

User Guide

WR850 Wireless Broadband Routers WR850GP and WR850G



WR850G



WR850GP

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/adaptor 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.

Canadian Compliance

This Class B digital apparatus meets all requirements of the Canadian Interference Causing Equipment Regulations. Cet appareil numérique de la classe B respecte 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 and WR850GP, WA840G and WA840GP comply with 47 CFR Parts 2 and 15 of the FCC Rules as a Class B digital device. This device complies with Part 15 of FCC Rules. Operation of the device is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference that may cause undesired operation.

Copyright © 2004 Motorola, Inc.

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

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

MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. Microsoft, Windows, Windows Me, Windows XP, DirectX, MSN, and NetMeeting are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Microsoft Windows screen shots are used by permission of Microsoft Corporation. Wi-Fi is a registered trademark of Wireless Ethernet Compatibility Alliance, Inc. AOL is a registered trademark and Instant Messenger is a trademark of America Online, Inc. QuickTime is a registered trademark of Apple Computer, Inc. Net2Phone is a registered trademark of Net2Phone, Inc. Battle.net is a registered trademark of Blizzard Entertainment. Unix is a registered trademark of The Open Group. The following websites are not sponsored, affiliated, or controlled by Motorola: www.dyndns.org, www.changeip.com, and www.ntp.org. All other product or service names are the property of their respective owners.

Contents

Section 1: Overview

Understanding Your User Guide	1-3
Box Contents	1-3
Understanding Functions	1-4
Router	1-4
LAN	1-4
TCP/IP	1-4
<i>Static IP Address</i>	1-4
<i>Dynamic IP Address</i>	1-5
DHCP Server	1-5
Sample Home Network Diagram	1-6
Positioning Your Router	1-6
Wireless Range	1-7
Technical Specifications	1-7
Router Physical Description	1-8
Back of Router	1-8
Front of Router	1-9
LED Description	1-10

Section 2: Installation

Hardware Setup	2-1
Antenna Installation	2-1
Router Physical Installation.....	2-2
<i>Horizontal Installation</i>	2-2
<i>Vertical Installation</i>	2-2
<i>Wall Mount Installation</i>	2-3
Electrical Connection to Router.....	2-6
Easy Software Setup	2-6
Manual Software Setup	2-6
Wired Connection to Router.....	2-7
Wireless Connection to Router	2-8
Configure Your Computers	2-9
<i>Configuring Windows 98SE and ME</i>	2-10
<i>Configuring Windows 2000</i>	2-12
<i>Configuring Windows XP</i>	2-15
Configure Your Wireless Security Settings	2-18
<i>Logging In</i>	2-18
<i>Wireless Security Setup</i>	2-19

Configure Your Basic Internet Settings	2-20
DHCP Configuration	2-20
PPPoE	2-20
Static IP	2-21
PPTP	2-21

Section 3: Configuration

Using the Configuration Utility	3-1
Logging In	3-1
Navigation	3-2
Help, Restart, and Logout	3-2
Configuring Internet Settings	3-3
Basic Internet Settings	3-3
Advanced Internet Settings	3-7
Troubleshooting Your Network Connections	3-8
Configuring Wireless Network Settings	3-9
Basic Wireless Configuration	3-9
Configuring Wireless Security Settings	3-11
Monitoring Wireless Access Points	3-16
Advanced Wireless Configuration	3-18
Configuring Parental Control Settings	3-21
Parental Control - Content Policy	3-21
Parental Control - URL Log	3-23
Configuring Networking Settings	3-25
Configuring DHCP Server Settings	3-25
Configuring the Router Host Name	3-28
Configuring Network Router Settings	3-28
Configuring DDNS Settings	3-30
Configuring NAT Settings	3-31
Configuring Port Trigger Settings	3-32
<i>Sample Port Trigger Entries</i>	<i>3-33</i>
Configuring Virtual Server Settings	3-34
Configuring the Firewall	3-35
Configuring Control Panel Settings	3-37
Configuring Device Security	3-37
Updating Firmware	3-38
Saving and Restoring Configuration Settings	3-39
Configuring Time Settings	3-40
Configuring UPnP	3-41
Enabling Event Logs	3-41

Section 4: Troubleshooting

Contact Us	4-1
Hardware Solutions	4-1
<i>My computer is experiencing difficulty in connecting to the router.....</i>	<i>4-2</i>
<i>My broadband modem already uses a built-in router.....</i>	<i>4-2</i>
Software Solutions.....	4-3
<i>I would like to test to see if my Internet connection is live.</i>	<i>4-3</i>
<i>I cannot access the Configuration Utility for the router.</i>	<i>4-4</i>
<i>How do I extend my wireless network to cover more area?</i>	<i>4-4</i>
<i>I cannot browse past the first screen of the Configuration Utility.....</i>	<i>4-4</i>
<i>What if Pass Phrase isn't supported? What do I enter for my security?.....</i>	<i>4-5</i>

Section 5: Glossary _____ 5-1

Section 1: Overview

Congratulations on purchasing the Motorola WR850GP Wireless Broadband Router or Motorola WR850G Wireless Broadband Router.¹

The WR850 includes both an 802.11b/g wireless access point and a 4-port Ethernet router. So it is both wireless and wired, providing the foundation for a truly customized network full of options.

Using the WR850, you can share files, pictures, peripherals, printers and more with everyone else on the network. By connecting a broadband modem (cable, DSL or other), you can also share a single high speed Internet connection.

The WR850 offers both the popular 802.11b wireless standard as well as the nearly 5-times-faster 802.11g standard, providing 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.

The WR850GP comes loaded with Performance Enhancement technology that accelerates your wireless network and your fun. This new technology boosts wireless performance among compatible Motorola devices up to 35% faster than over standard 802.11g networking.

Upgradeable firmware keeps the router's control software up-to-date. The WR850 captures the latest technology in a package that stays current, protects your home network, and provides you easy home network management.

Wireless Broadband Router WR850GP

Wireless Broadband Router WR850G



¹ Unless otherwise stated, this User Guide will use WR850 as the generic term for both the WR850G and WR850GP

Your wireless router is really several products built into one router:

Wireless Access Point

- Connects your router to your laptop wirelessly and allows you to roam unfettered
- Supports a multitude of devices that operate with both 802.11g and 802.11b wireless communication standards
- Protects your wireless communications using firm WPA, 802.1X, and WEP security algorithms
- Supports peer-to-peer communication using Wireless Distribution System (WDS) mode

4-port Full Duplex 10/100 Ethernet Switch and Router

- Supports wired connection of up to 4 computers or devices
- Shares a broadband Internet (cable, DSL, or other) connection with each of your networked devices
- Enables you to form a Local Area Network (LAN)

Security and Protection

- Firewall protects against Internet intruders
- NAT, IP, and MAC filtering hides your LAN IP addresses and devices from the Internet
- Virtual Private Network (VPN) frees you to connect to your corporate network

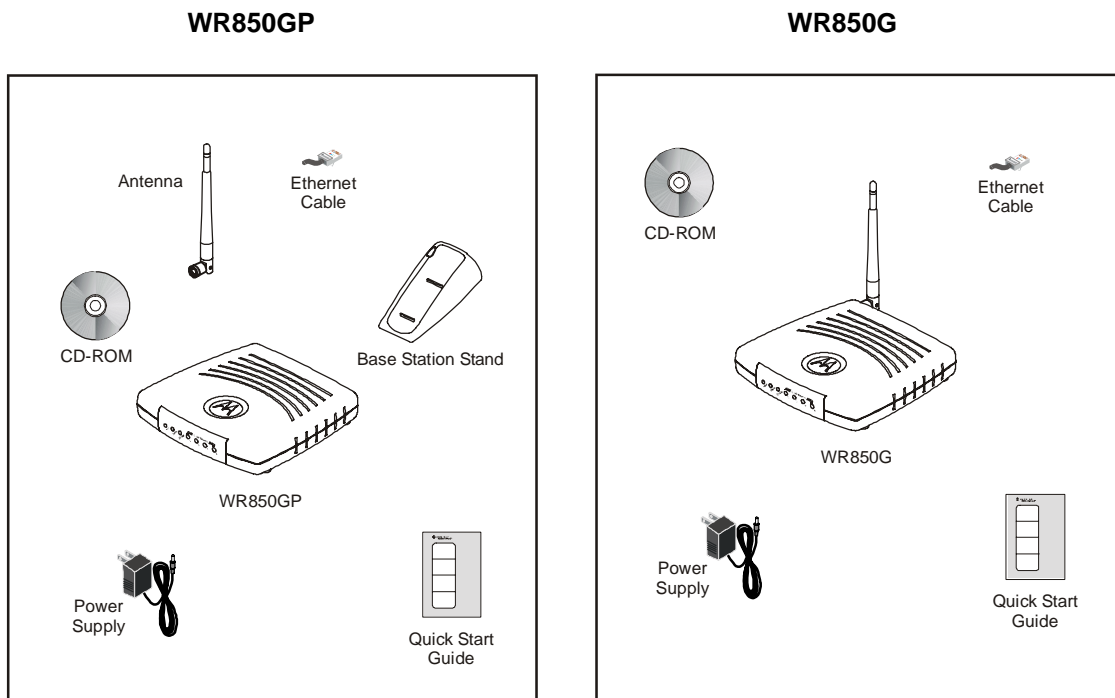
Understanding Your User Guide

The User Guide is divided into the following sections:

- Overview** Describes the router and its functions, the technology used, and the recommended methods for positioning the router.
- Installation** It is assumed that you will use the Installation Wizard on the CD-ROM to set up your router. If not, refer to this section for instructions on getting your router up and running.
- After you have completed this section, your router will be active and ready to work.
- Configuration** Describes the Configuration Utility that manages your router.
- Glossary** List of terms and acronyms.

Box Contents

Your box contains the following:



Understanding Functions

Before installing your wireless router, please take a few minutes to review the wireless networking functions described in this section.

Router

Generally, routers connect two networks together. The WR850 connects your home network with the Internet, which can be thought of as a very large network. Routers provide bandwidth security by keeping data out of your home network.

The router's firewall inspects each packet of data as it flows through the port before delivering it to the appropriate PC. Network Address Translation (NAT) translates one set of IP addresses, usually private, to another set, usually public. This is how your network remains protected and private on the Internet.

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.

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.

If you are using your wireless router to share an Internet connection, your Internet Service Provider (ISP) might have assigned you a static IP address, which you will use when configuring your router. See Section 3: Configuration.

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.

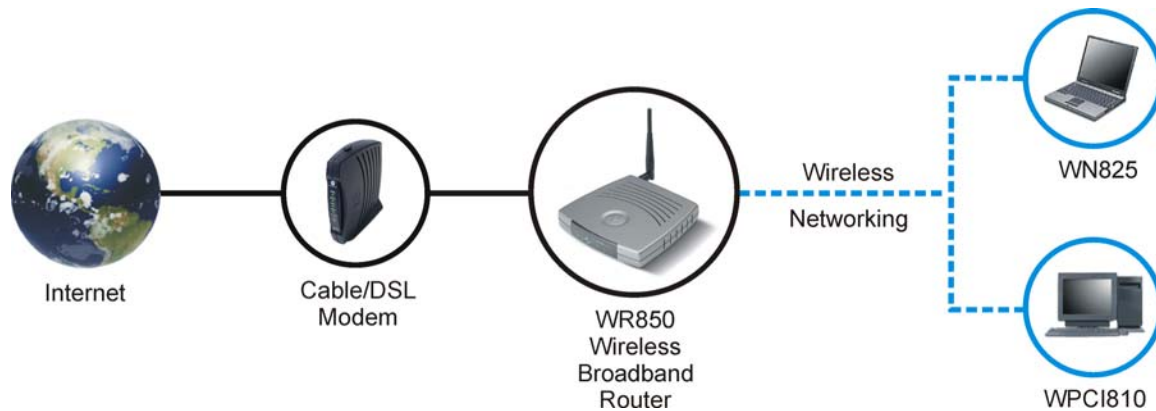
If you are using your wireless router to share an Internet connection, your ISP might have assigned you a dynamic IP address, which you use when configuring your router. See Section 3: Configuration.

DHCP Server

A Dynamic Host Configuration Protocol (DHCP) Server assigns IP addresses to clients connected to the router. A *client* is any wireless device that can connect with your router. The client (PC, gaming device, etc.) is automatically assigned an IP address every time a wireless device is added to your network, which frees you from manually assigning IP addresses.

Sample Home Network Diagram

Your wireless router serves as the centerpiece of your network, allowing you to share files, printers, and the Internet connection. A sample home network is shown below:



The Internet communicates with the modem which in turn communicates with the router. The router acts as the gateway to your network: it sends devices information such as requests for Internet access, file sharing, or multiplayer games. The router controls the information for your network, intelligently routing the information to its required destination while at the same time protecting your network from the public domain.

Positioning Your Router

To achieve the best wireless performance, review these guidelines before deciding where to place your router:

- Placing your base station in the physical center of your network is the best location because the antenna sends out the signal in all directions.
- Placing the router in a higher location, such as on top of a cabinet, helps disperse the signal cleanly, especially to receiving locations on upper stories.
- If possible, position your router so there is direct line of sight between the router and your other home network devices.
- Avoid placing the router 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 these devices away from the router.
- Mirrors, especially silver-coated, can reduce transmission performance.

Wireless Range

The following lists the expected wireless range of the router. 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)

Technical Specifications

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

For example, your router supports both the 'b' and 'g' specifications. The 802.11b specification transmits data rates up to 11 Mbps while the 802.11g specification transmits data rates up to 54 Mbps. These are theoretical standards 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 appliances also might interfere with the router – televisions, radios, microwave ovens, or 2.4 GHz cordless telephones. Therefore, positioning your router where it encounters the least interference helps maintain a better connection.

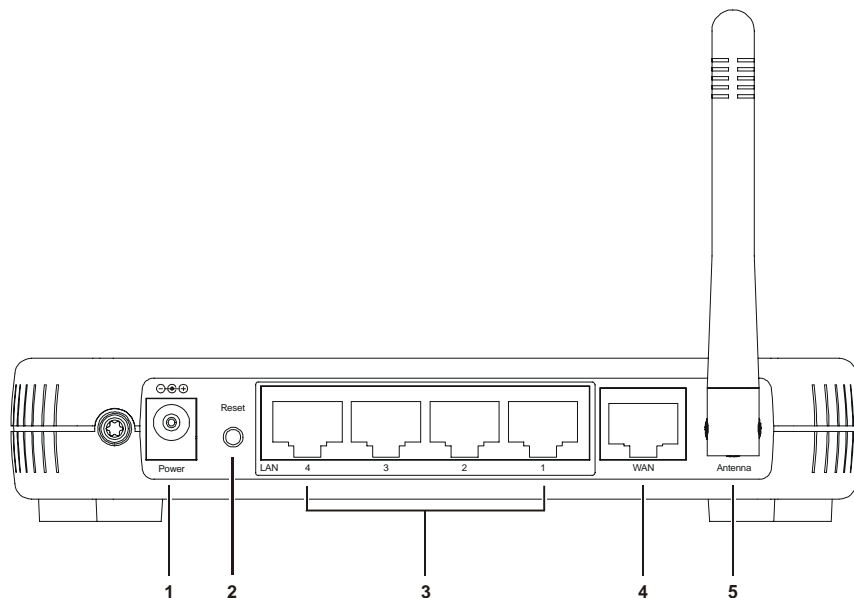
Router Physical Description

The following sections describe the physical characteristics of your router.

For instructions on installing your router, see Section 2: Installation.

Back of Router

The following illustration shows the WR850 back panel:

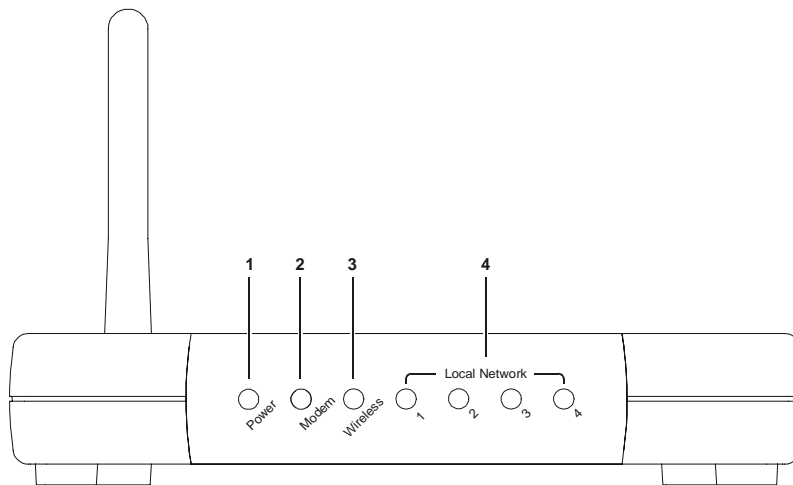


Feature	Description
1 Power	The receptacle where you plug in the power adapter.
2 Reset Button	<p>Resets your router or resets the router to the default login settings.</p> <p>If the router experiences trouble connecting to the Internet, briefly press and release the Reset button to reset the router. This retains the router's configuration information.</p> <p>To reset the router to the factory defaults, press and hold the Reset button for more than five seconds. This clears the router's user settings, including User ID, Password, IP Address, and Subnet mask. To re-configure the router, see Section 3: Configuration.</p>

Feature	Description
3 LAN Ports 1-4	<p>These four ports connect the router to your LAN or home network using Ethernet cables. This enables communication among clients, such as PCs or print servers, on the network. The LAN ports support either 10-BASE-T or 100-BASE-T transmission speeds as well as straight-through and crossover Ethernet cables.</p> <p>Any of these four ports can also serve as an uplink port to other network devices, such as another router or switch, which allows you to extend your network.</p>
4 WAN	<p>Connect your modem to your router using this port with your supplied Ethernet cable. This is the only port you can use for this procedure. This enables your router to access the Internet. The port supports 10/100 Mbps as well as straight-through and crossover Ethernet cables.</p>
5 Antenna	<p>The antenna used for wireless connections. You are able to rotate the antenna to gain the best signal reception.</p>

Front of Router

The following illustration shows the WR850 front panel:



The LEDs of the router 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/OFF	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 and the router's default user name, password, private LAN IP address, and private subnet mask address will be restored. The LED then turns off until the reset button is released. The power LED blinks RED if the firmware is corrupted, indicating the firmware needs to be restored.
2 Modem	OFF	None	No external Ethernet device has been attached and detected. The Ethernet link is down.
	ON	Red	The WAN interface has been disabled by the firmware.
	Blinking	Red	The WAN connection has lost IP connectivity with its default gateway even though the Ethernet link is still up. Or the WAN connection repair procedure is still in progress.
	ON/ <u>Blinking</u>	Amber	10BaseT link detected/ <u>active traffic present</u> .
	ON/ <u>Blinking</u>	Green	100BaseT link detected/ <u>active traffic present</u> .
3 Wireless	OFF	None	No mobile station or Access Point has been associated with this device.
	ON	Red	The wireless interface has been disabled by the firmware.
	ON/ <u>Blinking</u>	Amber	802.11b connection exists in this wireless domain/ <u>active traffic present</u> .
	ON/ <u>Blinking</u>	Green	802.11g connection exists in this wireless domain/ <u>active traffic present</u> .
4 LAN (x4)	OFF	None	No external Ethernet device has been attached and detected. The Ethernet link is down.
	ON/ <u>Blinking</u>	Amber	10BaseT link detected/ <u>active traffic present</u> .
	ON/ <u>Blinking</u>	Green	100BaseT link detected/ <u>active traffic present</u> .

Section 2: Installation

To get your network up and running:

- Set up your hardware.
- Insert the CD-ROM for product set up. Follow the prompts.

If you prefer to set up the router's software manually, refer to the Manual Software Setup found later in this section.

The following sections provide detailed instructions for completing these tasks.

Hardware Setup

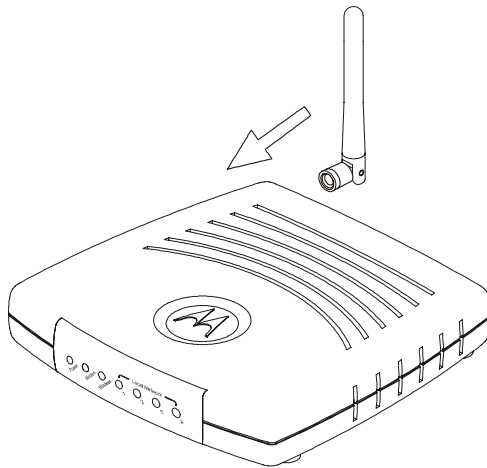
Hardware setup includes:

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

Antenna Installation

When shipped, the antenna for the WR850GP is not connected to the router. To attach the antenna to the router:

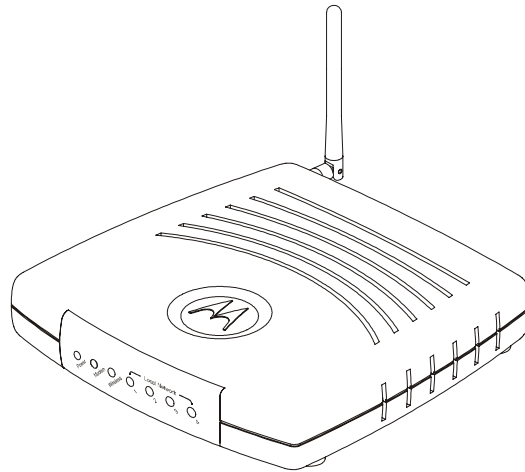
- 1 Locate the antenna port on the back of the router (the threaded knob).
- 2 Screw the antenna connector clockwise on to the threaded knob until firmly seated. Do not over-tighten.



Router Physical Installation

For the WR850GP, you can install the router horizontally or vertically. The WR850G can only be installed horizontally. Either router can also be mounted on a wall.

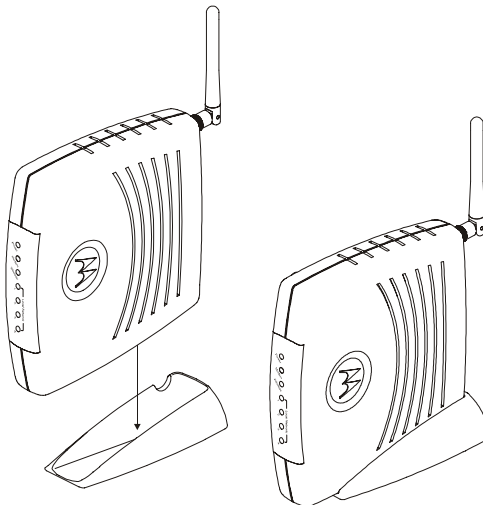
Horizontal Installation



- 1 Place the router in the desired location and follow the procedures below for connecting and configuring the router.

Vertical Installation

WR850GP only



- 1 Insert the router into the supplied base. Ensure that the antenna's location is on top. The router's foot slides snugly into a notch in the base to keep the router stable.
- 2 Follow the installation procedures for connecting and configuring the router.

Wall Mount Installation

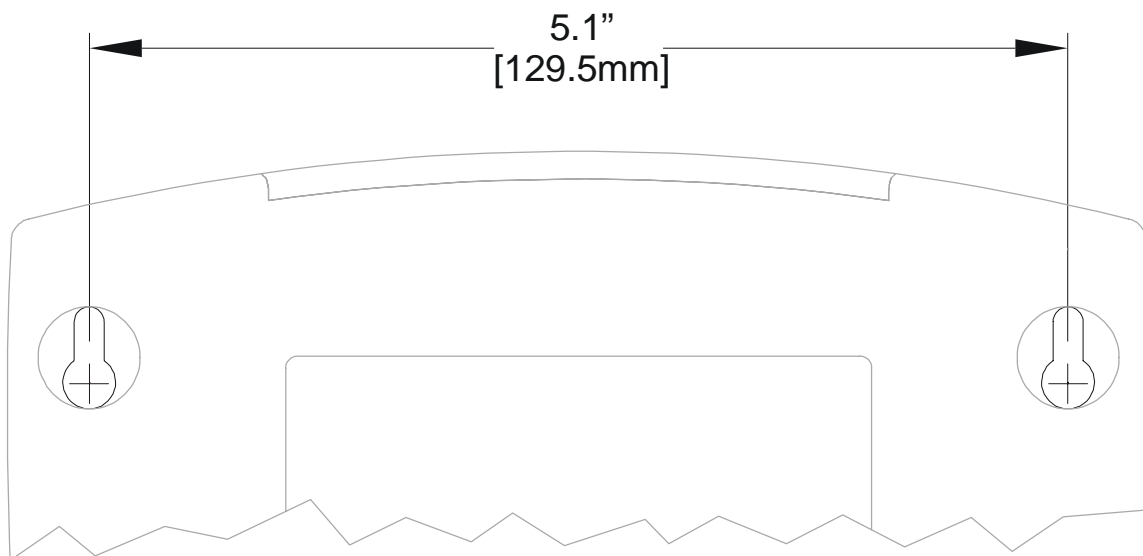
If you mount the router on the wall, you must:

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

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

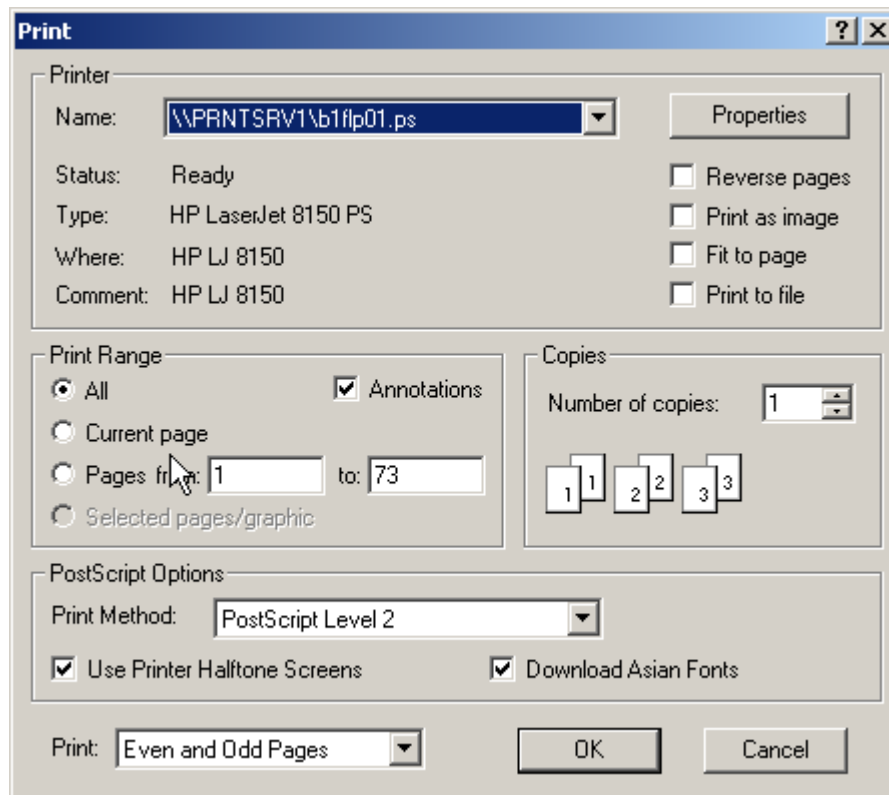
To mount your router on the wall:

- 1 Print the Wall Mounting Template shown on this page:



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

- Click the **Print** icon or choose **Print** from the File menu to display the Print dialog box:



In both the *Pages from* and *to* fields, enter the page number on which the Wall Mounting Template appears.

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

- Click **OK**.
- Measure the printed template with a ruler to ensure that it is the correct size.
- Use a center punch to mark the center of the holes on the wall.
- On the wall, locate the marks for the mounting holes you just made.

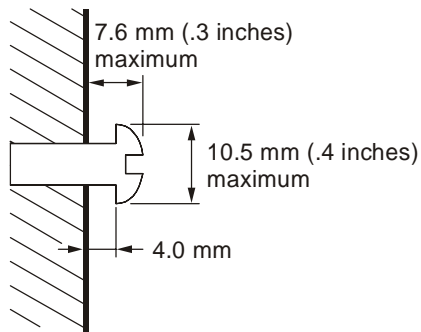
WARNING!



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

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

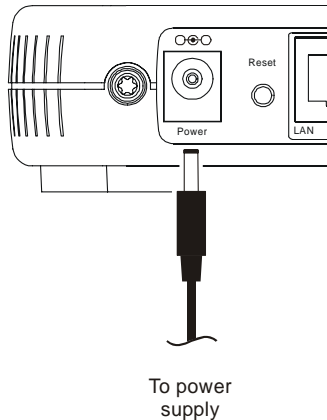
- 8 If necessary, seat an anchor in each hole. Use M5 x 38 mm (#10-16 x 1 1/2 inch) screws with a flat underside and maximum screw head diameter of 10.5 mm to mount the router.
- 9 Using a screwdriver, turn each screw until part of it protrudes from the wall, as shown:
 - There must be 4.0 mm (.16 inches) 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 two plastic feet, nearest to the LED panel, from the bottom of the router to uncover the keyholes.
- 11 Place the router so the keyholes are above the mounting screws.
- 12 Slide the router down until it stops against the top of the keyhole opening.
- 13 Follow the installation procedures for connecting and configuring the router.

Electrical Connection to Router

Your router does not have an On/Off power switch and therefore will only be powered on by plugging in the power adapter:



- 1 Connect the power adapter to the router's **Power** port, found on the back of the router.
- 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 set up your network. Once your network is up and running, for advanced configuration, see Section 3: Configuration.

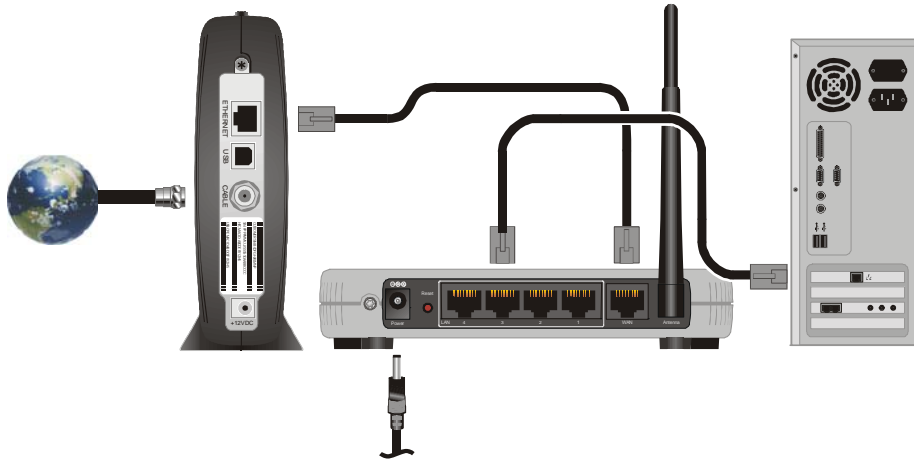
Manual Software Setup

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

To set up your wireless network:

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

Wired Connection to Router



If you are connecting your PC with an Ethernet cable to the router, your PC must be installed first with an Ethernet adapter.

You need two Ethernet cables for this procedure, one cable to connect the router to the modem and one cable to connect a PC to the router.

- 1 If you are currently running broadband to a single computer: Unplug the Ethernet cable that runs between your modem and PC from the back of your PC and plug it into the port labeled **WAN** on the back of your router.

If you are not running broadband to a single computer: Connect an Ethernet cable to the **WAN** port on your router.

- 2 Connect the other end of the same cable to your cable or DSL modem. It may be necessary to restart your cable or DSL modem after making this connection.
- 3 To connect the PC to the router, use a second Ethernet cable and connect it to the Ethernet port on your PC.
- 4 Connect the other end of the same cable into one of the **LAN** ports on your router. You have now connected your PC to the router.
- 5 To connect more devices, repeat steps 3 and 4.
- 6 To configure the router, see Section 3: Configuration.

Wireless Connection to Router

WARNING!



When first configuring your router, it is recommended that you have an Ethernet cable connected to the router. Performing the INITIAL configuration using a wireless connection is not secure and is not recommended.

After you have finished the initial configuration of the router, your connection will be secure and you can safely use either a wired or wireless connection.

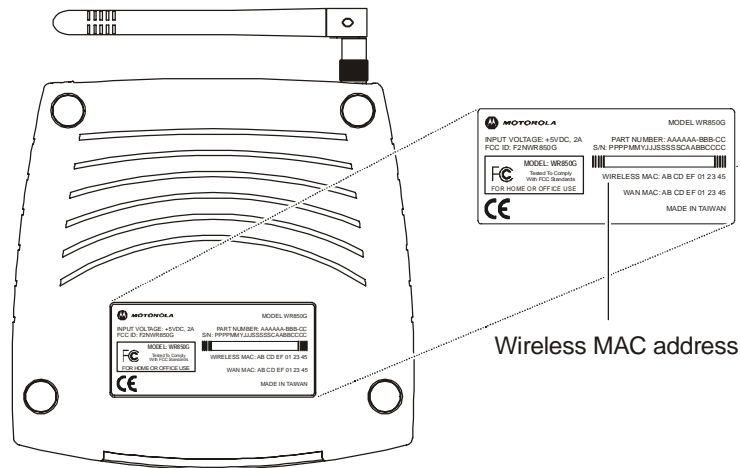
If you are connecting your client wirelessly to the router, you can use the Motorola WPCI810G, a wireless PCI card for your desktop PC. If you have a laptop, the Motorola WN825G wireless PC card provides access. A Motorola WU830G wireless USB adapter can also provide wireless access for desktops or laptops.

The WN825G and WPCI810G are not supported under Windows® 95, Windows 98, nor Windows NT. Windows 98SE, Windows Me®, Windows 2000, and Windows XP™ are supported. The WN825GP and WPCI810GP are supported under Windows 2000 and XP only.



- 1 If you are currently running broadband to a single computer: Unplug the Ethernet cable that runs between your modem and PC from the back of your PC and plug it into the port labeled **WAN** on the back of your router.
If you are not running broadband to a single computer: Connect an Ethernet cable to the **WAN** port on your router.
- 2 Connect the other end of the same cable to your cable or DSL modem. You have now connected the router to the modem. It may be necessary to restart your cable or DSL modem after making this connection.

- To connect the PC to the router through a wireless connection, verify the PC's wireless adapter SSID (Service Set Identifier) is set to the router'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.



Refer to your wireless network adapter's documentation for instructions on how to activate these settings.

- To configure the router, see Section 3: Configuration.

You have now completed the hardware installation. The next section, *Configure Your Computers*, steps you through the various configuration options needed for your PCs.

Configure Your Computers

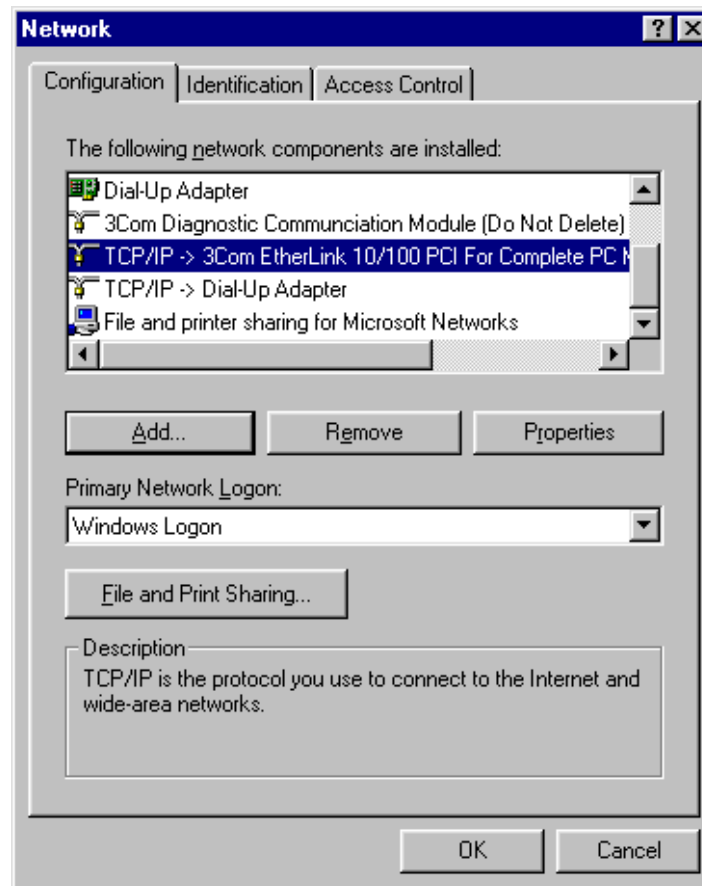
Each computer that will be part of your network needs to communicate with the router. To do this, you may need to configure each PC's network setting to automatically obtain an IP address. This section includes information on configuring computers with the following operating systems:

- Windows® 98SE
- Windows Me®
- Windows® 2000
- Windows XP™

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

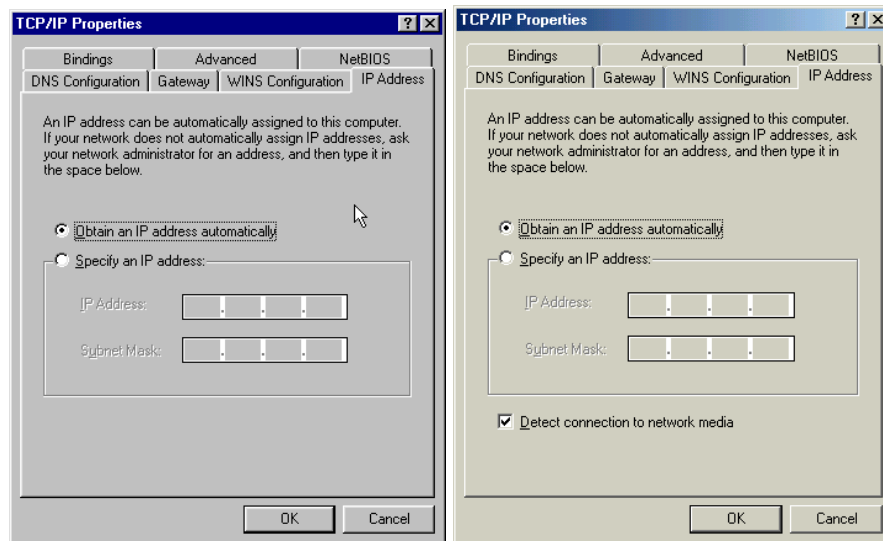
Configuring Windows 98SE and ME

- 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 on your PC. There may 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.

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



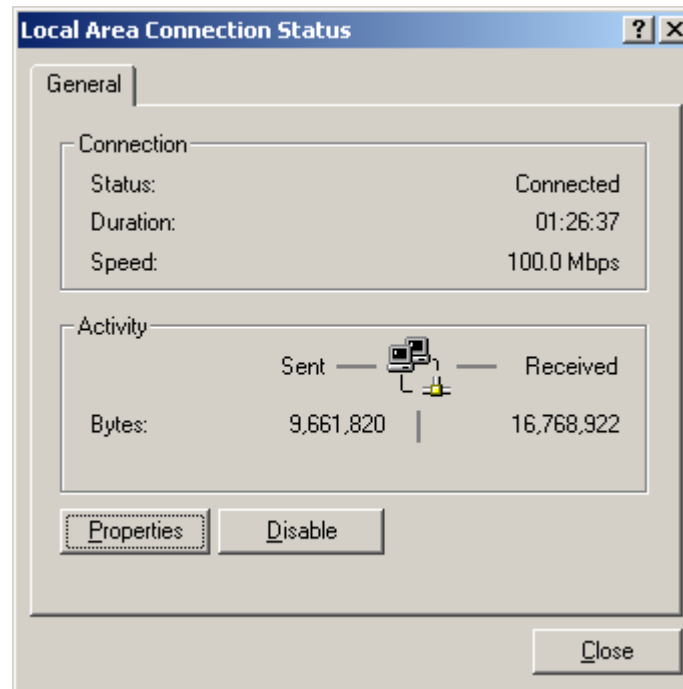
Windows 98SE

Windows ME

- 6 Click the **IP Address** tab.
- 7 Select **Obtain an IP address automatically**.
- 8 Click **OK**.
- 9 Click the **Gateway** tab and confirm that the *Installed Gateway* field is blank.
- 10 Click **OK** twice. Windows may ask for the Windows Installation disk. First check to see if the installation files are installed at c:\windows\options\cabs. Otherwise, load your Windows CD and follow the prompts.
- 11 Restart your computer to save your settings.
- 12 Proceed to the [Configure Your Wireless Security Settings](#) section to set up security.

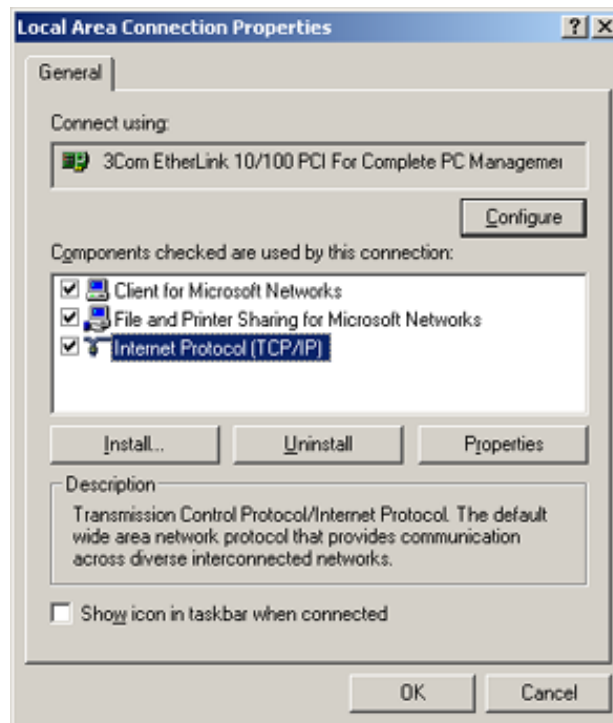
Configuring Windows 2000

- 1 Click **Start**.
- 2 Select **Settings**.
- 3 Select **Control Panel**.
- 4 Double-click **Network and Dial-Up Connections**.
- 5 Double-click **Local Area Connection**.



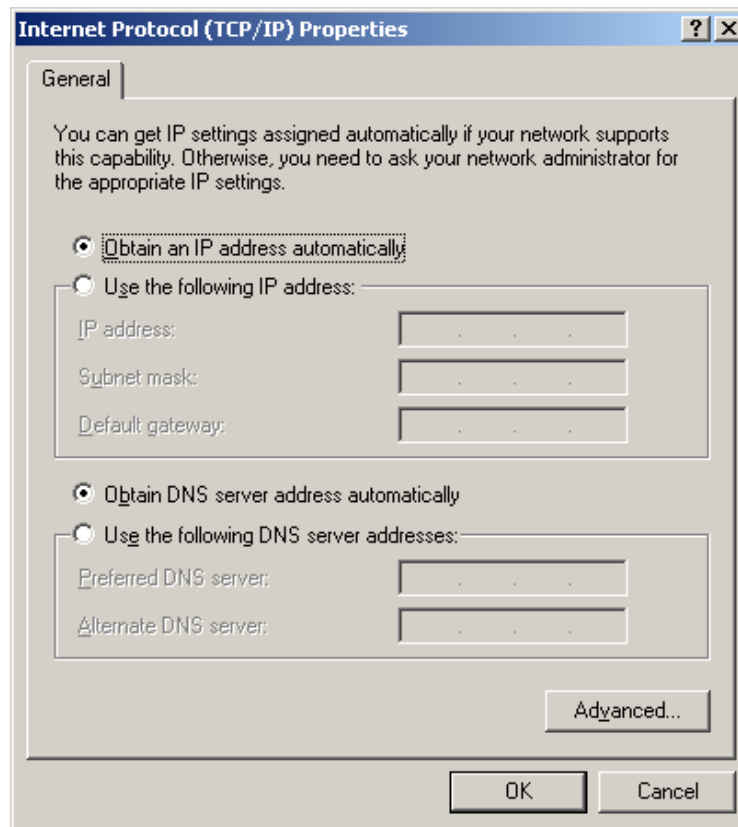
- 6 Click **Properties**.

The Local Area Properties window is displayed:



- 7 Ensure the box next to **Internet Protocol (TCP/IP)** is selected.
- 8 Click to highlight **Internet Protocol (TCP/IP)** and click **Properties**.

The Internet Protocol (TCP/IP) Properties window is displayed:

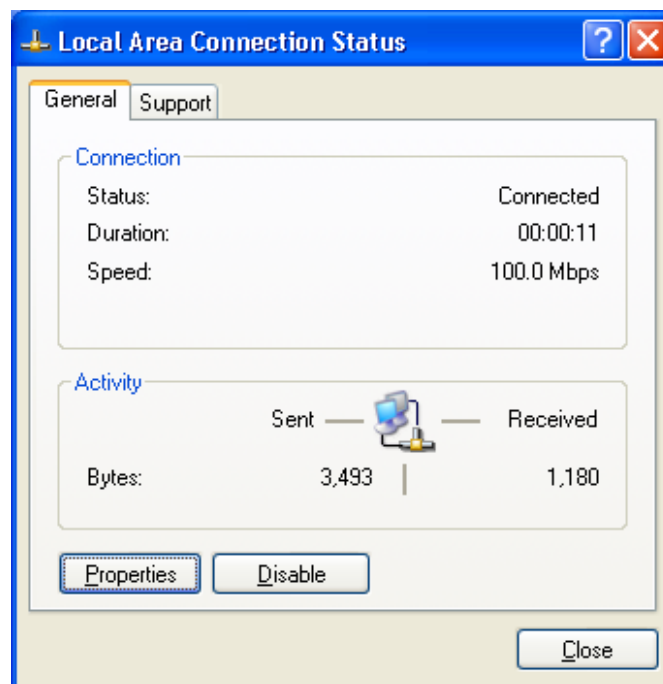


- 9 Select **Obtain an IP address automatically**. Click **OK** twice to exit and save your settings.
- 10 Restart your computer to save your settings.
- 11 Proceed to the [Configure Your Wireless Security Settings](#) section to set up security.

Configuring Windows XP

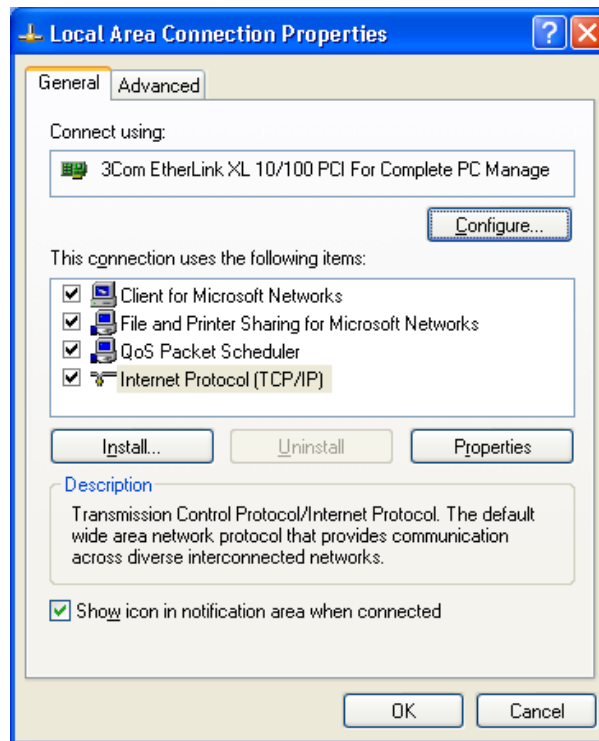
This configuration assumes you have retained the default interface for Windows XP. If you are running the 'Classic' interface, please follow the instructions for Windows 2000.

- 1 Click **Start**.
- 2 Select **Settings**.
- 3 Select **Control Panel**.
- 4 Double-click **Network and Dial-Up Connections**.
- 5 Double-click **Local Area Connection**.



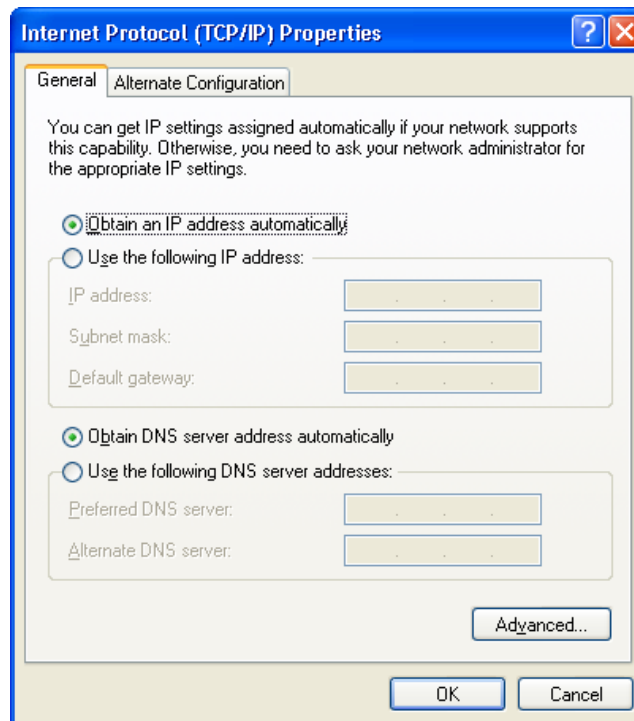
- 6 Click **Properties**.

The Local Area Properties window is displayed:



- 7 Ensure the box next to *Internet Protocol (TCP/IP)* is selected.
- 8 Click to highlight **Internet Protocol (TCP/IP)** and click **Properties**.

The Internet Protocol (TCP/IP) Properties window is displayed:



- 9 Click **Obtain an IP address automatically**. Click **OK** twice to exit and save your settings.
- 10 Proceed to the [Configure Your Wireless Security Settings](#) section to set up the security settings.

Configure Your Wireless Security Settings

Before your router can communicate securely with your computer, you must configure your wireless security settings. Failure to configure these settings properly could compromise your network to wireless hackers.

Logging In

WARNING!



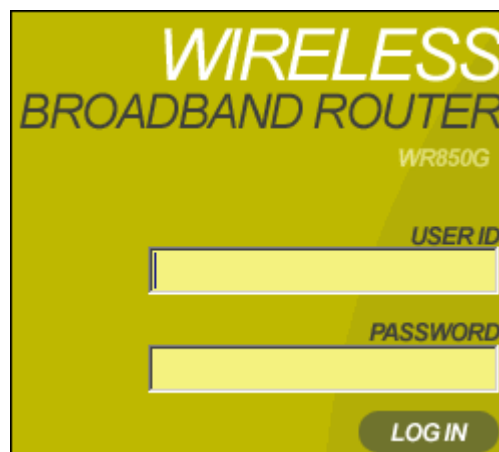
When first configuring your router, it is recommended that you have an Ethernet cable connected to the router. Performing the INITIAL configuration using a wireless connection is not secure and is not recommended.

After you have finished the initial configuration of the router, your connection will be secure and you can safely use either a wired or wireless connection.

- 1 Once the router is connected, open your web browser. In the URL field, enter **http://192.168.10.1** (the router's default IP address) and press the **Enter** key.



The login screen is displayed (the WR850G login screen is shown in the example below):



- 2 Enter the **User ID**. The default factory setting is *admin*.
- 3 Enter the **Password**. The default factory setting is *motorola*.

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

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

Wireless Security Setup

To set up the correct security protocols for your router:

- 1 Click **Control Panel > Device Security**.
- 2 In the Login User ID field, enter your **User ID**. Create an ID that contains multiple case-sensitive characters as well as numbers. It cannot be longer than 64 bytes.
- 3 In the Login Password field, enter your **Login Password**. Create a password that contains multiple case-sensitive characters as well as numbers and symbols like “_ +)”. It cannot be longer than 64 bytes.
- 4 Re-enter your 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 **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 ESS Authentication options.
- 11 Select **TKIP** from Encryption Status options.
- 12 Click **Apply** and then click **Restart**. Your wireless security configuration is now complete.

Configure Your Basic Internet Settings

The following settings configure your router for accessing the Internet. Detailed descriptions for using the web-based utility follow this section.

- 1 Log into the router's Configuration Utility. The **Internet > Basic** screen is displayed.
- 2 Select the *Connection Mode* your ISP has indicated you need to use. Based on which connection type you select, different areas become inaccessible, leaving only the necessary fields active.

DHCP Configuration

The default setting for the router, DHCP is most commonly used for cable modem connections. There is no configuration necessary for this setting because the ISP automatically supplies the information. Your ISP informs you if this is the connection to use.

- 1 Verify that **Cable Modem (DHCP)** is selected.
- 2 Click **Apply** to save the setting.

PPPoE

PPPoE (Point-to-Point Protocol over Ethernet) setting is most commonly used for DSL modem connections. Your ISP informs you if this is the connection to use.

- 1 From Connection Mode, select **DSL Modem (PPPoE)**.
- 2 In the PPP User Name field, enter the **PPP User Name** supplied by your ISP.
- 3 In the PPP Password field, enter the **PPP Password** supplied by your ISP.
- 4 Optionally, you may have to enter the **PPP Service Name** into this field. Enter the information supplied by your ISP.
- 5 Click **Apply** to save the setting. If you wish to start over, click **Clear**.

Static IP

If you are required to use a permanent IP address for connecting to the Internet, then select **Static Assigned**. Your ISP informs you if this is the connection to use.

- 1 From Connection Mode, select **Static Assigned**.
- 2 In the IP address field, enter the **IP address** supplied by your ISP.
- 3 In the Subnet Mask field, enter the **Subnet Mask** supplied by your ISP.
- 4 In the Default Gateway field, enter the values supplied by your ISP.
- 5 In the Primary DNS field, enter the values supplied by your ISP. If necessary, enter secondary or tertiary DNS values into the Secondary or Tertiary DNS fields.
- 6 Click **Apply** to save the setting. If you wish to start over, click **Clear**.

PPTP

Point to Point Tunneling Protocol (PPTP) is a service commonly found in Europe.

- 1 From Connection Mode, select **PPTP**.
- 2 In the PPP User Name field, enter the **PPP User Name** supplied by your ISP.
- 3 In the PPP Password field, enter the **PPP Password** supplied by your ISP.
- 4 In the PPTP Client IP field, enter the **PPTP Client IP** address supplied by your ISP.
- 5 In the PPTP Server IP field, enter the **PPTP Server IP** address supplied by your ISP.
- 6 Click **Apply** to save the setting. If you wish to start over, click **Clear**.

Section 3: Configuration

Use the information in this section to modify the router's settings. For example you can customize features for your home network, change settings such as your user name or password, or view the status of the network.

The screenshots seen here are intended for reference only; your version of firmware may differ slightly.

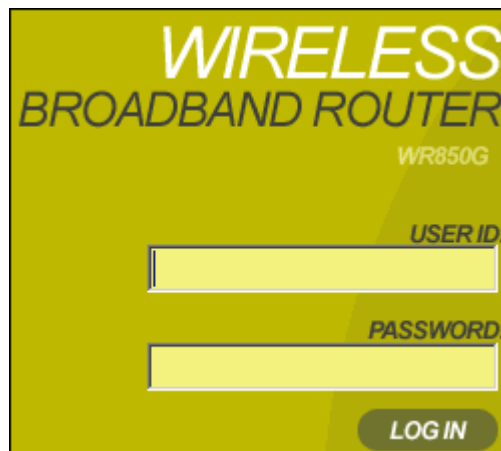
Using the Configuration Utility

Logging In

- 1 Once the router is connected, open your web browser. In the URL field enter **http://192.168.10.1** (the router's default IP address). Press the **Enter** key.



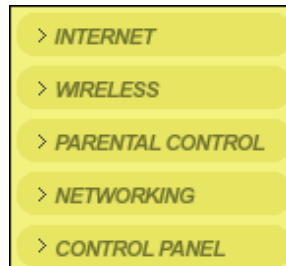
The login screen is displayed (the WR850G login screen is shown in the example below):



- 2 Enter the **User ID**. The default factory setting is *admin*.
- 3 Enter the **Password**. The default factory setting is *motorola*.
Once you have logged in, for security reasons you should change the User ID and Password. See below.
- 4 Click **Log In** to enter the Router's Web-based Configuration Utility.

Navigation

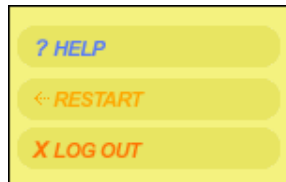
Each of the following subsections describe the components of the router's *Configuration Utility* which is accessible from a web browser. These sections include:



To navigate, click on a major section and then the associated subsection. For example, to adjust the time setting, click **CONTROL PANEL** on the left, then the **TIME** 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 | Accesses Help. |
| Restart | Restarts your session with the Configuration Utility. When Restart flashes, 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 | Logs out of the router's Configuration Utility. |

Configuring Internet Settings

The Internet Settings screens enable you to configure your Internet settings:



- Basic
- Advanced
- Network Diagnostic

Basic Internet Settings

After logging into the Configuration Utility, the Internet - Basic screen is displayed. It allows you to adjust basic settings for the router's Internet options.

You can also access this screen by clicking **Internet** on the login screen.

WAN Interface *inactive*
Connection Mode Cable Modem (DHCP) ▾
CONNECTION REPAIR
Connection Status DHCP state : Requesting DHCP Information
REFRESH
IP Address [] [] [] []
Subnet Mask [] [] [] []
Default Gateway [] [] [] []
Obtain DNS Server Address Automatically Yes No
Primary DNS [] [] [] []
Secondary DNS [] [] [] []
Tertiary DNS [] [] [] []
Host Name [] [] [] [] [] [] [] []
Domain Name [] [] [] [] [] [] [] []

PPP Authentication PAP ▾
PPP User Name [] [] [] [] [] [] [] []
PPP Password [] [] [] [] [] [] [] []
PPP Password Confirm [] [] [] [] [] [] [] []
PPP Service Name [] [] [] [] [] [] [] []
PPP Idle Timer enable
PPP Idle Time 0 (hr.) 0 (min.)
PPP Auto Reconnect enable
PPP MTU 0 bytes
PPTP Client IP [] [] [] []
PPTP Server IP [] [] [] []

APPLY **CANCEL**

Field or Button	Description
WAN Interface	<p>Displays the status of the router:</p> <p>Active Your WAN link is active.</p> <p>Inactive Your WAN link is not active.</p> <p>Disabled The WAN interface has been disabled. To enable the WAN interface, click the Advanced tab.</p>
Connection Mode	<p>The router supports four connection modes for acquiring its IP configuration settings of the WAN interface:</p> <ul style="list-style-type: none">▪ Cable Modem (DHCP)▪ DSL Modem (PPPoE)▪ Static Assigned▪ PPTP <p>Select the appropriate connection mode for your ISP (Internet Service Provider).</p>
Connection Repair	<p>Provides connection repair information depending on the connection mode selected.</p> <p>For example, for DHCP, the router issues a request for a new IP address from the ISP's DHCP server.</p>
Connection Status	<p>Provides current information about the connection status of the router.</p> <p>Press Refresh to update the status of the router.</p>
IP Address	<p>Displays the router's <i>IP Address</i> used to connect to your ISP. It is either automatically displayed or manually entered from information provided by your ISP.</p> <p>For example, if DHCP is selected, this is the IP Address that your router is currently using to access the Internet. If using Static Assigned, then you would enter the IP Address here.</p>
Subnet Mask	<p>Is automatically displayed or manually entered from information provided by your ISP.</p>

Field or Button	Description
Default Gateway	Is automatically displayed or manually entered from information provided by your ISP.
Obtain DNS Server Address Automatically	Select Yes to obtain the DNS information automatically, or No to enter the information manually.
Primary DNS	Is automatically displayed or manually entered from information provided by your ISP.
Secondary DNS	Is automatically displayed or manually entered from information provided by your ISP.
Tertiary DNS	Is automatically displayed or manually entered from information provided by your ISP.
Host Name	Is automatically displayed or manually entered from information provided by your ISP.
Domain Name	Is automatically displayed or manually entered from information provided by your ISP.
PPP Authentication	Available when PPPoE or PPTP is selected in the Connection Mode. Check with your ISP for the proper type of authentication to choose. <ul style="list-style-type: none">▪ PAP – Password Authentication Protocol▪ CHAP – Challenge Handshake Authentication Protocol▪ Auto – The router will offer PAP, CHAP, or None to the server, and the server will determine which PPP Authentication to use. Default setting.▪ None – No authentication used.
PPP User Name	Is automatically displayed or manually entered from information provided by your ISP.
PPP Password PPP Password Confirm	Is automatically displayed or manually entered from information provided by your ISP.

Field or Button	Description
PPP Service Name	Is either automatically displayed or manually entered from information provided by your ISP.
PPP Idle Timer	Click to enable PPP Idle Time.
PPP Idle Time	Enter the amount of time to elapse before the router automatically breaks the connection to the Internet.
PPP Auto Reconnect	Enables the router to automatically reconnect to the Internet when the connection has been cut.
PPP MTU	Allows you to adjust the Maximum Transmission Unit (in bytes) for the PPP connection. Available when PPPoE or PPTP is selected. Generally, the default value should be used.
PPTP Client IP	Is automatically displayed or manually entered from information provided by your ISP.
PPTP Server IP	Is automatically displayed or manually entered from information provided by your ISP.
Apply	Click to save your settings.
Cancel	Click to cancel any changes.

Advanced Internet Settings

The Internet – Advanced screen allows you to adjust additional Internet settings. To access the screen, click **Internet > Advanced**.

WAN Interface enable
 Factory WAN MAC Address 00:11:22:33:44:55
 Cloned WAN MAC Address enable [] : [] : [] : [] : [] : []
 Learned MAC Address **REFRESH**

Host Name	MAC Address
AZ74-5010	00:0B:FD:E1:5C:03
MG10325-02	00:0A:B7:BB:0A:1F

APPLY **CANCEL**

Field or Button	Description
WAN Interface	Check to enable the link to the Internet. Disabling this feature disconnects your Internet connection. The default is enabled.
Factory WAN MAC Address	Displays the default MAC address of the WAN interface. A MAC address is a 12-digit code assigned to a piece of hardware for identification. You can find the WAN MAC address on the label on the bottom of your unit.
Cloned WAN MAC Address	<p>Some ISPs require that you register the MAC address of your PC's network adapter.</p> <p>Your router can use the MAC address of your PC's network adapter as the router's WAN MAC address. To avoid calling your ISP and changing the MAC address that is registered with the ISP, follow these instructions:</p> <ol style="list-style-type: none"> 1 In the Cloned WAN MAC Address row, click Enable. 2 Enter a MAC address or click one of the Learned MAC addresses and click Apply. 3 After restarting the unit, the router will present the MAC address to the ISP you have entered here. 4 Deselect Enable to return to the default MAC address.

Field or Button	Description
Learned MAC Address	<p>Displays the MAC addresses (wired or wireless devices) the router has already recorded. If you wish to use one of the displayed MAC addresses:</p> <ol style="list-style-type: none"> 1 Click the address number. The number automatically appears in the Cloned WAN MAC Address field. 2 Click Apply to clone the displayed MAC address. 3 Click Refresh to search for additional MAC addresses on your LAN.
Apply	Click to save your settings.
Cancel	Click to cancel any changes.

Troubleshooting Your Network Connections

The Network Diagnostic screen helps you troubleshoot problems that might occur. To access the screen, click **Internet > Network Diagnostic**.

The screenshot shows a network diagnostic interface with three sections: PING, TRACE ROUTE, and DNS LOOKUP. Each section contains a text input field for entering a host name or IP address, followed by a large text area for displaying the results of the diagnostic test.

Field or Button	Description
Ping	Determines whether a particular IP address is online. This utility sends out a <i>packet</i> (block of data) and waits for a response.
Trace Route	Traces a route from the client machine to the remote host being contacted and reports the IP addresses of all the routers in between.

Field or Button	Description
DNS Lookup	Finds the IP address of a website name. For example, if you enter www.motorola.com , a DNS server returns the IP address of Motorola.

To use any of these functions:

- 1 Enter a **Host Name** or **IP Address** in the Ping, Trace Route, or DNS Lookup fields.
- 2 Click **Ping**, **Trace Route**, or **DNS Lookup** to activate the function. The results of your query are displayed.

Configuring Wireless Network Settings

The Wireless Network screens allow you to adjust settings for your wireless connection:



- Basic
- Security
- Site Monitor
- Advanced

Basic Wireless Configuration

This Wireless – Basic screen allows you to set up 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.

This window is where you enable or disable your Performance Enhancement.

Although your router has a default SSID, it is recommended that you change it to a name that is easy for you to remember.

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

Network Name (SSID)	<input type="text" value="motorola 345"/>		
Channel Number	<input type="text" value="11"/>		
Operation Mode	<input type="text" value="Compatibility (11b/g)"/>	<input checked="" type="checkbox"/>	Performance Enhancement Enabled
Wireless MAC Address	00:0C:E5:45:C0:A9		
			<input type="button" value="APPLY"/> <input type="button" value="CANCEL"/>

Field or Button	Description
Network Name (SSID)	Enter a name of no more than 32 alphanumeric characters. This SSID must be entered on every wireless device on your wireless network to communicate with the router. The default SSID is <i>motorola XXX</i> , where XXX are the last 3 characters of your Wireless MAC address, found on the label on the bottom of the unit.
Channel Number	Identifies the channel on which the router communicates. Each wireless client must use the same channel to enable communication. If changed wirelessly, once you restart the router, you will lose your the wireless connection. Change the wireless device's channel to the new channel to log back into the router. The default is Channel 11.
Operation Mode	Enables you to select the type of transmission protocol your wireless network uses. The options are: <ul style="list-style-type: none">▪ Compatibility (802.11b/g) – default setting▪ Performance (802.11g only)▪ Legacy (802.11b only)
Performance Enhancement <i>WR850GP only</i>	When enabled, the wireless data throughput of a WR850GP router is boosted when used exclusively with Performance Enhanced client devices, such as the WN825GP Wireless Notebook Adapters and/or WPCI810GP Wireless PCI Adapters. <ol style="list-style-type: none">1 From <i>Operation Mode</i> (see above), select Compatibility (802.11b/g) or Performance (802.11g only) to allow access to this feature.2 Check Performance Enhancement Enabled. When the Performance Enhancement feature is enabled, the wireless network can still support non-Performance Enhanced client devices, including standard 802.11g and/or 802.11b devices. Under these conditions the network steps down to support full backward compatibility. If you enable Performance Enhancement, it is recommended that you also enable Frame Bursting in the Wireless > Advanced screen. See Advanced Wireless Configuration for more information.

Field or Button	Description
Wireless MAC Address	Displays the Wireless MAC address of the unit. This is not the same as the WAN MAC address.
Apply	Click to save your settings.
Cancel	Click to cancel any changes.

Configuring Wireless Security Settings

The Wireless Security screen allows you to configure the security settings for your router. To access the screen, click **Wireless > Security**.

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

Field	Description										
ESS Authentication	<p><i>Extended Service Set (ESS)</i>. Authentication establishes either an open or secure verification of communication with an access point (AP). This setting does not encrypt your transmission.</p> <p>The options are:</p> <table border="0"> <tr> <td style="padding-right: 20px;">Open System</td> <td>No authentication is used. Default setting.</td> </tr> <tr> <td>Pre-Shared Key (PSK)</td> <td>The Pre-Shared Key (PSK) authentication method is used</td> </tr> <tr> <td>WPA</td> <td>Wi-Fi® Protected Access (WPA) authentication (802.1X) is used with an EAP type</td> </tr> <tr> <td>WPA-PSK</td> <td>WPA authentication (802.1X) is used with a pre-shared key</td> </tr> </table> <p><i>WPA-PSK is recommended for home users not using a RADIUS server.</i></p>	Open System	No authentication is used. Default setting.	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		
Open System	No authentication is used. Default setting.										
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										
Encryption Status	<p>Determines the type of security encryption algorithms used for the Key Index. This security setting encrypts your wireless transmission.</p> <ul style="list-style-type: none"> ▪ None, WEP64, and WEP128 are available only when Open System or Pre-Shared KEY (PSK) is selected in the ESS Authentication field. ▪ TKIP and AES are available only when WPA or WPA-PSK are selected in the ESS Authentication field. <p>The options are:</p> <table border="0"> <tr> <td style="padding-right: 20px;">None</td> <td>No security. Default setting.</td> </tr> <tr> <td>WEP64</td> <td>Wired Equivalent Privacy - 64-bit strength (provides 4 Keys)</td> </tr> <tr> <td>WEP128</td> <td>Wired Equivalent Privacy - 128-bit strength (provides 2 Keys)</td> </tr> <tr> <td>TKIP</td> <td>Temporal Key Integrity Protocol - changes the temporal key often (provides 1 Key)</td> </tr> <tr> <td>AES</td> <td>Advanced Encryption Standard (provides 1 Key)</td> </tr> </table> <p><i>TKIP is recommended for home users. If available, AES provides stronger encryption.</i></p>	None	No security. Default setting.	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)
None	No security. Default setting.										
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)										

Field	Description
802.1X mode	<p>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 or WPA-PSK is selected in the ESS Authentication field, this option is automatically selected.</p> <p>If not already enabled, select to activate this feature. When enabled, Dynamic Key generation occurs, meaning a key is automatically generated when the client requests one.</p>
Key Input Method	<p>Available if PSK and/or WEP is selected. The options are:</p> <ul style="list-style-type: none">▪ Pass Phrase (default setting)▪ Hexadecimal▪ ASCII <p>If you select either Pass Phrase or Hexadecimal, in Key Content, the format of the Key appears in a hexadecimal format.</p> <p><i>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 either ASCII or hexadecimal format for the non-Motorola wireless products.</i></p>
Pass Phrase	<p>Enter the Pass Phrase to be used for Key encryption. Keep a record of this Pass Phrase so you can enter the same phrase for the Motorola client devices on your wireless LAN, if supported. You will use this Pass Phrase when using WPA security with your client devices. Pass Phrase must be between 8 and 63 characters.</p> <p>The default pass phrase is <i>motorola</i>.</p>
Key Length	<p>The option selected determines the strength of the key. Only available when ESS mode is set to PSK and the Encryption Status is set to None.</p> <p>There are two options:</p> <ul style="list-style-type: none">▪ 128-bit▪ 64-bit.

Field	Description
Key Index	<p>Use the drop-down list here to select one of the Key Content fields below (Key 1, Key 2, etc). A maximum of four different Keys (1, 2, 3, or 4) are available. The number of keys is determined by what is selected in the ESS Authentication and Encryption Status fields.</p> <p><i>The Key selected here must match the key selected in the client. For example, if you select Key 1 here you have to select Key 1 for the client.</i></p> <p>The default is 1.</p>
Key Content	<p>Enter key content in these fields. The Key Content format is selected in the Key Input Method field.</p>
Key 1	
Key 2	<p>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. The Key will not automatically fill in until you have clicked Apply.</p>
Key 3	
Key 4	<p>If you have selected Hexadecimal or ASCII formatting (in the Key Input Method field), you can then enter your own Hexadecimal or ASCII keys. To enter keys manually, you must also have WEP64 or WEP128 selected in the Encryption Status field.</p> <ul style="list-style-type: none"> ▪ 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) <p><i>If entering a key manually, don't leave a key field blank or enter all 0's. These are not secure keys.</i></p>
Group Key Renewal Interval	<p>This is the number of seconds that pass until your router sends out a new group key. Only available if WPA or 802.1X are selected.</p> <p>The default is 300 seconds.</p>
RADIUS Server IP	<p>Enter the RADIUS Server IP and Port number. RADIUS is an authentication and accounting system to verify users.</p>
RADIUS Server Port Number	<p>To display these fields, either of the following conditions need to exist:</p> <ul style="list-style-type: none"> ▪ Open System or WPA is selected, along with either WEP64 or WEP128, and 802.1X is enabled ▪ WPA is selected and TKIP or AES is selected. <p>The default RADIUS Port Number is 1812.</p>

Field	Description
RADIUS Shared Secret	Type and re-type the RADIUS password in these fields.
RADIUS Shared Secret Confirmation	
Wireless MAC Access Control List	<p>Enables you to control which device accesses your wireless network based upon their MAC address. The default is disabled. The options are:</p> <ul style="list-style-type: none">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 router.Allow Allows only the wireless devices in the Access Control List (ACL) to communicate with the wireless router.Deny Denies wireless devices in the ACL from communicating with the wireless router. <p>To add a MAC address to the ACL:</p> <ol style="list-style-type: none">1 Check Enable.2 Select Allow or Deny from the drop-down list.3 Enter a MAC address or use one of the Learned MAC Addresses. To use one of the Learned MAC addresses, click the address number. The number automatically appears in the Wireless MAC Address Control List. To alter a MAC address, remove and replace with the updated address.4 Click Add to enter the address into the ACL.5 Click Apply to save. <p>To delete a MAC address from the ACL:</p> <ol style="list-style-type: none">1 Click 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.
Learned MAC Addresses	<p>Displays the MAC addresses (wireless devices only) the router has already recorded.</p> <p>If you wish to use one of the displayed MAC addresses, click the address number. The number automatically appears in the Wireless MAC Address Control List.</p> <p>Click Refresh to force the router to search for additional MAC addresses.</p>

Field	Description
Apply	Click to save your settings.
Cancel	Click to cancel any changes.

Monitoring Wireless Access Points

The Site Monitor screen displays information about wireless Access Points (AP) and stations:

Station Association List	Identifies only those stations that are connected to your wireless router.
Site Survey	Displays information about other APs in the area.

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

The screenshot shows the Site Monitor interface with two main sections: Station Association List and Site Survey.

Station Association List: Includes a REFRESH button and a table with columns for MAC Address and Host Name. One entry is visible: MAC Address 00:0A:B7:BA:FD:B8 and Host Name mgi0391-02.

Site Survey: Includes a SCAN button and a table with columns for SSID, MAC Address, Channel, Signal Strength, Wireless Mode, and Security. One entry is visible: SSID motorola, MAC Address 00:08:0E:D3:02:85, Channel 1, Signal Strength 30%, Wireless Mode 802.11b, and Security None.

Field	Description
Station Association List	
Refresh	Click to refresh the Station Association List.
MAC Address	Displays the MAC address of clients found on the LAN.
Host Name	Displays the name of the device attached.

Field	Description
Site Survey	
Scan	Click Scan 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.

Advanced Wireless Configuration

The Wireless – Advanced screen allows you to turn your wireless network on and off and adjust wireless parameters. Generally, these settings should remain at their default values.

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

Field	Description
Radio Interface	Allows you to turn on and off the wireless feature. If you disable the radio interface, your router continues to service your wired network. The default is enabled.
Short Preamble	Improves the efficiency of a network's throughput when transmitting and receiving data. Motorola recommends that you enable this feature. The default is disabled.
Frame Bursting	Allows you to send more frames (collection of packets) within a given time period, which enhances network efficiency and reduces overhead. This feature works with other Motorola products to increase performance throughput. Motorola recommends that you enable this feature. This feature's default setting is <i>disabled</i> for the WR850G and <i>enabled</i> for the WR850GP.
RTS Threshold	Allows you to modify the RTS threshold, which is 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.

Field	Description						
Fragmentation Threshold	<p>Allows you to set 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.</p> <p>The default is 2346.</p>						
Beacon Period	<p>Allows you to set the time units for the beacon period. A <i>beacon</i> is a packet broadcast by the AP 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.</p> <p>Since changes to the Beacon Period and Delivery Traffic Indicator Maps (DTIM) settings may affect wireless performance, it is best to use the default settings.</p>						
DTIM Period	<p>Allows you to set the Delivery Traffic Indicator Maps (DTIM) period value from 1 to 255 in multiples of Beacon Periods. The default is 3.</p> <p>Since changes to the Beacon Period and Delivery Traffic Indicator Maps (DTIM) settings may affect wireless performance, it is best to use the default settings.</p>						
Basic Rate Set	<p>Allows you to set the transmission rate. The router broadcasts different transmission rates so clients know which transmission rate to use to join the network.</p> <p>The options are:</p> <table><tbody><tr><td>1 to 2 Mbps</td><td>The slowest speed available.</td></tr><tr><td>Default</td><td>Ensures compatibility with 802.11b or 802.11g devices</td></tr><tr><td>All</td><td>Ensures compatibility with all devices.</td></tr></tbody></table>	1 to 2 Mbps	The slowest speed available.	Default	Ensures compatibility with 802.11b or 802.11g devices	All	Ensures compatibility with all devices.
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	<p>Ensures that your wireless router does not interfere with neighbor networks. 802.11g networks cause “collisions” on 802.11b networks, so the Protection Mode forces the 802.11g network to negotiate around the 802.11b network.</p> <p>The options are:</p> <p>Disable 802.11g Protection Mode is never used.</p> <p>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. Default setting.</p>
WDS Mode	<p>Enables WDS mode, which allows 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.</p> <p>When WDS Mode is enabled, any AP configured to your router’s settings can connect to your network. The default is disabled.</p>
WDS Restrict Mode	<p>Protects your network by assigning access to only the access points you designate. Assign the access points’ MAC addresses in the WDS Restrict MAC Addresses fields.</p> <p>The default is enabled.</p>
WDS Restrict MAC Addresses	<p>To activate these fields, WDS Restrict Mode must be enabled.</p> <ul style="list-style-type: none">▪ Enter up to four wireless MAC addresses▪ To edit an entry, highlight the number and change▪ To delete a number, delete each field
Apply	Click to save your settings.
Cancel	Click to cancel any changes.

Configuring Parental Control Settings

Parental Control settings allow you to tailor the type of content your router can access. *Content Policies* allow you to specify the websites or keyword searches users can access. Up to ten policies can be created, each of which can be customized for specific time periods and associated with any of the PCs your router supports.

For example, if you want to restrict the websites your children can access during the day, you can create a "Kids' Policy" that restricts defined websites during the time of day when children could potentially access the computer unsupervised.

The following screens are available in Parental Control:



- Content Policy
- URL Log

Parental Control - Content Policy

To access the screen, click **Parental Control > Content Policy**. Instructions for creating a policy appear after this screen description.

Field	Description
Content Policy	Enables or disables the Content Policy feature. The default is disabled.

Field	Description
Policy Number	The policy number you assign.
Policy Name	The name of the policy, up to 32 characters. You can enter up to ten different policies, tied to the Policy Number.
Allow URL	Allows the recipient of the policy to access the URL(s) designated in the URL field.
Deny URL	Blocks the recipient of the policy from accessing the URL(s) designated in the URL field.
URL	The URL to which the policy will apply. The initial entry must end with a semicolon.
Keyword Filter	Words that deny Internet access to the recipient of the policy.
Schedule	The time of day that the policy is in effect.
MAC Filter	<p>Enables the MAC Filter, which uses the MAC addresses for filtering.</p> <ul style="list-style-type: none">You can enter multiple MAC addresses for a single policy or multiple policies for a single MAC address. <p>To set up a filter:</p> <ol style="list-style-type: none">Manually enter a MAC address or click on a Learned MAC address.Click Add to enter it into the MAC Filter list.To edit a MAC address, click it. Click Remove and then add the revised MAC address.
Learned MAC Addresses	Displays the MAC addresses discovered on the LAN. Click Refresh to rediscover the MAC addresses available on the LAN.
Apply	Click to save your settings.
Cancel	Click to cancel any changes.

To create a policy:

- Enter a **name** in the Policy Name field.

- Decide if you want to Allow or Deny a URL (the address of a website). You can add more than one URL, separated by semicolons. The final entry **must** end with a semicolon.

The following selections are optional for the policy:

- Enter a Keyword filter.
- Enable a time-based policy by enabling and selecting the time/date options.
- Select a MAC address to which the policy will apply, ensuring that MAC Filter has been enabled. You can easily select a MAC address by clicking one in the Learned MAC Address table.

- Click **Apply** to save the policy.

Parental Control - URL Log

A *URL* is the address of a website. A *URL Log* allows you to view a list of all websites that have been accessed by the PCs on your network.

To begin tracking the websites accessed by your PCs, click **Parental Control > URL Log**. The URL Log screen is displayed. Click **Enable** to begin tracking websites.

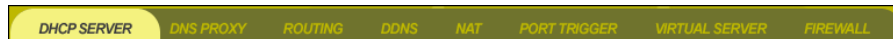
Field	Description
URL Log	Click to enable the feature.
URL Log Table Refresh	Click to update the list with the latest URL Log.
Visited URL	Displays the URL (website) that the PC has accessed.

Field	Description
LAN IP	Displays the IP address of the device on your network (LAN or Wireless) that accessed the Internet.
LAN MAC Address	Displays the PC's MAC address.
LAN Host Name	Displays the PC's Host Name.
Time	Displays the time of access.
Service/Port Number	Displays the Port number used for access.
Apply	Click to save your settings.
Cancel	Click to cancel any changes.

Configuring Networking Settings

The Networking screens allow you to configure your router to work with your Local Area Network (LAN). You should not need to make any changes to these settings.

The following screens are available in Networking:



- DHCP Server
- DNS Proxy
- Routing
- DDNS
- NAT
- Port Trigger
- Virtual Server
- Firewall

Configuring DHCP Server Settings

The Domain Host Control Protocol (DHCP) server automatically assigns IP addresses to all the clients on your network, relieving you of the responsibility for issuing separate IP addresses. *It is highly recommended that you administer your network using the DHCP function.* The PCs must be configured to “Obtain an IP Address Automatically.” See the *Installation* section of this User Guide for further details.

To access the screen, click **Networking > DHCP Server**.

LAN MAC Address **00:0C:19:76:08:26**

LAN Private IP . . .

LAN Subnet Mask . . .

LAN DHCP Server enable

Address Pool Begins **192 . 168 . 10 .**

Address Pool Size

Default Lease Duration (wk.) (day) (hr.) (min.)

Active Leases **REFRESH**

Computer Name	IP Address	MAC Address	Expires
	192.168.10.2	00:00:00:00:00:00	Expired
mgj0391-02	192.168.10.3	00:0A:B7:BA:FD:B8	22 hours, 34 minutes, 7 seconds
AZ74-5010	192.168.10.4	00:0B:FD:E1:5C:03	19 hours, 18 minutes, 40 seconds
MGI0325-02	192.168.10.5	00:0A:B7:BB:0A:1F	21 hours, 43 minutes, 58 seconds

APPLY **CANCEL**

Field	Description
LAN MAC Address	Displays the LAN MAC address of the router. This field cannot be edited.
LAN Private IP	Enables you to create your own private IP network. Enter an IP address string that you will use for your network. Because it is a private network, your router gives you the ability to choose any string you prefer. The default is 192.168.10.1
LAN Subnet Mask	Enables you to create your own Subnet Mask for your network. The Subnet Mask determines which portion of a destination LAN IP address is the network portion and which portion is the host portion. Enter a Subnet Mask address that you will use for your network. The default is 255.255.255.0
LAN DHCP Server	Enables or disables the DHCP server. You can only run one DHCP server on your network. The default is enabled.

Field	Description
Address Pool Begins	Indicates the beginning IP number. Based on the number entered in the LAN Private IP field. The default is 2.
Address Pool Size	<p>You can reserve up to 253 slots on your DHCP server for potential clients. For example, when using the router's default IP of 192.168.10.1, then all numbers up to 192.168.10.254 are available for use.</p> <p>If you want to make available every number, enter 253. The default is 50.</p>
Default Lease Duration	<p>Displays the Hours and Minutes of the default lease duration. To change, enter a new duration. The default is 1 day.</p>
Active Leases	<p>Displays the current clients that the DHCP server has assigned IP addresses, including the client's Computer Name, IP and MAC address, and the duration of its lease.</p> <p>Click Refresh to obtain the latest list.</p>
Apply	Click to save your settings.
Cancel	Click to cancel any changes.

Configuring the Router Host Name

This feature allows you to change the Host Name of your router. This feature only applies to your private home network.

To access the screen, click **Networking > DNS Proxy**.

No.	LAN Private Host Name	Host IP address
1	WR850G	192.168.10.1

Field	Description
LAN Private Host Name	Displays the current Host name for the router. Enter in a new name if desired. The default is wr850g (all lower case).
Host Table	Displays the current active Host Name and its associated IP address.
Apply	Click to save your changes.
Cancel	Click to cancel your changes.

Configuring Network Router Settings

From the Networking – Routing screen, you can define up to 20 static routes that specify the Destination IP, Subnet Mask, Gateway, Interface, and Metric (how many “hops” the router can make). You can also configure the Network Routing Table here.

RIP (Routing Information Protocol) versions 1 and 2 are routing protocols that are part of the TCP/IP protocol standard. RIP dynamically determines a route based on the smallest hop count between source and destination.

To access the screen, click **Networking > Routing**.

The screenshot shows a configuration page for Routing. At the top, there are two checkboxes: "RIP v1" (checked) and "RIP v2" (checked), both labeled "enable". Below this is a "Routing Table Entry List" section with a "REFRESH" button. It contains a table with columns: Destination LAN IP, Subnet Mask, Gateway IP, and interface. The table has two rows: (192.168.10.0, 255.255.255.0, 192.168.10.1, LAN&Wireless) and (127.0.0.1, 0.0.0.0, 127.0.0.1, LOOPBACK). Below the table are input fields for "Destination IP" (192.168.10.5), "Subnet Mask" (255.255.255.255), "Gateway IP" (192.168.10.1), "Interface" (Internet (WAN)), and "Metric" (1). There are "ADD", "EDIT", and "REMOVE" buttons. At the bottom is a "Routing Table" section with a table with columns: Destination IP, Subnet Mask, Gateway IP, interface, and Metric. It has two rows: (192.168.10.4, 255.255.255.255, 192.168.10.1, lan, 1) and (192.168.10.5, 255.255.255.255, 192.168.10.1, wan, 1). At the bottom right are "APPLY" and "CANCEL" buttons.

- | | |
|---------------------------------|--|
| Field | Description |
| RIP V1 | Enables or disables RIPv1.
The default is disabled. |
| RIP V2 | Enables or disables RIPv2.
The default is disabled. |
| Routing Table Entry List | <p>To add a Routing Entry:</p> <ol style="list-style-type: none"> 1 Select a Destination IP number, (the client’s Routing IP address). 2 Enter Subnet Mask and Gateway IP address. 3 Select the Interface (LAN & Wireless or Internet (WAN)) to which the entry will apply. 4 Enter the Metric (or how many hops the routing can take). 5 Click Add to enter the Routing Entry into the Routing Table. 6 Click Apply to save the entry. <p>To edit or remove an entry, click the desired entry and perform the requested action.</p> |

Configuring DDNS Settings

The router supports the Dynamic Domain Name System (DDNS) feature. DDNS enables you to assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own web server, FTP server, or another server behind the router. Before you can use this feature, you must sign up for DDNS service at a DDNS service provider, such as www.dyndns.org or www.changeip.com. Once you have signed up, write down your User Name and Password assigned by the service.

To access the screen, click **Networking > Dynamic DNS**.

Field	Description
DDNS	Enables or disables DDNS. The default is disabled.
DDNS Server	Select the desired DDNS service provider.
User Name	Enter the User Name (up to 30 bytes) provided by the DDNS provider.
User Password User Password Confirm	Enter and re-enter the Password (up to 30 bytes) provided by the DDNS provider.
Host Name	Enter a desired Host Name for your WAN IP Address.
Apply	Click to save your settings.
Cancel	Click to cancel any changes.

Configuring NAT Settings

The Networking – NAT screen allows you to add another level of security to your Internet activity and online games. Network Address Translation (NAT) translates the multiple IP addresses on a private LAN to one public address that is sent out to the Internet by your ISP. This means the addresses of the PCs on your home network are never transmitted on the Internet.

The Networking – NAT screen also allows you to enable a gaming Demilitarized Zone (DMZ), which allows only one IP address (for a computer or device) to be exposed to the Internet for online game playing or video conferencing.

To access the screen, click **Networking > NAT**.

Field	Description
NAT	Enables or disables NAT. The default is enabled.
Gaming DMZ Device	Click to enable. The default is disabled.
My Gaming Device	Enter the IP Address for your gaming device. The default is disabled. <i>For security purposes, turn off your gaming device when not in use so that it does not become the target of intrusion.</i>
TCP Session Idle Time	Enter the TCP Session Idle Time which is the amount of time a TCP session will remain idle before timing out. The default is 8 hours.
UDP Session Idle Time	Enter the User Datagram Protocol (UDP) Session Idle Time, which is the amount of time a UDP session will remain idle before timing out. UPD is used primarily for broadcasting messages over a network. User Datagram Protocol, along with the IP, sends data in the form of message units (datagram) between network devices over a LAN or WAN. The default is 8 hours.

Field	Description
ICMP Session Idle Time	Enter the Internet Control Message Protocol (ICMP) Session Idle Time, which is the amount of time a ICMP session will remain idle before timing out. ICMP is used for error, problem, and informational messages sent between IP hosts and gateways. The default is 5 minutes.

Apply Click to save your settings.

Cancel Click to cancel any changes.

Configuring Port Trigger Settings

When you run a computer application that accesses the Internet, it typically initiates communications with a computer on the Internet. In some applications, especially games, the computer on the Internet attempts to communicate with your computer. NAT does not normally allow these incoming connections to occur, but you can use *port triggering* to bypass this. Port triggering is a function that allows incoming communication with specified applications.

The WR850 is already configured with port triggering for some common applications. You can also configure additional port triggers using the Networking – Port Trigger screen.

To access the screen, click **Networking > Port Trigger**.

Port Trigger Name: Netmeeting & H.323Netme enable

Outgoing Protocol: TCP

Outgoing Port: 1720 ~ 1720

Triggered Incoming Protocol: UDP

Incoming Port: 1024 ~ 65534

ADD EDIT REMOVE

Name	Enable	Outgoing Proto/Port	Incoming Proto/Port
Netmeeting & H.323Netme	enable	TCP/1720-1720	TCP/1024-65534
Netmeeting & H.323Netme	enable	TCP/1720-1720	UDP/1024-65534

Idle Timer: 0 Hour 10 Min

APPLY CANCEL

To add a Port Trigger entry:

- 1 Enter the **name** of the application in the Port Trigger Name field. There is a limit of 32 characters for the name.

- Click **enable** if you wish the port trigger to become active immediately. Otherwise, you can save the information and enable it at later date.

To enable at a later date, select the entry, check **enable**, and then click **Add**.

- From the Outgoing Protocol drop-down list, select TCP or UDP.
- In the Outgoing Port fields, enter the From and To ranges (0 to 65535) for your application.
- From the Trigger Inbound Protocol drop-down list, select TCP or UDP.
- In the Incoming Port field, enter continuous value(s) (0 to 65535), separated by dashes, for your application. You can also enter multiple non-continuous values, separated by semicolons.
- In the Idle Time fields, enter the elapsed time before the Port Trigger mapping closes for all of the listed entries.
- Click **Apply** to save your settings. To cancel your changes, click **Cancel**.

To edit or remove an entry, select it and then click **Edit** or **Remove** to perform the action.

Sample Port Trigger Entries

Below are common Port Trigger Entries for popular applications.

Port Trigger Name	Outgoing Protocol	Outgoing Port	Incoming Protocol	Triggered Incoming Port Range
AOL® Instant Messenger™	TCP	5190	TCP	5190
Battle.net®	TCP/UDP	6112	TCP/UDP	4000,6112
DirectX®7	TCP	47624	TCP/UDP	2300-2400
DirectX®8	UDP	6073	UDP	2302-2400
MSN® Messenger	TCP	6891-6901	TCP	1863,5190, 6891-6901
Net2Phone®	UDP	6801	UDP	6801
NetMeeting® & H.323	TCP	1720	TCP/UDP	1024-65534
QuickTime®	TCP	554	UDP	6970-6999

Configuring Virtual Server Settings

The Virtual Server sets up an automatic inbound forwarding mechanism for services running on your computer, such as web servers, email servers, or other specialized applications. You must configure your server with a static IP address to use this service.

To access the screen, click **Networking > Virtual Server**.

Virtual Server Name enable

Incoming Protocol

Incoming port

Forwarding IP 192.168.10.

Forwarding port

Schedule Everyday Sun Mon Tue Wed Thu Fri Sat

24 Hours From: : AM To: : AM

VS Table

Name	Enable	Proto/Port#	IP/Port#
<input type="text" value="FTP"/>	<input type="text" value="disable"/>	<input type="text" value="TCP/21"/>	<input type="text" value="192.168.10.0/21"/>
<input type="text" value="TFTP"/>	<input type="text" value="disable"/>	<input type="text" value="UDP/69"/>	<input type="text" value="192.168.10.0/69"/>
<input type="text" value="Telnet"/>	<input type="text" value="disable"/>	<input type="text" value="TCP/23"/>	<input type="text" value="192.168.10.0/23"/>
<input type="text" value="HTTP"/>	<input type="text" value="disable"/>	<input type="text" value="TCP/80"/>	<input type="text" value="192.168.10.0/80"/>
<input type="text" value="HTTPS"/>	<input type="text" value="disable"/>	<input type="text" value="TCP/443"/>	<input type="text" value="192.168.10.0/443"/>

To add a Virtual Server entry:

- 1 Enter the name of the server in the Virtual Server Name field. There is a limit of 32 characters for the name.
- 2 Click **enable** if you wish the virtual server to become active immediately. Otherwise, you can save the information and enable it at later date.
To enable at a later date, select the entry from the Virtual Server table and then check **enable**.
- 3 From the Incoming Protocol drop-down list, select TCP, UDP, or Both.
- 4 Enter the port value (0 to 65535) in the Incoming Port field
- 5 In the Forwarding IP field, enter the **IP Address** of the server to which you will forward.
- 6 Enter the **port value** (0 to 65535) in the Forwarding Port field.
- 7 (Optional) If you want to schedule the time and day of week for the forwarding service to be active, select the time and day in the Schedule row. If you want the forwarding service to be active all the time, select **Everyday** and **24 Hours**.
- 8 Click **Add** to add the entry to the VS table.
- 9 Click **Apply** to save the entry.

To update or remove an entry, select it and then click **Edit** or **Remove** to perform the action.

Configuring the Firewall

The firewall on your router shields your network from the Internet by examining network *packets* (units of data sent on a network) before they are forwarded to your router. The Networking – Firewall screen allows you to further customize this feature by adding packet filters that will restrict specific data from entering your router.

Instructions for adding a packet filter follow the screen description below.

To access the screen, click **Networking > Firewall**.

Field	Description
Firewall	Click to disable the Firewall. The default is enabled.
Multicast Pass-through	Click to enable Multicast Pass-through. The default is disabled. Multicast Pass-through is typically used for work-related activities, such as video conferencing.
Apply	Click to save your settings.
Cancel	Click to cancel any changes.

To add a Packet Filter entry:

- 1 Enter a descriptive ***name*** in the Packet Filter Name field.
- 2 From the Filter Action drop-down list, select Allow or Deny. Allow permits data that meets the criteria selected. Deny blocks the data that meets the selected criteria.
- 3 From the Packet Direction drop-down list, select Inbound or Outbound, based on whether you want to monitor incoming or outgoing packets.
- 4 From the Packet Protocol drop-down list, select the type of protocol to monitor: TCP, UDP, ICMP, or ALL.
- 5 Enter the ***IP range*** in the Source IP Range field.
- 6 Enter the ***port range*** in the Source Port Begins and Ends fields.
- 7 Enter the ***Destination IP range*** in the Destination IP Range field.
- 8 Enter the ***Destination Port range*** in the Destination Port Begins and Ends fields.
- 9 Click **Add** to add the entry.
- 10 Click **Apply** to save the entry. To cancel your changes, click **Cancel**.

To update or remove an entry, select it and then click **Edit** or **Remove** to perform the action.

The position of the Packet Filter entry determines the order in which the policy will be applied.

Configuring Control Panel Settings

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

The following screens are available in Control Panel:



- Device Security
- Firmware Update
- Configuration Data
- Time
- UPnP
- Event Log

Configuring Device Security

This screen allows you to change your user ID and password and to manage your router remotely.

To access the screen, click **Control Panel > Device Security**.

Login User ID	<input type="text" value="admin"/>
Login Password	<input type="password" value="*****"/>
Login Password Confirm	<input type="password" value="*****"/>
WAN Web Login	<input type="checkbox"/> enable
WAN Web Login Port	<input type="text" value="8080"/>
Login Idle Time	<input type="text" value="10"/> (min.)
WAN Ping Response	<input type="checkbox"/> enable

Field	Description
Login User ID	Changes the User ID used for logging into the router's Configuration Utility. It cannot be longer than 63 bytes. A blank user name is not allowed. The default is admin.

Field	Description
Login Password Login Password Confirm	Use this option to change the Password used to log into the router's Configuration Utility. It cannot be longer than 63 bytes. A blank password is not allowed. The default is motorola.
WAN Web Login	Enables you to log into the router from the Internet. Click to enable. The default is disabled.
WAN Web Login Port	Enables you to specify different ports on the router to allow remote login. The default is 8080.
Login Idle Time	Sets the amount of idle time (no actions occur) that elapses before the router automatically logs off the user. The default is 10 minutes.
WAN Ping Response	Enables a remote user to ping the router. Select to enable WAN Ping response. The default is disabled.
Apply	Click to save your settings.
Cancel	Click to cancel any changes.

Updating Firmware

The Firmware Update screen allows you to update your router's firmware (the mechanism that controls your router's hardware).

To check for a firmware update, access this website www.motorola.com/broadband/networking.

To update the firmware:

- 1 Download the latest firmware file to your computer from the Motorola website.
- 2 Click **Control Panel > Firmware Update** to access the Firmware Update screen:

The screenshot shows a yellow-themed interface for updating firmware. It displays the following information:

- Model Number:** WR850G
- Firmware Revision:** 3.00, Oct.27, 2003
- Firmware Update File:** A text input field is present, followed by a "Browse..." button.
- At the bottom center, there is a yellow "UPDATE" button.

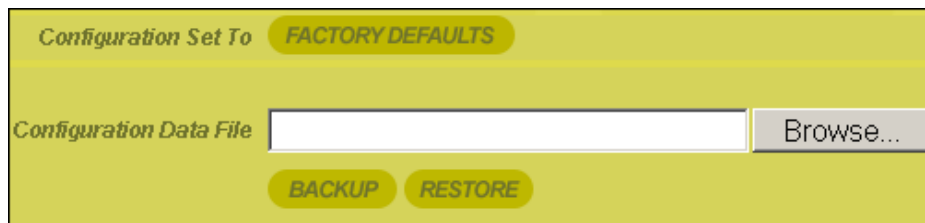
- 3 To locate the file you downloaded, type the path to the file or click **Browse** and navigate to it.

- 4 Click **Update** to update the router with the selected firmware file.
- 5 Follow the prompts to restart.

Saving and Restoring Configuration Settings

This Configuration Data screen allows you to save and restore your router's configuration settings. You are also able to reset the router to its factory default settings.

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



To reset the router 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.

Configuring Time Settings

The Time screen enables you to configure time settings.

To access the screen, click **Control Panel > Time**.

Field	Description
Current Time	Displays the current time.
Time Zone	Select your local time zone. The default is EST.
Auto Daylight Adjust	If you want to automatically adjust for Daylight Savings Time, check to enable this feature. The default is enabled.
NTP Time Synchronization	If you want to automatically check the current time, check to enable this feature. The default is enabled.
NTP Server 1, 2, 3	Enter the current Network Time Protocol (NTP) servers from which you can choose to synchronize your device. A listing of public NTP servers, their access policies, and their Service Areas can be found through the following URL: http://www.ntp.org . To change, enter the host name or IP address for a desired Time Server.
Apply	Click to save your settings.
Cancel	Click to cancel any changes.

Configuring UPnP

The UPnP screen allows you to enable/disable Universal Plug and Play (UPnP). UPnP allows an application to smoothly map to the router.

To access the screen, click **Control Panel > UPnP**.

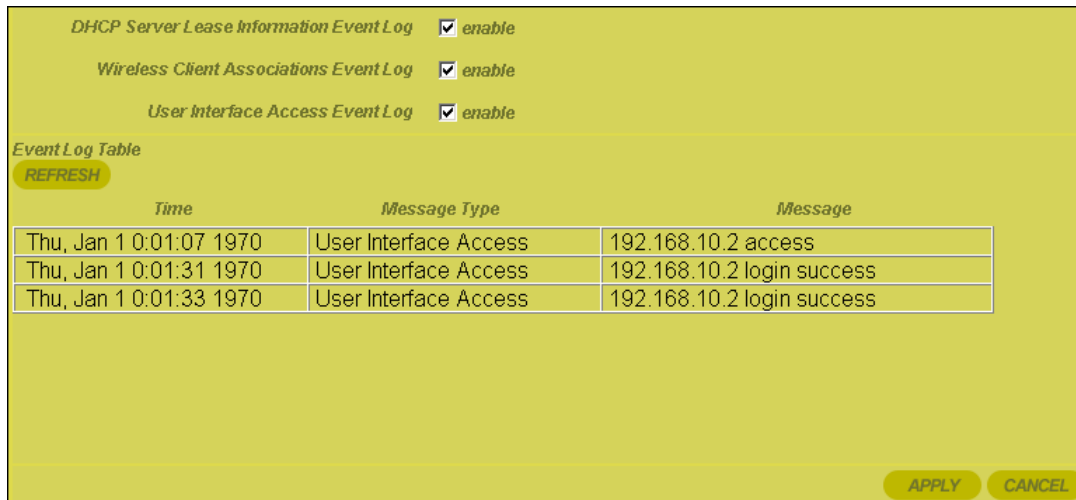


Field	Description
LAN UPnP Device	Click to enable this feature. The default is disabled.
Apply	Click to save your settings.
Cancel	Click to cancel your changes.

Enabling Event Logs

An event is a message generated by your router that indicates an action has occurred on your network. The Event Log screen enables you to view information about events, including date, time, and a brief description of the event.

To access the screen, click **Control Panel > Event Log**.



Click to enable the different types of Event Log information to track. After making your selections, click Restart to initiate your selections.

- DHCP Server Lease Information lists information about leases handed out to devices on the LAN.
- Wireless Client lists information about wireless clients that have attempted to associate with the Router.
- User Interface lists information about accesses to the router's Configuration Utility.

Click **Apply** to save your settings or **Cancel** to cancel changes.

Section 4: Troubleshooting

This section details possible solutions to common problems that might occur in using the router.

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 router is powered on and that the Wireless LED is flashing.
- 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 wireless router have the same security settings that will allow your computer to access the wireless network. Also, verify that the Access Control List (ACL) is not configured to block your PC. For details on adjusting your security settings, see Configuring Wireless Security Settings in Section 3: Configuration.
- Ensure that your wireless adapter is within range of your router or is not behind an obstruction. For example, metal structures will interfere with the signal, as will 2.4 GHz cordless phones, and microwaves.
- Ensure that your router's antenna is connected and that your PC's wireless adapter antenna is also connected.

My computer is experiencing difficulty in connecting to the router.

- Ensure that all of your cabling connections are firmly connected. This includes the cables from the wall to your modem, between the router and modem, and, if available, from the router 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 or router and PC. See the illustration below. 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. To check the status of your adapter, click the monitor icon in the System Tray at the bottom right of your screen. 
You can also check the status of the Ethernet adapter by selecting **Control Panel > Network and Dial-Up Connections**.

My broadband modem already uses a built-in router.

Because the two routers will cancel each other out, turn off the NAT function in the modem to enable access for your router. Refer to your modem's documentation for further instructions.

Software Solutions

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

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 Configure Your Computers in Section 2: Configuration, for further details.

- 1 Open a command prompt by clicking **Start** and **Run**.
- 2 For Windows 98 and ME, in the Open field, type **command** and press **Enter** or **OK**.
For Windows 2000 and XP, type **cmd**. Or, navigate using your **Start** button to **Programs>Accessories>Command Prompt**.
- 3 In the Command window, type **ipconfig**.
 - You should see an IP address for your network adapter:

```

Ethernet Adapter Local Area Connection:

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

IP Address. . . . . : 192.168.10.10

Subnet Mask . . . . . : 255.255.255.0

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

- 4 In the *Command* window, type **ping** followed by the **Router's IP address** and press **Enter**.
 - If you receive a reply (the first word will be *Reply...*), then your computer is connected to the router. Proceed to *Step 4*.
 - If you do NOT receive a reply, repeat steps 1 – 4 on a different computer to verify that the first computer is not the cause of the problem.

Your computer's Default Gateway's IP address may also be your router's IP address. Verify the router's IP address by logging on to the router's Configuration Utility and selecting **Internet > Basic**.

- 5 In the Command window, type **ping** followed by your **ISP's default gateway** and press **Enter**.
 - If you receive a reply (For example: *Reply from 216.109.125.72...*), then your connection to the Internet is live.

To verify the ISP default gateway's IP address, log on to the router's Configuration Utility, select **Internet > Basic**, and verify the address in the Default Gateway field.

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

I cannot access the Configuration Utility for the router.

- Verify your Ethernet connection to the router.
- 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 IP address of your network adapter must be on the same network and not a duplicate of any others on the network (for example: 192.168.10.10 and using a subnet mask of 255.255.255.0 can be used to login to the router's default IP address of 192.168.10.1). To adjust the IP address for your PC, refer to Configure Your Computers in Section 2: Configuration.
- Verify that you can ping the router on this IP address.
- In the *Command* window, type **ping** and your router's default IP address and press **Enter**.
- If you have changed the factory configured default IP address of the router, you will need to set your network adapter accordingly.
- Verify you are entering the correct URL in the browser. The default is <http://192.168.10.1>. If you think you have changed the IP address used to configure the router 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 router's user settings, including User ID, Password, IP Address, and Subnet mask.
- Once the router is reset to factory default, re-verify the Ethernet connectivity and IP address issues.

How do I extend my wireless network to cover more area?

You need more than one access point with WDS (Wireless Distribution System) enabled to expand your wireless network. For example, if you are running a WR850G or WR850GP, you will need another wireless Access Point (AP), most likely a WA840G or WA840GP (but you can use another WR850G or WR850GP, just ensure that you do not run two DHCP servers at the same time).

Set up both the WR850 and the WA840 with the same Wireless SSID and Pass Phrase or WEP keys. Also, ensure that WDS is enabled on both units (found on the **Wireless > Advanced** tab of your **Configuration Utility**). It is suggested that you also enable WDS Restrict Mode to limit the exposure of your wireless network to outside users. The wireless MAC addresses of both APs need to be added to both APs when using WDS Restrict Mode, i.e. the WA840's wireless MAC address needs to be in the WR850's WDS Restrict Mode list, and vice versa.

Once enabled, your laptop can now roam between the two APs, thereby extending your wireless network. Currently, WDS will not work with WPA enabled, in that case; only WEP will be available for wireless encryption.

I cannot browse past the first screen of the Configuration Utility.

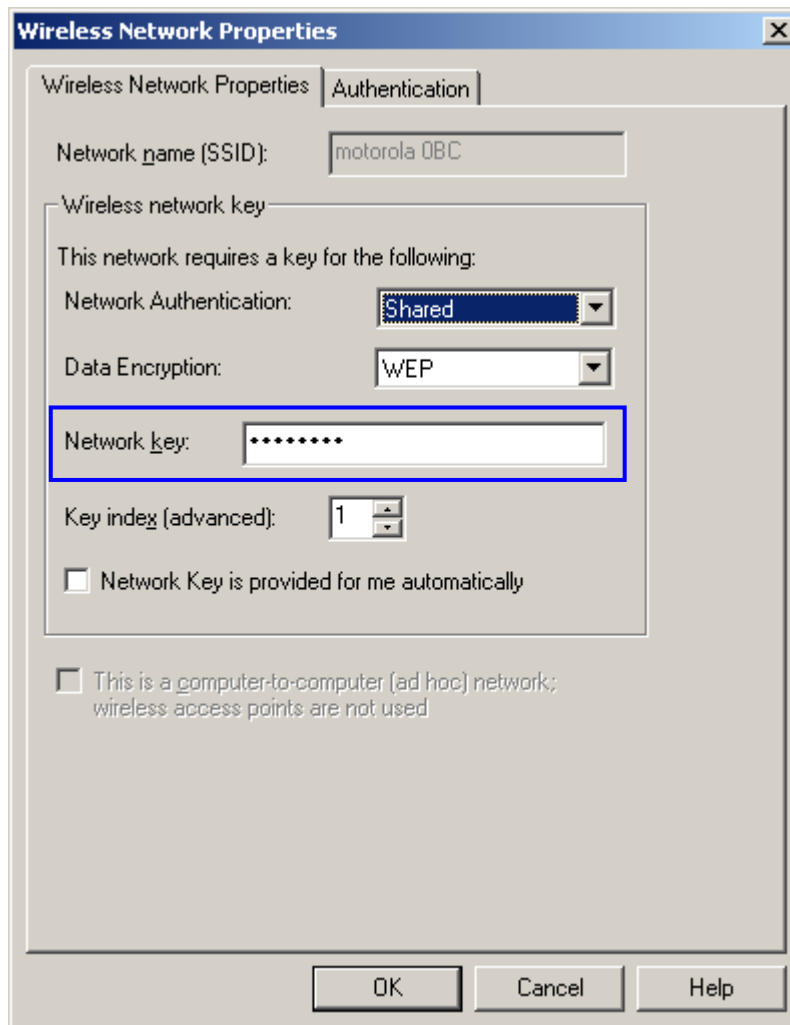
Sometimes, especially when upgrading, some leftover files may be in your Internet Cache. Flush your cache and restart your unit to fix. From Internet Explorer's menu, select **Tools > Options** and click **Delete Files** to clear your cache.

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

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

Key Content	
Key 1	03F32226A6E587A3F611
Key 2	F6684088B19A42DFF63

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



Section 5:Glossary

A

Access Point (AP)

A device that provides wireless LAN connectivity to wireless clients (stations). The WR850 acts as a wireless access point.

Adapter

A device or card that connects a computer, printer, or other peripheral device to the network or to some other device. A wireless adapter connects a computer to the 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:

The WR850 is simultaneously a DHCP client and a DHCP server.

- A DHCP server at the system headend assigns a public IP address to the WR850.
- The WR850 contains a built-in DHCP server that assigns private IP addresses to clients.

DMZ

DeMilitarized Zone. This service opens one IP address to the Internet, usually for online gaming, and acts as a buffer between the Internet and your network.

DNS

The Domain Name System is the Internet system for converting domain names (like www.motorola.com) to IP addresses. A DNS server contains a table matching domain names such as Internetname.com to IP addresses such as 192.169.9.1. When you access the world-wide web, a DNS server translates the URL displayed on the browser to the destination website IP address. The DNS lookup table is a distributed Internet database; no one DNS server lists all domain name to IP address matches.

Domain Name

A unique name, such as motorola.com, that maps to an IP address. Domain names are typically much easier to remember than are IP addresses. See *DNS*.

Download

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

Driver

Software that enables a computer to interact with a network or other device. For example, there are drivers for printers, monitors, graphics adapters, modems, Ethernet, USB, HPNA, and many others.

DSL

Digital Subscriber Line

DSSS

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

Dynamic IP Address

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

E**ESS**

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

Ethernet

The most widely used LAN type, also known as IEEE 802.3. The most common Ethernet networks are 10Base-T, which provide transmission speeds up to 10 Mbps, usually over unshielded, twisted-pair wire terminated with RJ-45 connectors. Fast Ethernet (100Base-T) provides speeds up to 100 Mbps. "Base" means "baseband technology" and "T" means "twisted pair cable."

Each Ethernet port has a physical address called the MAC address. Also see *MAC address*.

Event

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

F**Firewall**

A security software system on the WR850 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*.

The WR850 enables up to 253 computers supporting IEEE 802.11b/g or Ethernet to share a single broadband Internet connection.

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 8 million bits.

Mbps

Million bits per second (megabits per second). A rate of data transfer.

MTU

The Maximum Transmission Unit is the largest amount of data that can be transmitted in one discrete message on a given physical network. The MTU places an upper bound limit 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 WR850 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 WR850 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 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 4 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 is 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 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



516587-001
7/04

MGBI