98SE **Windows ME**

2 Select **Obtain an IP address automatically**.

3 Click **OK** and then complete the procedure by following steps 10 through 12.

Configuring Windows 2000

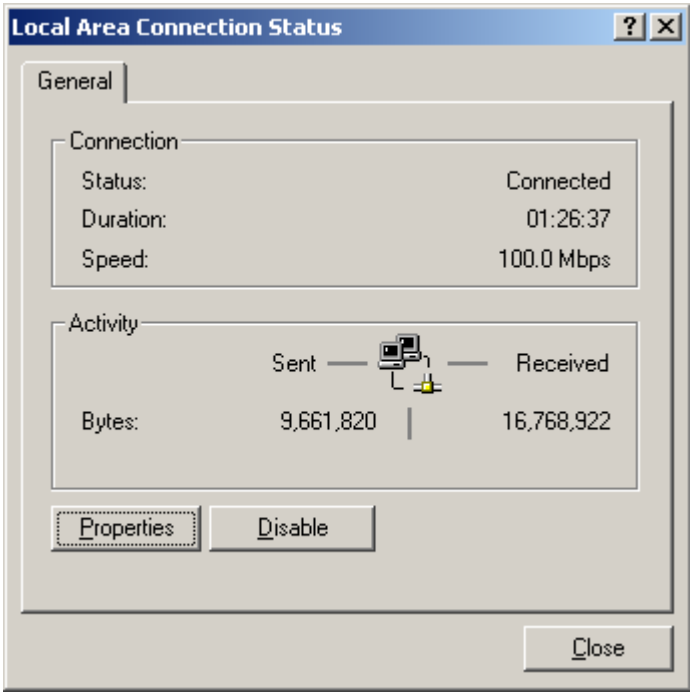
1 Click **Start**.

2 Select **Settings**.

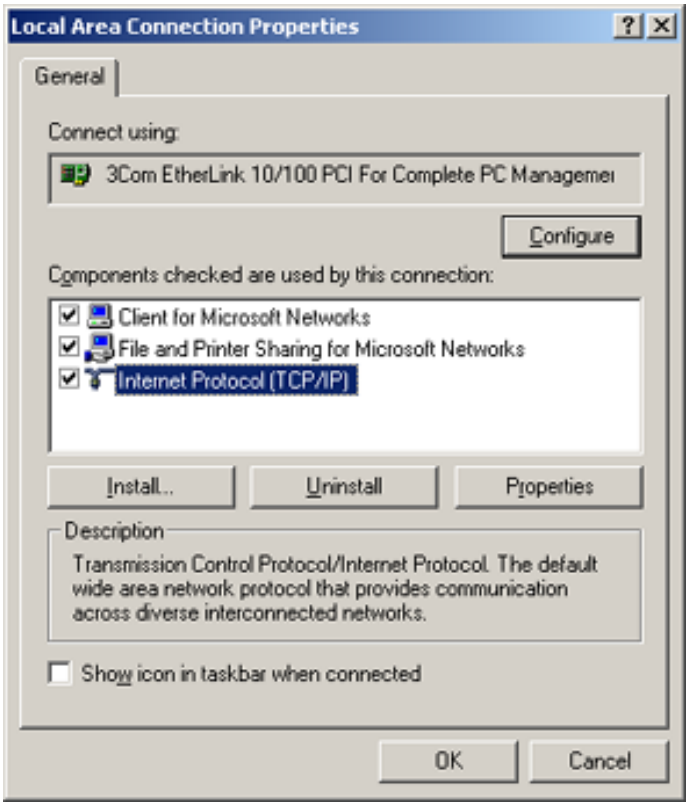
3 Select **Control Panel**.

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

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

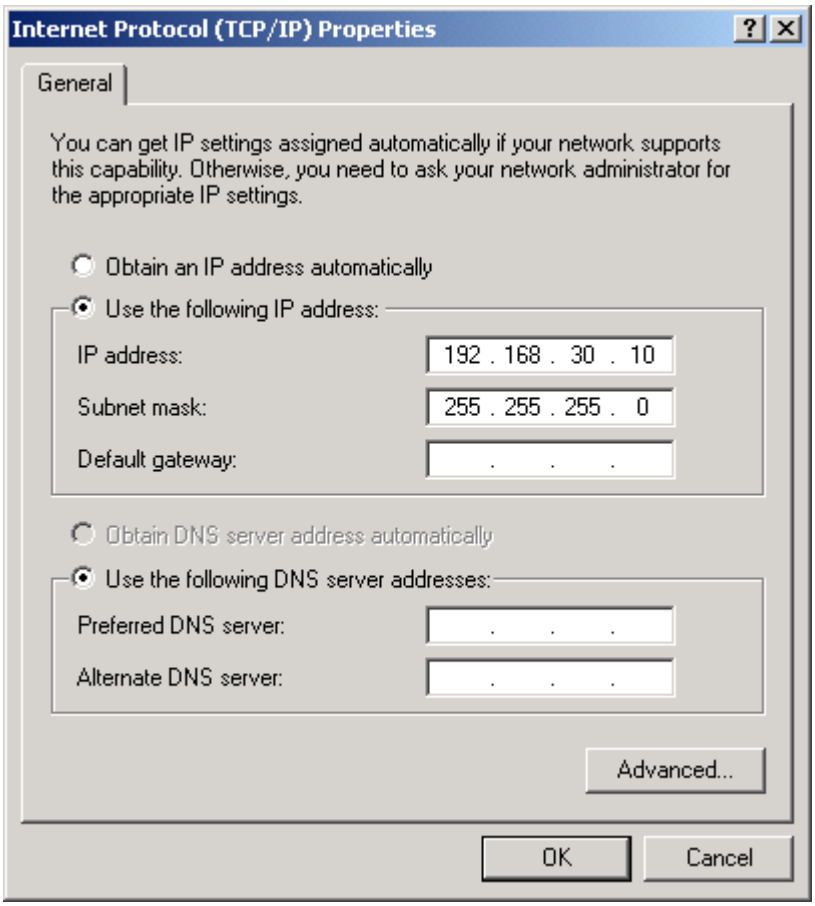


6 Click the **Properties** button.



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 **192.168.30.10** into the IP Address field.

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

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

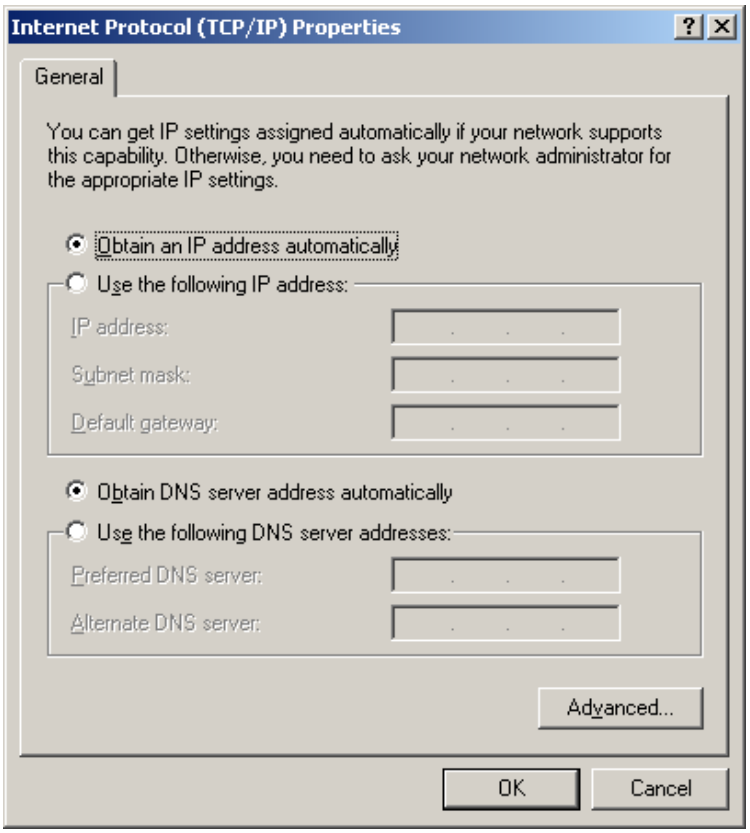
12 **Restart** your computer to save your settings.

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

Windows 2000 DHCP Server Configuration

After your initial configuration has been completed, you may need to setup your PC for using a DHCP server, using the procedure below.

1 Follow Steps 1 through 8 from above.



2 Select **Obtain an IP address automatically**.

3 Click **OK** and then complete the procedure by following steps 11 and 12.

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.

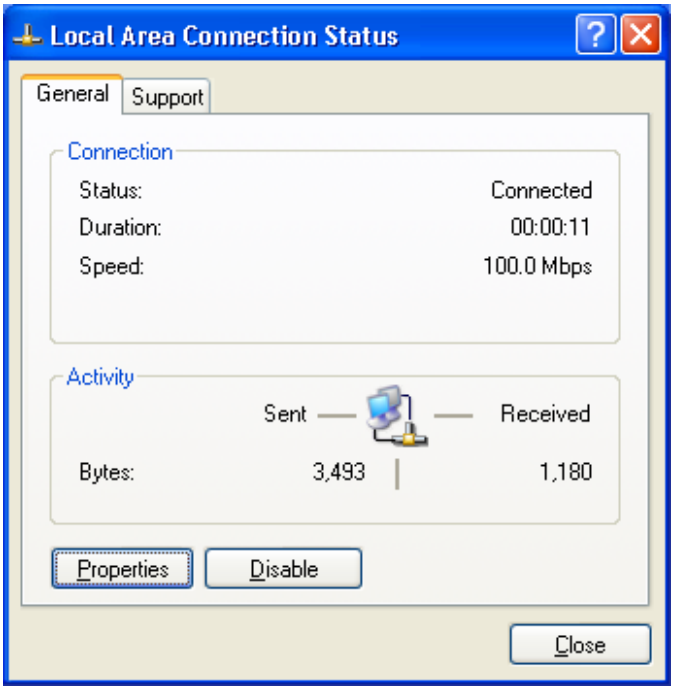
1 Click **Start**.

2 Select **Settings**.

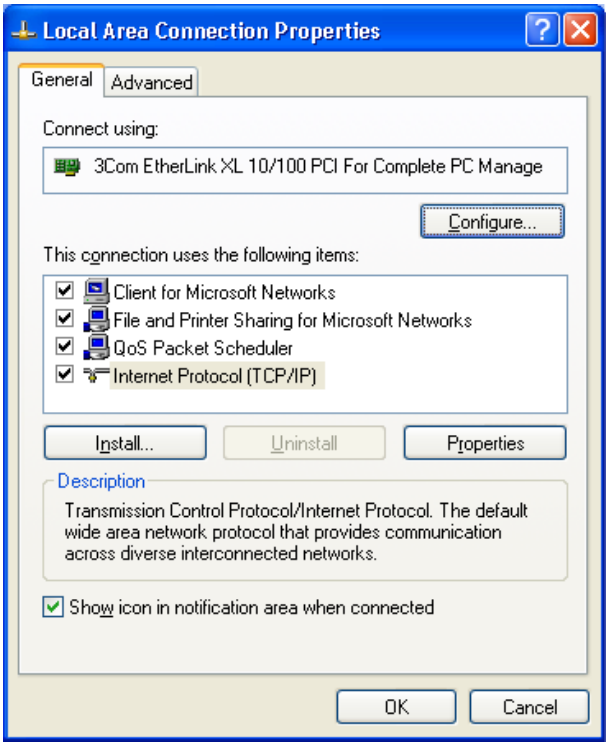
3 Select **Control Panel**.

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

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

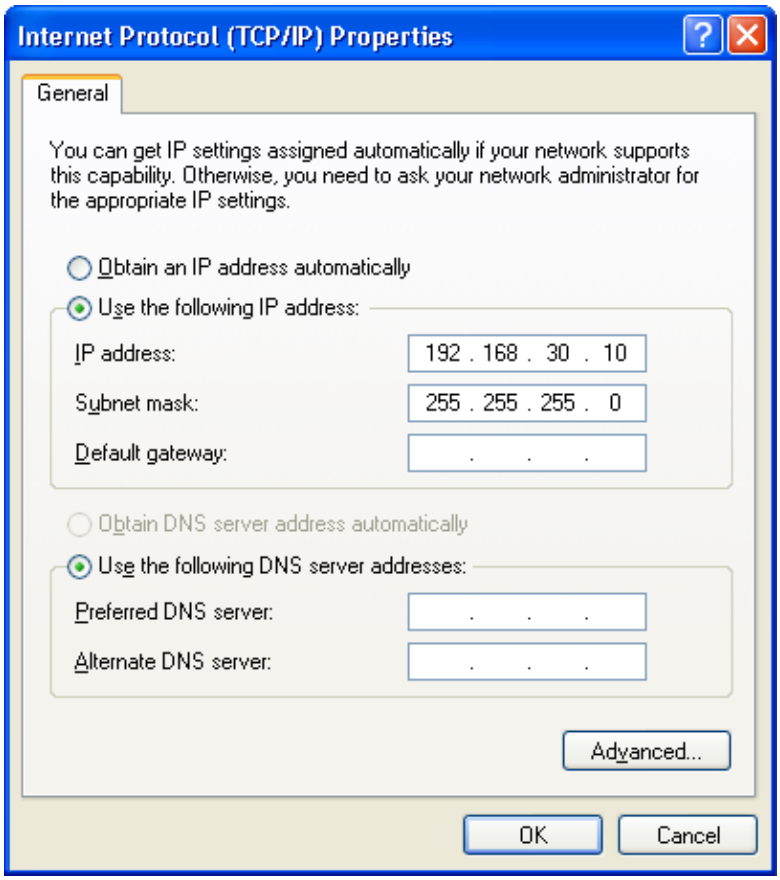


6 Click the **Properties** button.



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 **192.168.30.10** into the IP Address field.

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

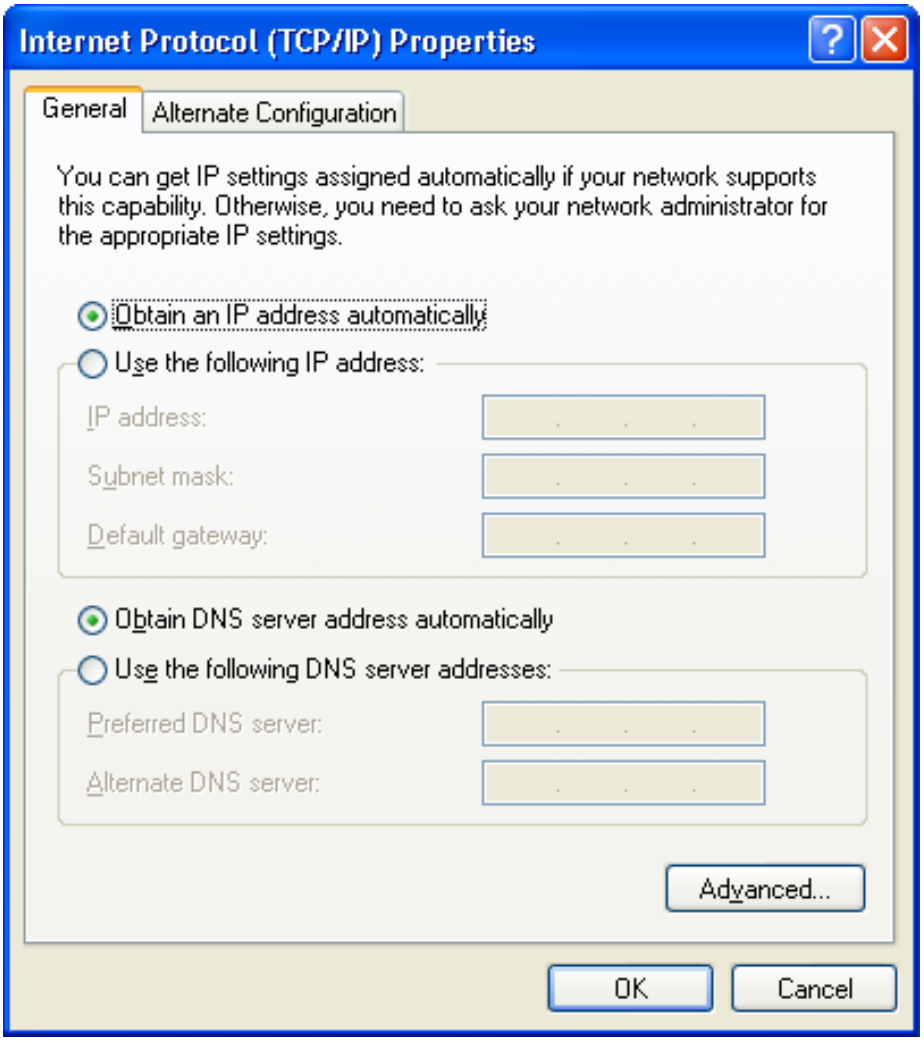
11 Click **OK** twice to exit and save your settings.

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

Windows XP DHCP Server Configuration

After your initial configuration has been completed, you may need to setup your PC for using a DHCP server, using the procedure below.

1 Follow Steps 1 through 8 from above.



2 Select **Obtain an IP address automatically**.

3 Click **OK** and then complete the procedure by following step 11.

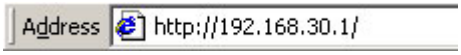
Configure Your Wireless Security Settings

Due to the limitation of the Wi-Fi WPA Test Plan, your Wireless Ethernet Bridge'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 possible, connect your computer with an Ethernet cable to the Wireless Ethernet Bridge and not wirelessly. If you log into the Wireless Ethernet Bridge 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 Wireless Ethernet Bridge is safe.

1 Once the Wireless Ethernet Bridge is connected, open your web browser. Enter into the URL field **http://192.168.30.1** (the Wireless Ethernet Bridge'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.

After 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 Wireless Ethernet Bridge's Web-based Configuration Utility.

Wireless Security Setup

Follow these procedures to setup the correct security protocols for your Wireless Ethernet Bridge.

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

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

3 In the Login Password field, enter in the desired ***PASSWORD***. For strong security, select an ID that contains multiple of case-sensitive characters as well as numbers and symbols like "**_ +)**". It cannot be longer than 64 bytes.

4 In the Password Confirm field, 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 Select a Profile and navigate to the **Basic** tab.

8 Enter the ***Network ID (SSID)*** to match the SSID of the network and click **APPLY**. Or, if using in Ad-Hoc mode, enter a ***user friendly SSID***, which will be used by your client adapter.

9 Navigate to **Security**.

10 Select **Pre-Shared Key (PSK)** from the drop down list of ESS Auth Mode.

11 Select **WEP128** from the drop down list of Encryption Status.

12 Click **APPLY** and click **RESTART** again. Your wireless configuration is now complete for the selected Profile.

Section 3:Configuration

You can use the information in this section to modify the Wireless Ethernet Bridge's 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 After the Wireless Ethernet Bridge is connected, open your web browser. Enter into the URL field the Wireless Ethernet Bridge's IP address. The default is **http://192.168.30.1** (the Wireless Ethernet Bridge's default IP address). Press the **Enter** key.

The login screen appears.

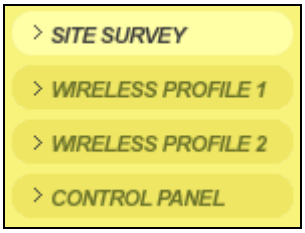
2 Enter the ***USER ID***. The default factory setting is "admin", without the quotation marks.

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

4 Click **LOG IN** to enter the Wireless Ethernet Bridge's **Web-based Configuration Utility**.

Navigation

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



- Site Survey
- Wireless Profile 1
- Wireless Profile 2
- Control Panel

To navigate, click on a major section and then the associated subsection. For example, to set the security profile for Profile 1, click **WIRELESS PROFILE 1** on the left, then the **BASIC** 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 Log Out

Click the appropriate command to execute the action.

HELP	If assistance is required in using the Wireless Ethernet Bridge, 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 your convenience, you should finish all your configuration changes and then restart the unit.**
LOG OUT	To log out of the Wireless Ethernet Bridge's Configuration Utility, click **LOG OUT**.

Active Profile and Site Monitor

These screens enable you to configure your Wireless Ethernet Bridge for different wireless scenarios and to search for Access Points (APs).

- Active Profile
- Site Monitor

Site Survey – Active Profile

This is the first screen that appears when logging into the web-based utility. It enables you to select the Profile you want to use. A Profile enables you to configure your unit for different wireless networks.

For example, if you need to switch between a home network and a friend's network, you can configure a Profile for each network. Or, if you need to setup a temporary wireless network at a tradeshow, then the extra Profile enables you to maintain your primary settings.

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

Field or Button	Description
Active Profile Selection	Select the Profile you want to enable. The Profile selected here activates the settings of Wireless Profile 1 or 2.
Mode	Enables you to select the type of transmission protocol your wireless network uses. The default is Auto. The options are: ▪ Auto (802.11b and 802.11g) ▪ G Only (802.11g only) ▪ B Only (802.11b only)

Site Survey – Site Monitor

This screen displays information about wireless Access Points (AP) and stations, and their associated information. The settings displayed here help you to configure the Ethernet Bridge appropriately.

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

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

SCAN

Type	SSID	MAC Address	Channel	Signal Strength	Wireless Mode	Security
Infra	motorola	00:06:F4:00:CC:AA	6	53%	802.11b/g	None
Infra	motorola	00:08:0E:D3:02:85	1	35%	802.11b/g	None

Field or Button	Description
Scan	Click to search for more access points/routers.
Type	Network Type - either Infrastructure (Infra) or Ad-Hoc is displayed.
SSID	The SSID of the device found.
MAC Address	The MAC address of the device found.
Channel	The channel on which the device is broadcasting.
Signal Strength	The Signal Strength of the device found.
Wireless Mode	The protocol used, 802.11b or 802.11g.
Security	The security protocol used.

Configuring Wireless Profile 1 or 2

The Wireless Profile 1 or 2 screens enable you to adjust settings for your wireless connection for a specific wireless profile. Refer to each subsection for further descriptions. These include:

- Basic
- Security
- Advanced
- Professional

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.

To access the screen, click **Wireless Profile 1** or **2** > **Basic**.

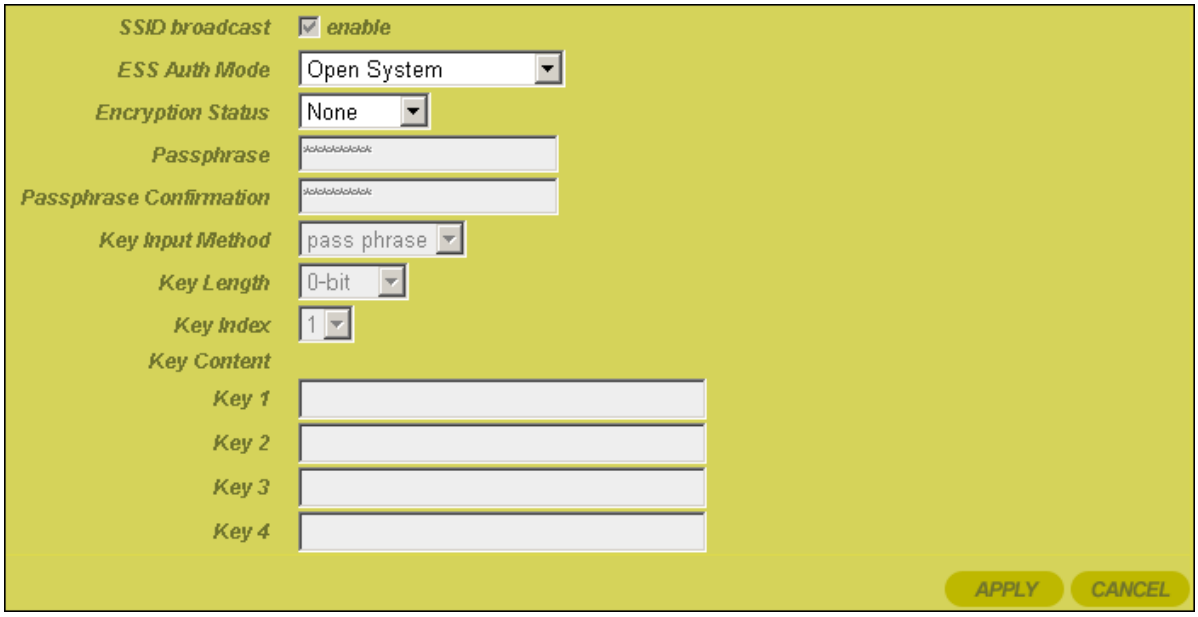
Click **APPLY** to save your settings or **CANCEL** to cancel changes.

Field or Button	Description
Network ID (SSID)	Enter a Network ID (SSID) of no more than 32 alphanumeric characters. The same SSID has to be entered on every wireless device on your wireless network. The default SSID is empty.
Network Type	Type of network. For a discussion of Network Types, refer to Section 1:Type of Networks. The options are: ▪ Infrastructure ▪ Ac-Hoc

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 Profile 1** or **2** > **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 Wireless Ethernet Bridge to devices on your network. This option is only available when Ad-Hoc is enabled. This enables wireless clients, like a laptop, to receive the Wireless Ethernet Bridge's SSID and then join the Ad-Hoc network. If you don't want the SSID to be broadcast, disable this feature. The default is enabled.

Field	Description
ESS Auth Mode	*Extended Service Set (ESS*) Authentication Mode. 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 the AP you are trying to associate with will not verify the identification of your unit. Pre-Shared Key (PSK) — The Pre-Shared Key (PSK) authentication method is used. You need to share the same key between your AP and client. Select the option that best meets your needs. Shared Key is the best choice as it provides the stronger security. The default is Open System.
Encryption Status	Determines the type of security encryption algorithms for the Key Index. The security setting encrypts your wireless transmission. 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) Select the option that best matches your needs. Motorola recommends using WEP128 because it provides a stronger security algorithm. The default is None.

Field	Description
Passphrase	Enter the Passphrase to be used for Key encryption. This is the Passphrase used by other Access Points (AP), so you must enter the same phrase for all of the Motorola client devices on your wireless LAN. The Passphrase must be between 8 and 63 characters.
Passphrase Confirmation	Enter the Passphrase again.
Key Input Method	Available if Shared Key in ESS Auth Mode is selected. The options are: ▪ Passphrase ▪ Hexadecimal ▪ ASCII If you select either Passphrase or Hexadecimal, the format of the Key appears in a hexadecimal format. The Passphrase is determined by the password entered in the Passphrase filed. *If you are using other non-Motorola wireless products with Shared Key (PSK) enabled, you may need to 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 Passphrase.
Key Length	This is only available when ESS Auth Mode is set to Pre-Shared Key (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 ESS Auth Mode or Encryption Status fields. You are selecting one of the Key Content fields below. The Key selected here must match between the WE800G and the AP in Infrastructure mode and other clients in Ad-Hoc mode. For example, if you select Key 1 here you have to match Key 1 of the AP. 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 Key Input Method field. For the key content, the phrase is auto-generated by the password entered in the Passphrase field. For non-Motorola clients, you will use these Keys (and not Passphrase) 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.*

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.

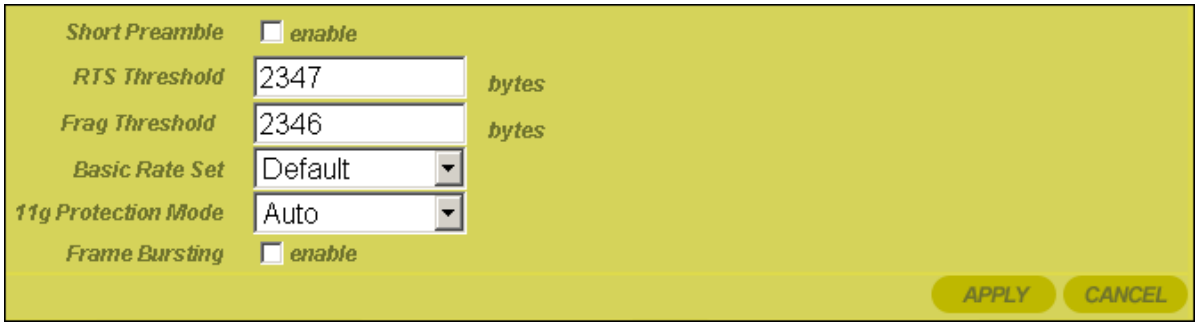
To access screen, click **Wireless Profile 1** or **2** > **Advanced**. Click **APPLY** to save your settings or **CANCEL** to cancel changes.

Field	Description
Radio Interface	Enables you to turn on and off the wireless feature. The default is enabled.
MAC Address	Displays the MAC address of the unit.
Country Code	Displays the country code.
Channel Number	This selection is only available in Ad-Hoc mode. Select the channel number on which the device will broadcast.

Wireless – Professional

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 Profile 1** or **2** > **Professional**. Click **APPLY** to save your settings or **CANCEL** to cancel changes.



Field	Description
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 access point 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 and click **APPLY** to save the setting.
Frag 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 and click **APPLY** to save the setting.

Field	Description
Basic Rate Set	The Wireless Ethernet Bridge broadcasts different transmission rates so clients know which transmission rate to use to join the network. The Mode selected on the Site Survey > Active Profile tab determines this setting. You can also alter the setting here. The default is Default. The options are: **All** — Ensures compatibility with all devices. **Default** — Ensures compatibility with 802.11b or 802.11g devices **1 to 2 Mbps** — The slowest speed available.
11g Protection Mode	Ensures that your Wireless Ethernet Bridge 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 co-exist in the network. The default is Auto. The options are: **Disabled** — 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
Frame Bursting	Frame Bursting enables you to send more frames (collection of packets) within a given time period. This feature works with other Motorola products to increase performance throughput. The default is disabled.

Configuring Control Panel Settings

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

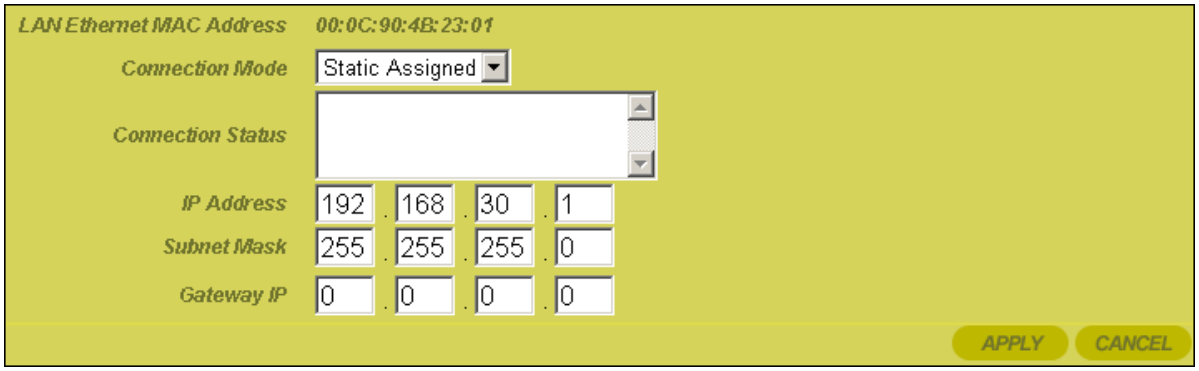
The following screens are available in Control Panel:

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

Control Panel – Network Address

This screen enables you to view the LAN Ethernet MAC Address and select a connection mode.

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



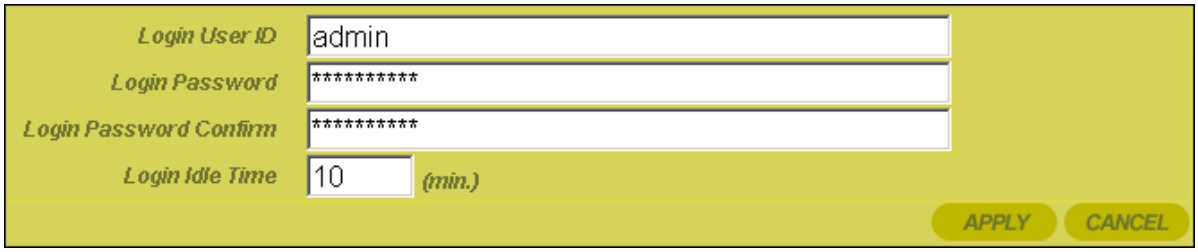
Field	Description
LAN Ethernet MAC Address	Displays the MAC address used for accessing a Local Area Network (LAN). This is the Ethernet MAC address of the unit.

Field	Description
Connection Mode	Select a connection mode. The options are DHCP or Static Assigned.
Connection Status	Provides current information about the connection status of the Wireless Ethernet Bridge.
IP Address	This is the IP address you use to connect to the unit. If connecting to a DHCP server, the IP address will appear here. If using Static Assignment, enter the IP address here.
Subnet Mask	This is the Subnet Mask address you use to connect to the unit. If connecting to a DHCP server, the Subnet Mask address will appear here. If using Static Assignment, enter the Subnet Mask address here.
Gateway IP	This is the Gateway IP address the device will use to connect back to you. If connecting to a DHCP server, the Gateway IP address will appear here. If using Static Assignment, enter the Gateway IP address here.

Control Panel – Device Security

This screen enables you to change your User ID and password and enables you to manage your Wireless Ethernet Bridge remotely.

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



Field	Description
Login User ID	Changes the User ID used for logging into the Wireless Ethernet Bridge'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 Wireless Ethernet Bridge'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 Login Password.
Login Idle Time	The amount of idle time (no actions occur) that elapses before the Wireless Ethernet Bridge automatically logs off the user. The default is 10 minutes.

Control Panel – Firmware Update

This screen enables you to update the firmware (Wireless Ethernet Bridge'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 **Control Panel** > **Firmware Update**.

To update the firmware:

1. Access this website www.motorola.com/broadband/networking.
2. Download the latest file to your computer.

3 Click **Control Panel** > **Firmware Update**.

4 Locate the file you downloaded, by typing the path to the file or clicking **Browse** and navigating to it.

5 Click **UPDATE** to update the Wireless Ethernet Bridge with the selected firmware file.

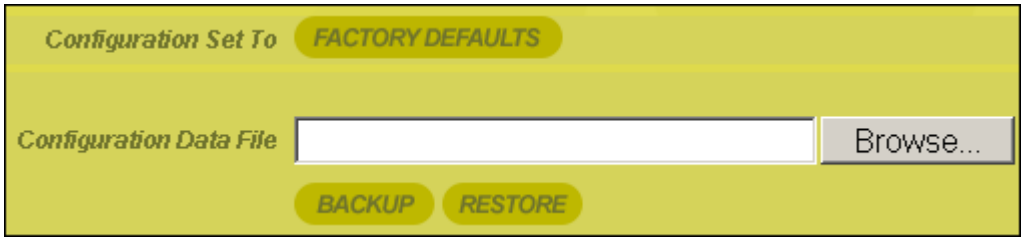
6 The Wireless Ethernet Bridge will inform you that you successfully updated the unit.

7 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 Wireless Ethernet Bridge, to a file. You are also able to reset the Wireless Ethernet Bridge to the factory default settings.

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



To reset the Wireless Ethernet Bridge 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 navigating to it.

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

Section 4:Troubleshooting

This section details possible solutions to problems that might occur when using the Wireless Ethernet Bridge WE800G.

Contact Us

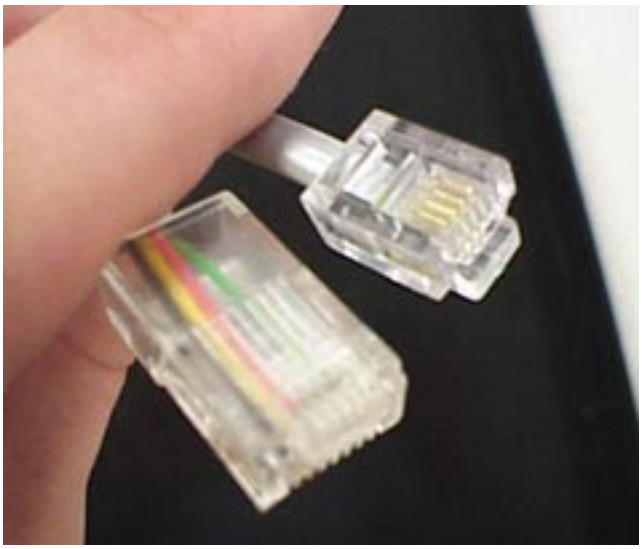
If you are unable to locate a solution here, please access our website at www.motorola.com/broadband/networking for the latest information. You can also reach us 7 days a week, 24 hours a day at 1-877-466-8646.

Hardware Solutions

My computer is experiencing difficulty connecting to the wireless network.

- Ensure that your wireless access point/wireless router is powered on and that the Wireless LED is lit.
- Check your cable connections to ensure they are tight and secured.
- 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 WE800G and your computer. 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.

- 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 WE800G. Also in Start > Settings > Control Panel > Network and Dial-Up Connections, you can examine the state of your Ethernet connection with the WE800G. Make sure “Show icon in task bar when connected” is checked.
- Ensure that your WE800G is within range of your wireless access point/wireless router or is not behind an obstruction. For example, metal structures may interfere with the signal, as will 2.4 GHz cordless phones, and microwaves.
- Ensure that your wireless access point/wireless router’s antenna and your WE800G antenna are connected.

Software Solutions

I cannot access the Configuration Utility for the unit.

- Verify your Ethernet connection to the WE800G.
- Verify that you are using the correct version of Internet Explorer or Netscape (Internet Explorer must be above version 5.2).
- Verify that the IP address of the PC being used to configure the router is on the same network as the router's configuration IP address. The default IP address of WE800G is 192.168.30.1. If after initial set up, the PC that's used to configure the WE800G has been assigned a different IP address by DHCP or assigned a different static IP address which is not on the same 192.168.30.x network, it may be necessary to do one of the following two things:
  - If the WE800G configuration utility needs to be accessed "on-the-fly". Write down the PC's current IP address. Temporarily change the PC's IP address to static 192.168.30.10 (or something similar). Log into the WE800G. Set the WE800G's network address to DHCP or to a static address that will be on the same network as the PC's current IP address and not a duplicate of any others on the network. Record the new WE800G IP address (in case of DHCP, it can be retrieved from the access point/wireless router after the WE800G has restarted.) Restore the PC's IP configuration. Use the recorded new WE800G IP address to access the WE800G configuration utility.
  - If the WE800G configuration utility only needs to be accessed occasionally: Temporarily change the PC's IP address to static 192.168.30.10 (or something similar). Log into the WE800G. After configuring the WE800G, log out. Restore the PC's IP configuration.
- Verify you are entering the correct URL in the browser. The default is http://192.168.30.1. If you think you have changed the IP address used to configure the WE800G 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 WE800G user settings, including User ID, Password, IP Address, and Subnet mask.
- Once the WE800G is reset to factory default, re-verify the Ethernet connectivity and IP address issues.

My WE800G cannot associate with the wireless access point/router.

- Ensure that your WE800G and the wireless access point/wireless router have the same security settings that enable your computer to access the wireless network. Section 2: Configure Your Wireless Security Settings describes how to adjust security settings. Some of the key settings are:
  - ESS Auth Mode (Open versus Pre-Shared Key (PSK))
  - Encryption status (none, 64WEP, 128WEP)
  - Content of Passphrase if the Passphrase option is selected
  - Active key (1-4 for 64WEP, 1-2 for 128WEP)
  - Actual key value for the current active key
  - SSID. The WE800G must have the exact SSID as the wireless access point/wireless router. For Motorola wireless access points or wireless routers, the default SSID is “motorola xyz”, where “xyz” is the last three digits of the wireless access point/wireless router’s MAC address. The SSID is case sensitive. Make sure there are no trailing spaces.

  The WE800G must be set to match the wireless access point/wireless router for those settings
- As a suggestion, it may be easier to set the wireless access point/wireless router’s security to open system and no encryption and set the WE800G accordingly. After making sure the WE800G can work under this condition, turn on the security features on the wireless access point/wireless router and then turn on the security features on the WE800G and try again.

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 the configuration information that came with your router.

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:

Connectionspecific DNS Suffix.: Example.example.example.com.

IP Address. . . . . . . . . . . : 192.168.30.2

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

Default Gateway . . . . . . . . . : 192.168.30.1
```

3 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 192.168.30.1**.

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, 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 192.168.30.1**.

- 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 by referring to documentation that came with your wireless access point/wireless router.
- 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.

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

DDNS

Dynamic Domain Name System enables you to assign a fixed host and domain name to a dynamic Internet IP address. It is used when you are hosting your own web server, FTP server, or another server behind the router.

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 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.

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 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 to a device 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*.

UPnP

Universal Plug and Play

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.

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

494160-001
07/03

MGBI