User Guide

Wireless Broadband Router

WR850G

MOTOROLA

intelligence everywhere™

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

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

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

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

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

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

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

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

Place this equipment on a stable surface.

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

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

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

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

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

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

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

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

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

Installation must at all times conform to local regulations.

FCC Compliance Class B Digital Device

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

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

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

Canadian Compliance

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

FCC Declaration of Conformity

Motorola, Inc., Broadband Communications Sector, 101 Tournament Drive, Horsham, PA 19044, 1-215-323-1000, declares under sole responsibility that the WR850G, WE800G, WA840G, WN825G, WPCI810G, and BR700 compile with 47 CFR Parts 2 and 15 of the FCC Rules as a Class B digital device. This device complies with Part 15 of FCC Rules. Operation of the device is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference that may cause undesired operation.

Wireless LAN Information

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

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

Wireless LAN and your Health

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

Restrictions on Use of Wireless Devices

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

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

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

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

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

FCC Certification

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

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

Canada - Industry Canada (IC)

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

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

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

Contents

Section 3:Configuration 3-1

Section 4:Troubleshooting 4-1

Section 5:Glossary 5-1

Section 1:Overview

Congratulations on purchasing the Motorola WR850G Wireless Broadband Router. With this router you have entered the world of freedom and independence – freedom from wires and the independence to communicate wherever YOU choose.

The WR850G is built with both the popular 802.11b wireless standard and the new nearly 5-times-faster 802.11g standard, providing you the ultimate in flexibility and speed. With Wi-Fi® Protected Access (WPA) included, your wireless connections are robust and secure, giving you the security to communicate without fear that your signal might be compromised.

Upgradeable firmware keeps the router's control software up-to-date. The WR850G captures the latest technology in a package that stays current, protects your home network, and provides you easy home network management.

Wireless Broadband Router WR850G

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

- Wireless Access Point
- 4-port Full Duplex 10/100 Ethernet Switch and Router
- Firewall and NAT protection

Wireless Access Point

Connects your router to your laptop wirelessly and allows you to roam unfettered. Using the 802.11g and 802.11b standards ensures compliance now and into the future. WPA ensures that your laptop communicates with your router without fear of hackers listening in.

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

Enables connection of up to 4 PCs directly, or using optional Motorola Home Networking Wireless products extends your network. The routing function enables each of your networked PCs to share a broadband Internet (cable, DSL, or other) connection.

Firewall and NAT Protection

Protection against Internet intruders is crucial. Of course, the product also supports Virtual Private Network (VPN) connections through the firewall, allowing you the freedom to connect when you need it.

Also supported are the WEP (Wired Equivalent Privacy) and MAC address filtering protocols, giving you the choice to share your Internet connection with only those whom you designate.

Your Motorola Wireless Broadband Router WR850G protects and connects you by sharing your files, Internet connection, printers and multi-player games, all in one great unit.

Features

The WR850G has the following features:

- CD-ROM based Installation Wizard to provide easy installation
- Web-based configuration of features using any web browser
- Wireless security using WPA, 802.1X Authentication, and Advanced Encryption Standard (AES)
- Compatibility with both 802.11g and 802.11b standards
- Wireless Distribution System (WDS) mode supporting peer-to-peer communication with other WR850G or WA840G units
- Firmware upgrade to stay current with latest specifications
- Firewall protection with NAT translation, IP and MAC address filtering

- A built-in DHCP server to easily configure a private Local Area Network (LAN)
- Virtual Private Network (VPN) pass-through allowing remote connection with your corporate network

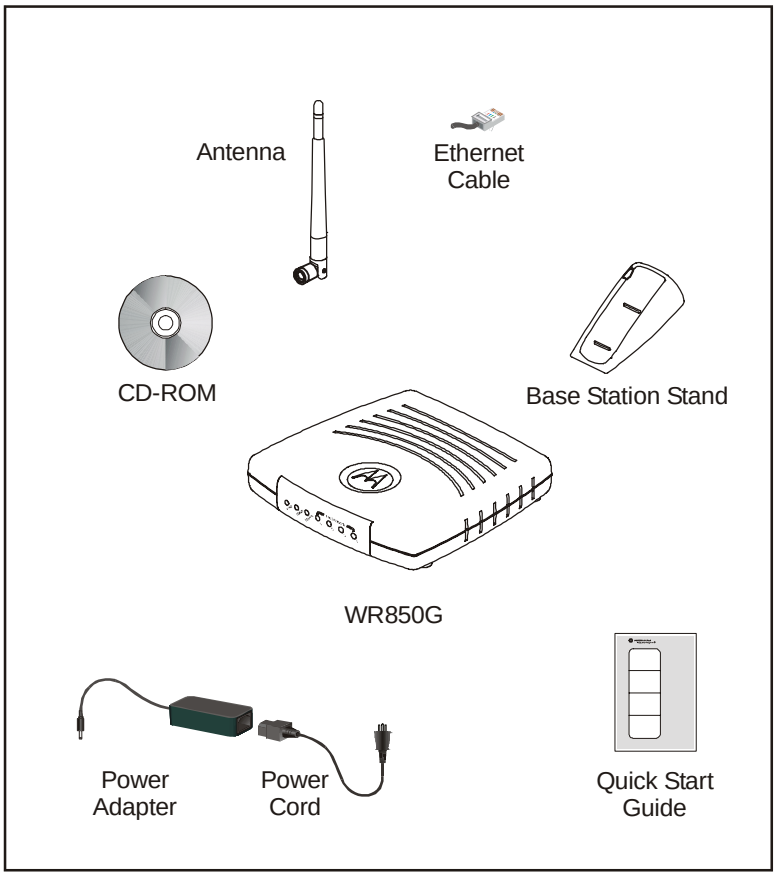
Understanding your User Guide

The User Guide is subdivided into the following sections:

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

Box Contents

Your box contains the following:



Understanding Functions

The various technologies and features utilized by your wireless router require some explanation so you can make the correct choices when configuring your wireless router.

Router

Routers connect two networks together, or in your case, 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 where it does not belong.

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.

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 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 more information in *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.

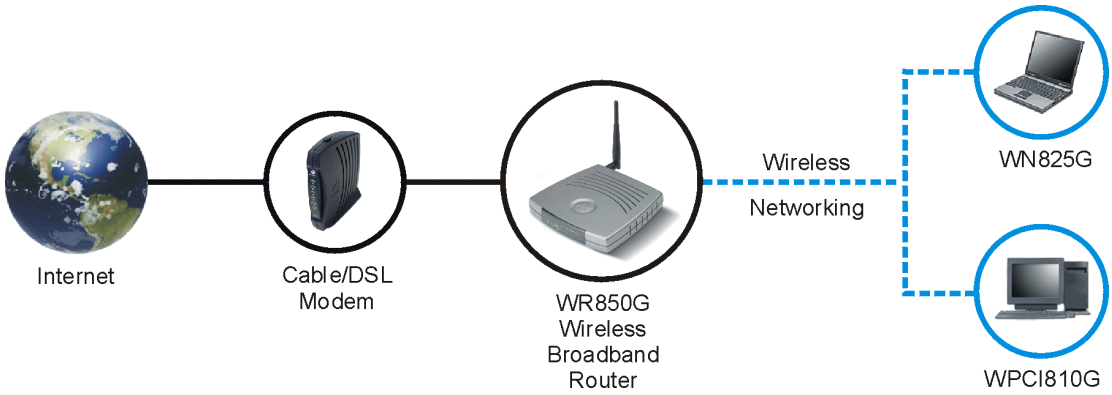
If using your wireless router to share an Internet connection, your ISP might have assigned you a dynamic IP address, which you use when configuring your router. See more information in *Configuration*.

DHCP Server

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

Simple 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 Local Area Network (LAN) 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, sending information to whichever device asks for information, be it from requests for Internet access to file sharing to 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.

Wireless Connections

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.

Wireless Range

The following lists the expected wireless range of the unit. This table is only a guide and coverage varies due to local conditions.

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

Recommended Wireless Environment

The following information helps you achieve the best wireless performance:

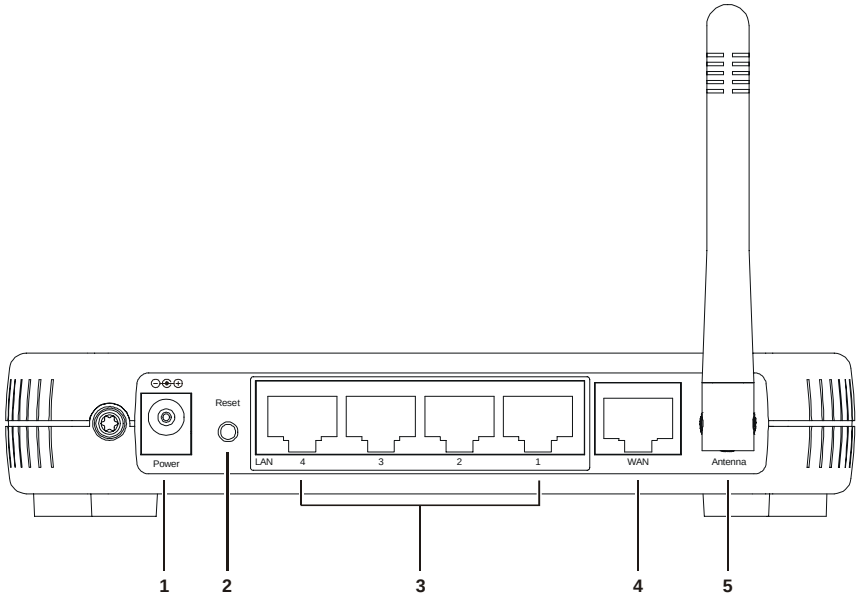
- Placing your base station in the physical center of your network is the best location because the antenna sends out the signal in all directions.
- Placing the unit in a higher location, such as on top of a cabinet, helps disperse the signal cleanly, especially to receiving locations on upper stories.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

Router Physical Description

The following sections describe the physical characteristics of your unit.

Back of Router

The following illustration shows the WR850G back panel:

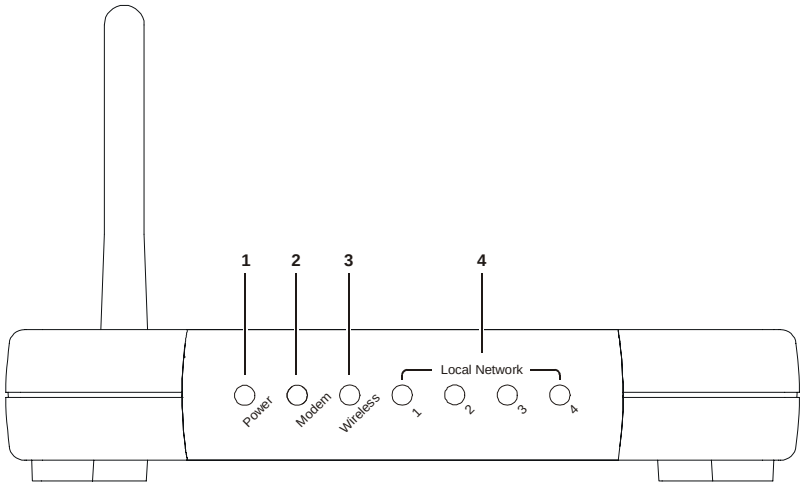


	Feature	Description
1	Power	The receptacle where you plug in the power adapter.
2	Reset Button	A dual-function button. It either resets your unit or resets the unit to the default login settings. If the router is experiencing trouble connecting to the Internet, briefly press and release the Reset button to reset the router. This retains the router's configuration information. To reset the unit to the factory defaults, press and hold the Reset button for more than 5 seconds. This clears the router's user settings, including User ID, Password, IP Address, and Subnet mask. Refer to the *Configuration* section for re-configuring the router.

	Feature	Description
3	LAN Ports 1-4	These four ports can connect your LAN with 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. Any of these four ports can also serve as an uplink port to other network devices, such as another router or switch, enabling you to extend your network.
4	WAN	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.
5	Antenna	The antenna used for wireless connections. You are able to rotate the antenna to gain the best signal reception.

Front of Router

The following illustration shows the WR850G 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 keeps blinking 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/Blinking	**Amber**	10BaseT link detected/active traffic present.
	ON/Blinking	**Green**	100BaseT link detected/active traffic present.
3 Wireless	OFF	**None**	No mobile station or Access Point has associated with this device.
	ON	**Red**	The wireless interface has been disabled by the firmware.
	ON/Blinking	**Amber**	802.11b connection exists in this wireless domain/active traffic present.
	ON/Blinking	**Green**	802.11g connection exists in this wireless domain/active traffic present.
4 LAN (x4)	OFF	**None**	No external Ethernet device has been attached and detected. The Ethernet link is down.
	ON/Blinking	**Amber**	10BaseT link detected/active traffic present.
	ON/Blinking	**Green**	100BaseT link detected/active traffic present.

Section 2:Installation

To get your network up and running:

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

If you prefer to setup 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

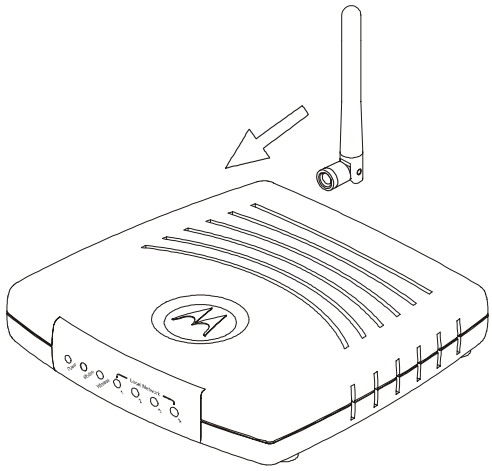
Hardware setup includes:

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

Antenna Installation

When shipped, the antenna is separate from the main unit. You are required to attach the antenna to the main unit.

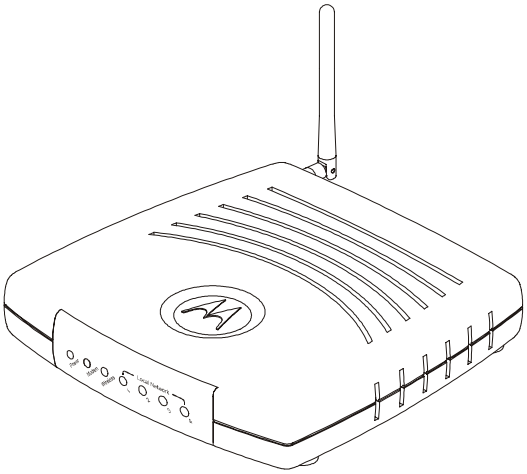
1. Take the bottom of the antenna and locate, on the right backside of the unit, the threaded knob.
2. Screw the antenna connector clockwise on to the threaded knob until firmly seated. Do not overtighten.



Router Physical Installation

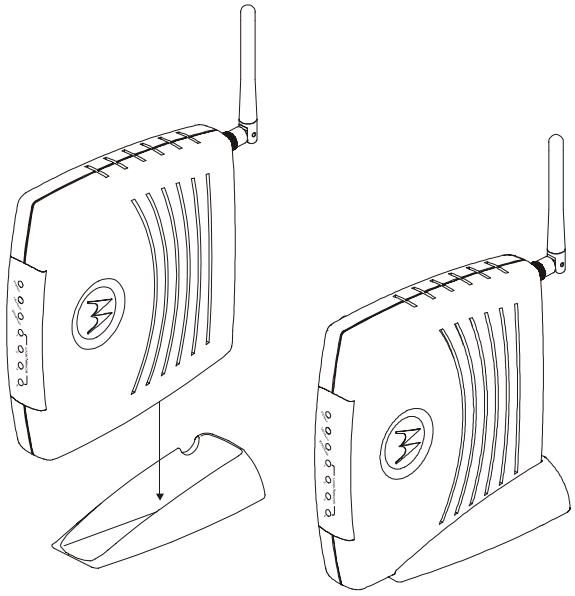
You can install the router in various physical orientations – horizontally, vertically, or hung on the wall. Your own needs determine the best placement.

Horizontal Installation



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

Vertical Installation



1 To use the router in a vertical position, 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 unit stable.

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

Wall Mount Installation

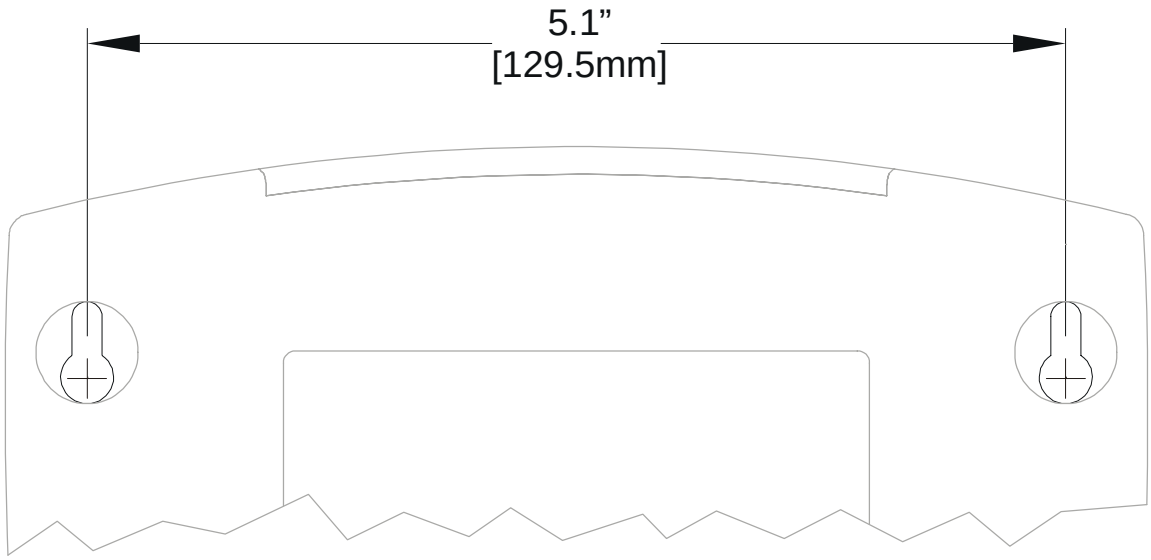
If you mount the router on the wall, you must:

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

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

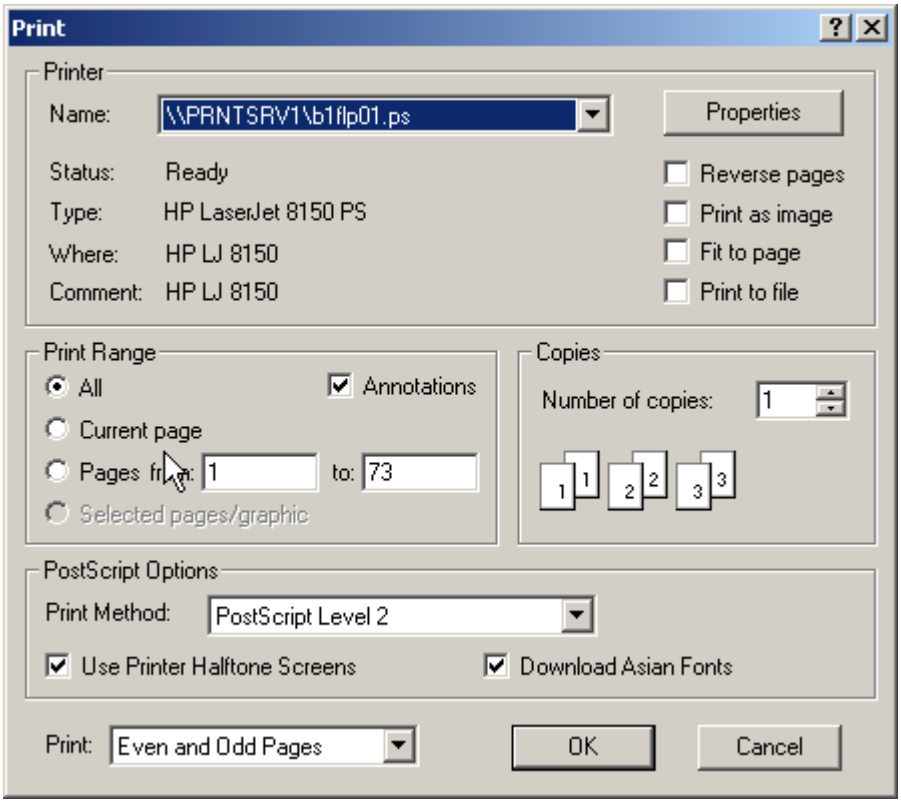
To mount your router on the wall:

1 Print the Wall Mounting Template:



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

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



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

3 Click **OK**.

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

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

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

WARNING!

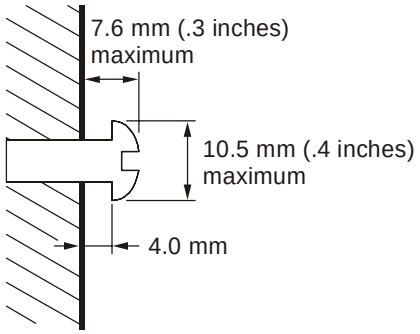
Before drilling holes, check the structure for potential damage to water, gas, or electric lines.

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

8 If necessary, seat an anchor in each hole. Use M5 x 38 mm (#10-16 x 11/2 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.

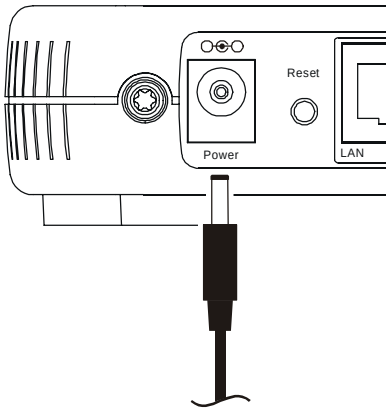
11 Place the router so the keyholes are above the mounting screws.

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 unit.

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:



To power supply

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

Easy Software Setup

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

Manual Software Setup

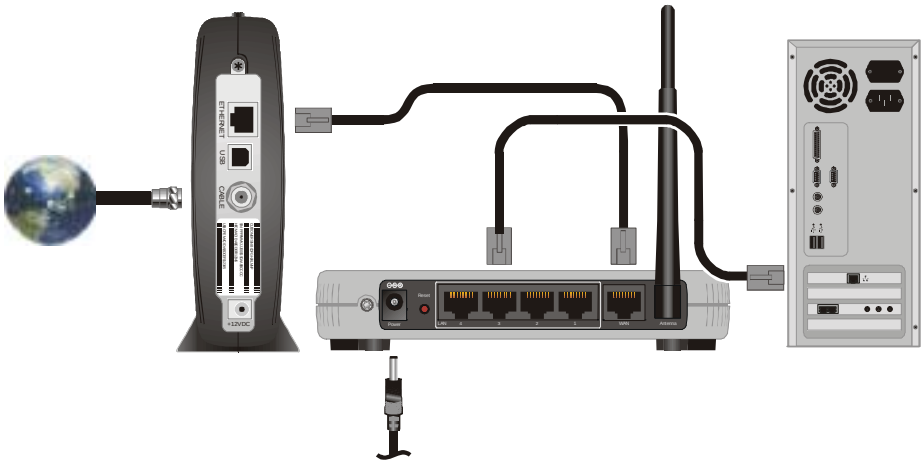
If you'd prefer to manually setup your network, use this section to configure it. This section details the physical connection of the router to your network as well as the configuration needed by your PC.

To set up your wireless network:

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

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

Wired Connection to 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 have been running broadband to a single computer before, 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.
2. If you have not been running broadband to a single computer, take one end of an Ethernet cable and plug it into the WAN port. The WAN port is the only port that works for your connection from the modem to the router.
3. Take the other end of the same cable and plug it into 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.
4. To connect the PC to the router, use a different Ethernet cable and plug it into your Ethernet port on your PC.
5. Use the other end of the same cable and plug it into one of the LAN ports on your router. You have now connected your PC to the router.
6. To connect more devices, repeat steps 4 and 5.
7. To configure the router, refer to *Section 3: Configuration*.

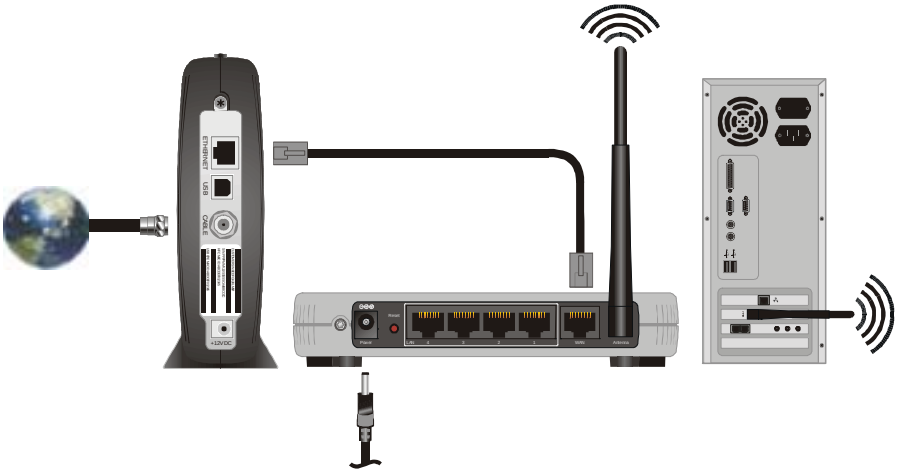
Wireless Connection to Router

WARNING!

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

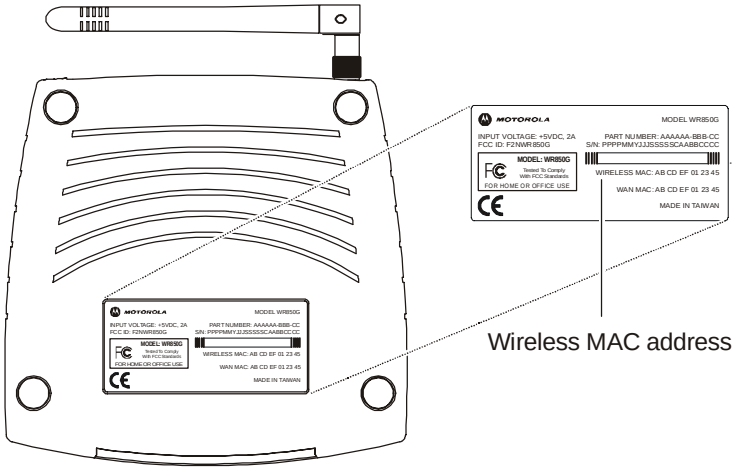
If you are connecting your client (most likely a PC) wirelessly to the router, you can use the Motorola WPCI810G, a wireless PCI card for your desktop PC. If you have a laptop, the Motorola WN825G wireless PC card provides access.

Note: The WN825G/WPCI810G is not supported under Windows 95, 98, nor NT. To connect the router to the modem, you need at least one Ethernet cable.



1. If you have been running broadband to a single computer before, unplug the cable, that runs between your modem and PC, and plug it into the port labeled WAN on the back of your router. Otherwise, take one end of an Ethernet cable and plug it into the WAN port. The WAN port is the only port that works for your connection from the modem to the router.
2. If the same cable isn't plugged in already, take the other end of the cable and plug it into 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.

3 To connect the PC to the router through a wireless connection, ensure 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 device's documentation for instructions on how to activate these settings.

4 To configure the router, refer to *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 is going to be part of your network needs to "talk" to 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

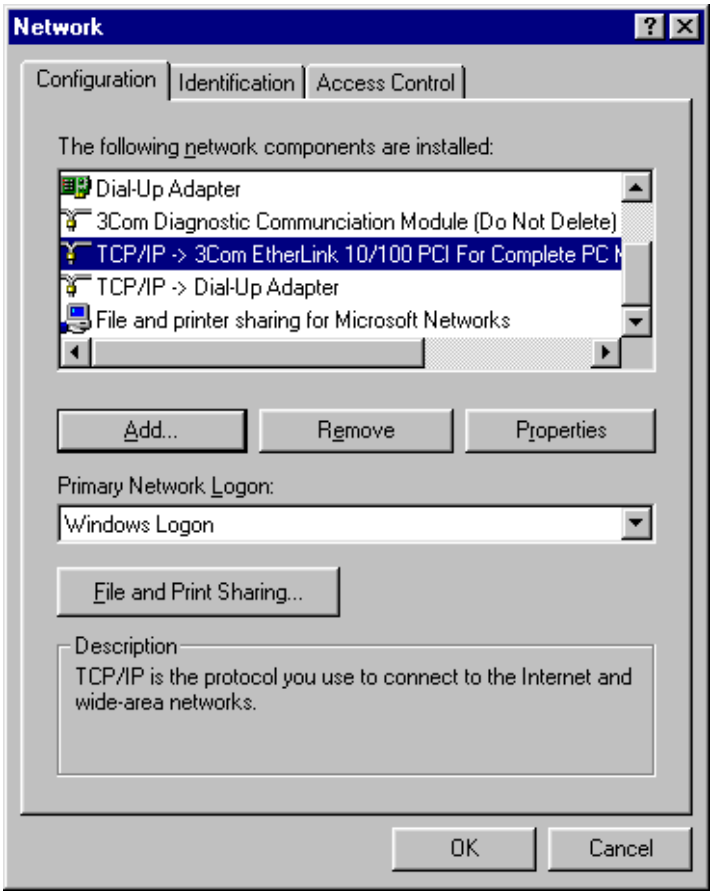
Determine the operating system for each computer you are including in your wireless network and follow the steps to configure the network settings for that PC.

Configuring Windows 98SE and ME

1 Click **Start**.

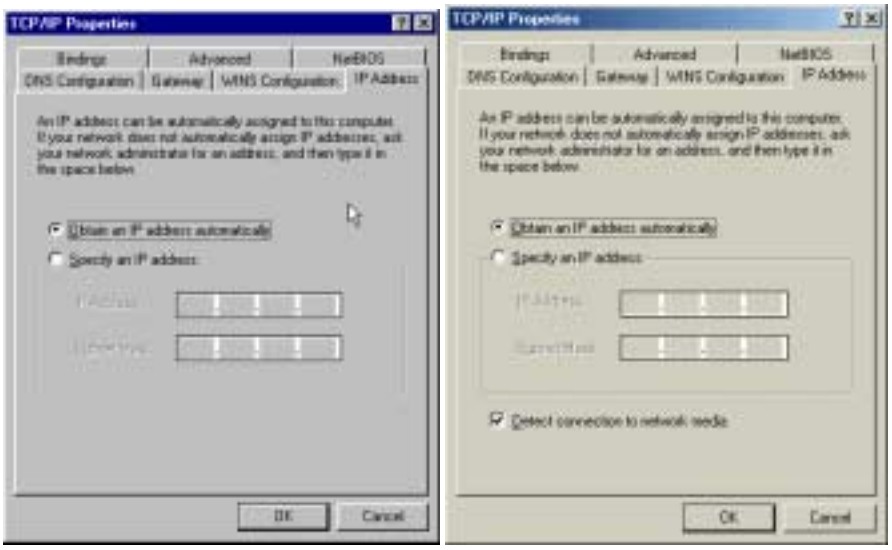
2 Select Settings > Control Panel.

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



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

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



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 check to make sure that the *Installed Gateway* field is blank.

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

11 Restart your computer to save your settings.

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

Configuring Windows 2000

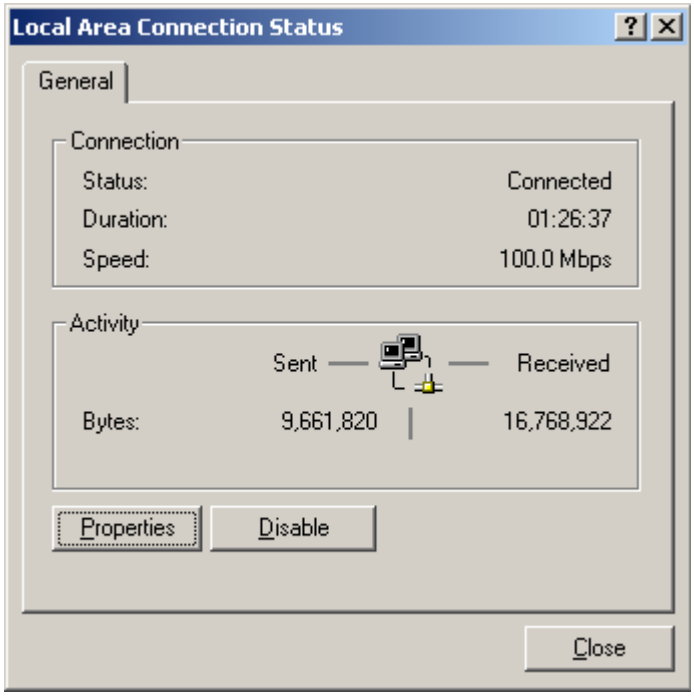
1 Click **Start**.

2 Select **Settings**.

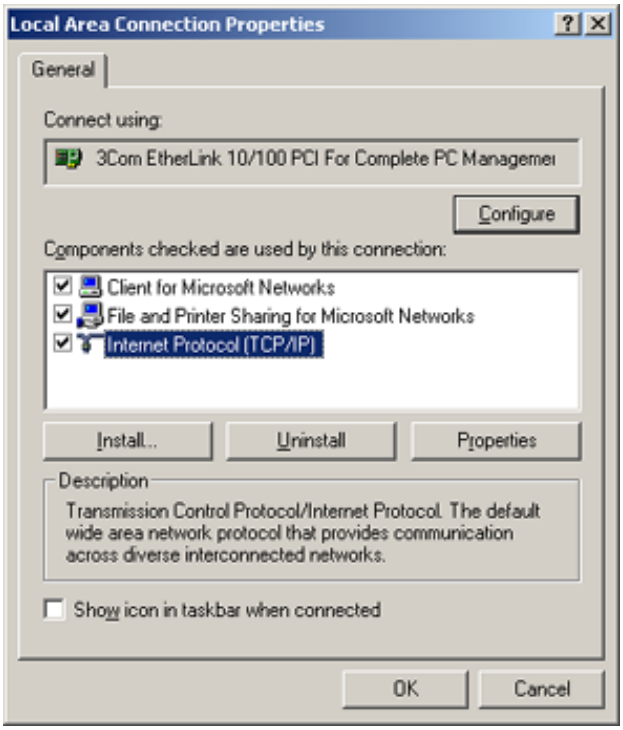
3 Select **Control Panel**.

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

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

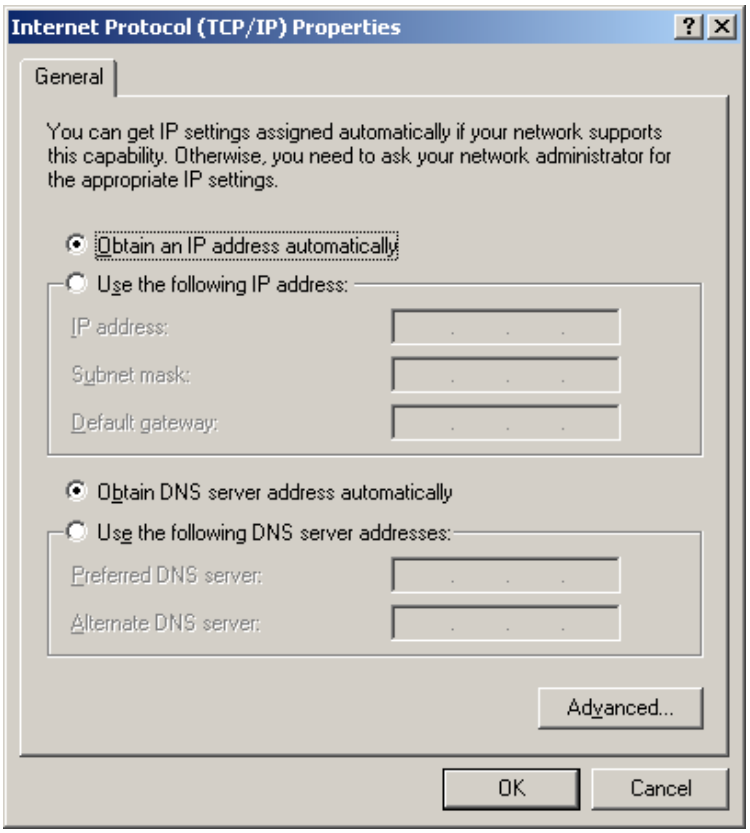


6 Click the **Properties** button.



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

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



9 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 Settings* section to set up the security settings.

Configuring Windows XP

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

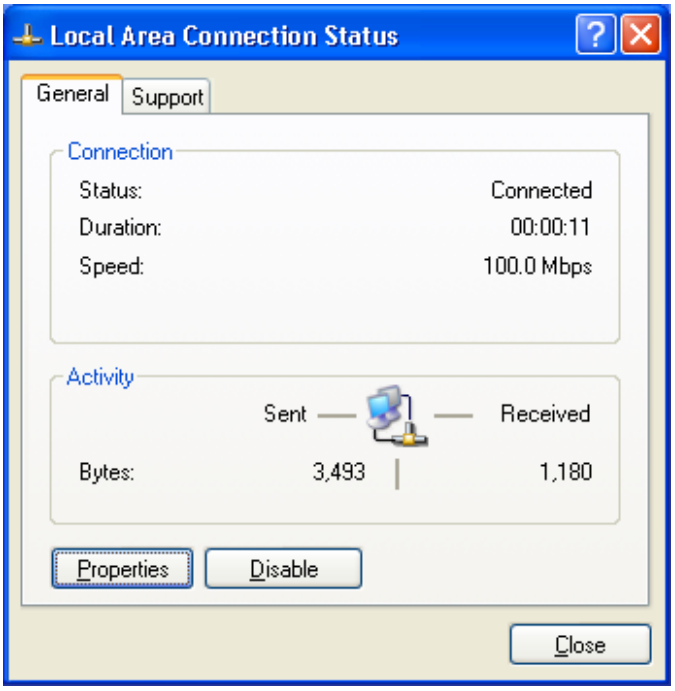
1 Click **Start**.

2 Select **Settings**.

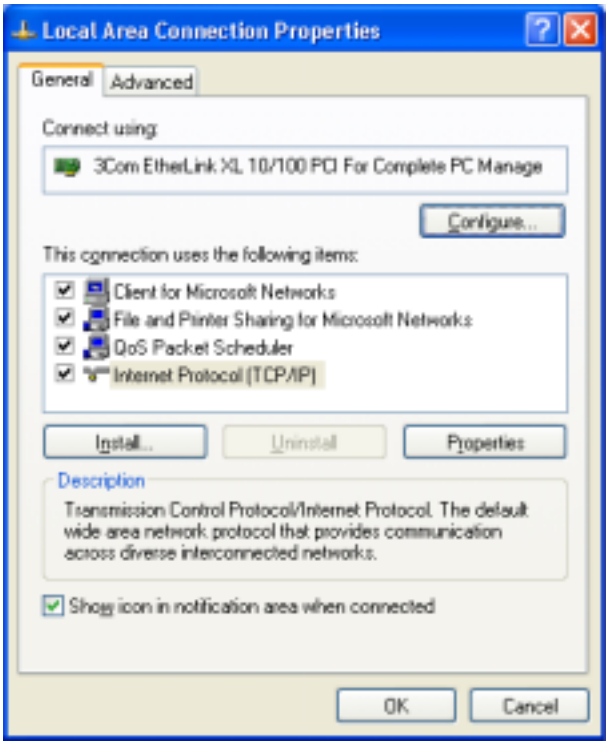
3 Select **Control Panel**.

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

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

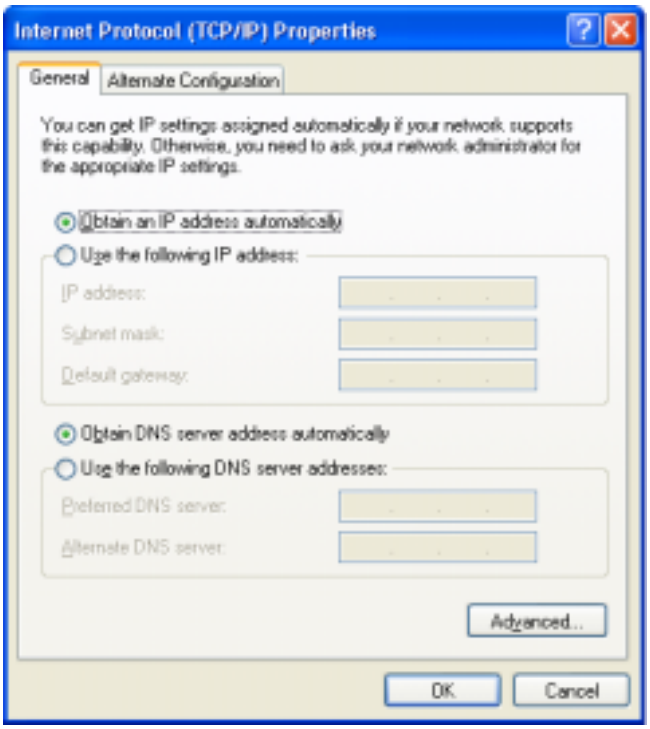


6 Click the **Properties** button.



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

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



9 Click **Obtain an IP address automatically**. Click **OK** twice to exit and save your settings.

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

Configure Your Wireless Security Settings

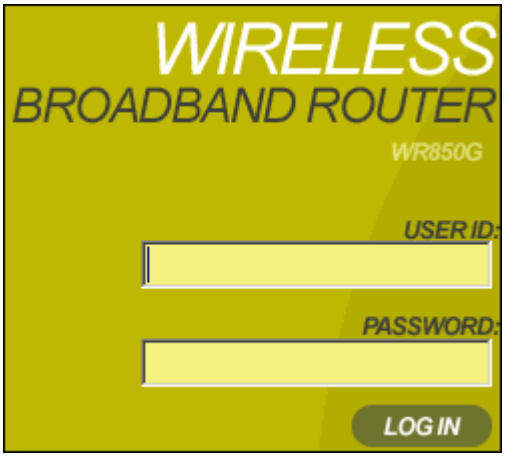
Your router requires adjustments to ensure that all security settings are enabled before you communicate securely with your computer. Failure to configure these settings properly could compromise your network to wireless hackers.

Logging In

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

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

2 The login screen appears.



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

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

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

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

Wireless Security Setup

To setup the correct security protocols for your router:

1. Click **Control Panel** > **Device Security**.
2. In the Login User ID field, enter the desired ***User ID***. For strong security, select 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 the desired ***Login Password***. For strong security, select an ID that contains multiple case-sensitive characters as well as numbers and symbols like "_ +)". It cannot be longer than 64 bytes.
4. Re-enter the same Password.
5. Click **Apply**.
6. Once the settings have been accepted, click **Restart** and log back into the *Configuration Utility* using your new User ID and Password.
7. Navigate to **Wireless** > **Basic**.
8. Change the ***SSID*** to a user-friendly name and click **Apply**.
9. Navigate to **Wireless** > **Security**.
10. Select **WPA-PSK** from the ESS Authentication Mode options.
11. Select **AES** from ESS Encryption Status options.
12. Click **Apply** and click **Restart** again. Your wireless security configuration is now complete.

Configure Your Basic Internet Settings

The following settings illustrate how to 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*. You are presented with the **Internet** > **Basic** screen.
2. Starting at the **Basic** screen, 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 appropriate fields to fill in the necessary information.

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 might have to enter the ***PPP Service Name*** into this field. Enter the information supplied by your ISP.
5. Click **Apply** to save the setting, or, if you want 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, or, 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, or, if you wish to start over, click **Clear**.

Section 3:Configuration

You can 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, view the status of the network, and more.

Using the Configuration Utility

Logging In

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

2 The login screen appears.

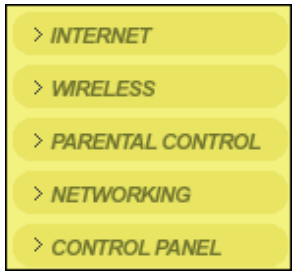
3 Enter the ***User ID***. The default factory setting is "admin", without the quotation marks.

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

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

Navigation

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



- Internet
- Wireless
- Parental Control
- Networking
- Control Panel

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

Configuring Internet Settings

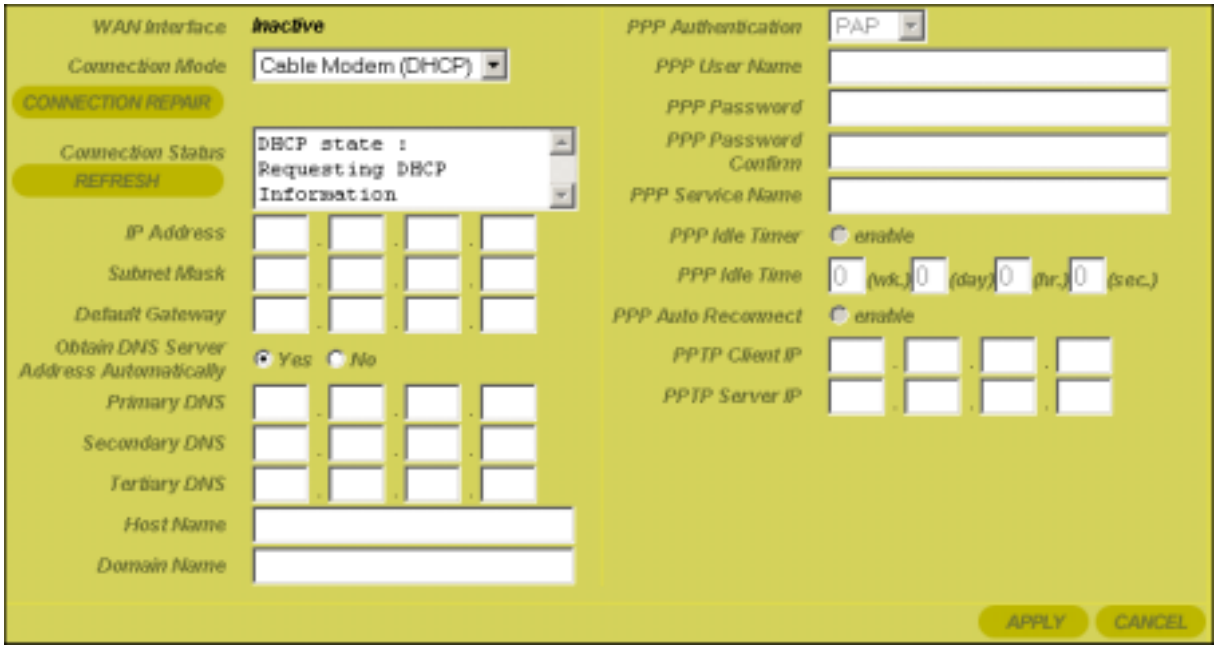
These screens enable you to configure your Internet settings:

- Basic
- Advanced
- Network Diagnostics

Internet - Basic

This is the first screen that appears when logging into the web-based utility. It enables you to adjust a large variety of the basic settings for configuring the router's Internet options. To access the screen, click **Internet** on the login screen.

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



Field or Button	Description
WAN Interface	Provides the status of the router: **Active** Your WAN link is active. **Inactive** Your WAN link is not active. **Disabled** The WAN interface has been disabled. This can be altered on the **Internet** > **Advanced** tab.
Connection Mode	The router supports four connection modes: ▪ Cable Modem (DHCP) ▪ DSL Modem (PPPoE) ▪ Static Assigned ▪ PPTP Select the appropriate connection method for your ISP (Internet Service Provider). Based on which connection type you select, different areas are grayed out (become inaccessible), leaving you only the appropriate fields to fill in. For details on each Connection Mode type, refer to *Section 2:Installation*.
Connection Repair	Provides connection repair information depending on the connection mode selected. For example, for DHCP, the router issues a request for a new IP address from the ISP's DHCP server.
Connection Status	Provides current information about the connection status of the router. Press the **Refresh** button to update the status of the router.

Field or Button	Description
IP Address	The router's *IP Address* used to connect to your ISP. It is either automatically displayed or manually entered from information provided by your ISP. 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.
Subnet Mask	Is either automatically displayed or manually entered from information provided by your ISP.
Default Gateway	Is either 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 either automatically displayed or manually entered from information provided by your ISP.
Secondary DNS	Is either automatically displayed or manually entered from information provided by your ISP.
Tertiary DNS	Is either automatically displayed or manually entered from information provided by your ISP.
Host Name	Is either automatically displayed or manually entered from information provided by your ISP.
Domain Name	Is either automatically displayed or manually entered from information provided by your ISP.

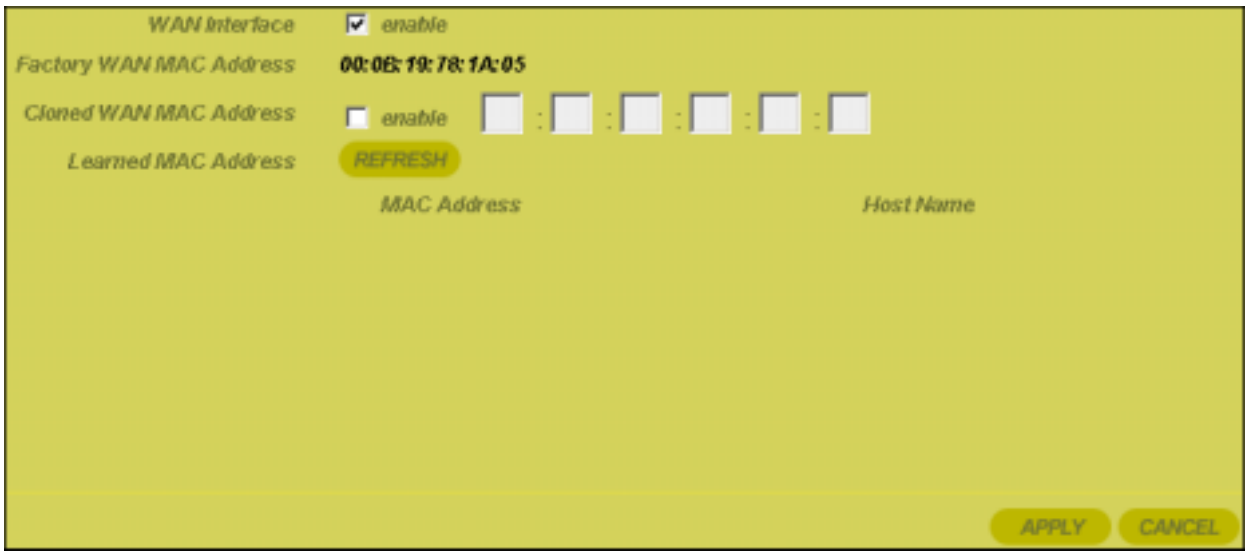
Field or Button	Description
PPP Authentication	Available when PPPoE or PPTP is selected in the Connection Mode. Check with your ISP for the proper type of authentication to choose. The default Auto. ▪ PAP – Password Authentication Protocol ▪ CHAP – Challenge Handshake Authentication Protocol ▪ Auto – The router will offer PAP, CHAP, or None to the server, and the server will determine which PPP Authentication to use. ▪ None – No authentication used.
PPP User Name	Is either automatically displayed or manually entered from information provided by your ISP.
PPP Password	Is either automatically displayed or manually entered from information provided by your ISP.
PPP Password Confirm	The same password as the PPP Password field.
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 Timeout	The amount of time to elapse before the router automatically breaks the connection to the Internet. Enter amount of time necessary for PPP Idle Timeout.
PPP Auto Reconnect	Enables the router to automatically reconnect to the Internet when the connection has been cut.
PPTP Client IP	Is either automatically displayed or manually entered from information provided by your ISP.

Field or Button	Description
PPTP Server IP	Is either automatically displayed or manually entered from information provided by your ISP.

Internet - Advanced

This screen enables you to adjust additional Internet settings. To access the screen, click **Internet** > **Advanced**.

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

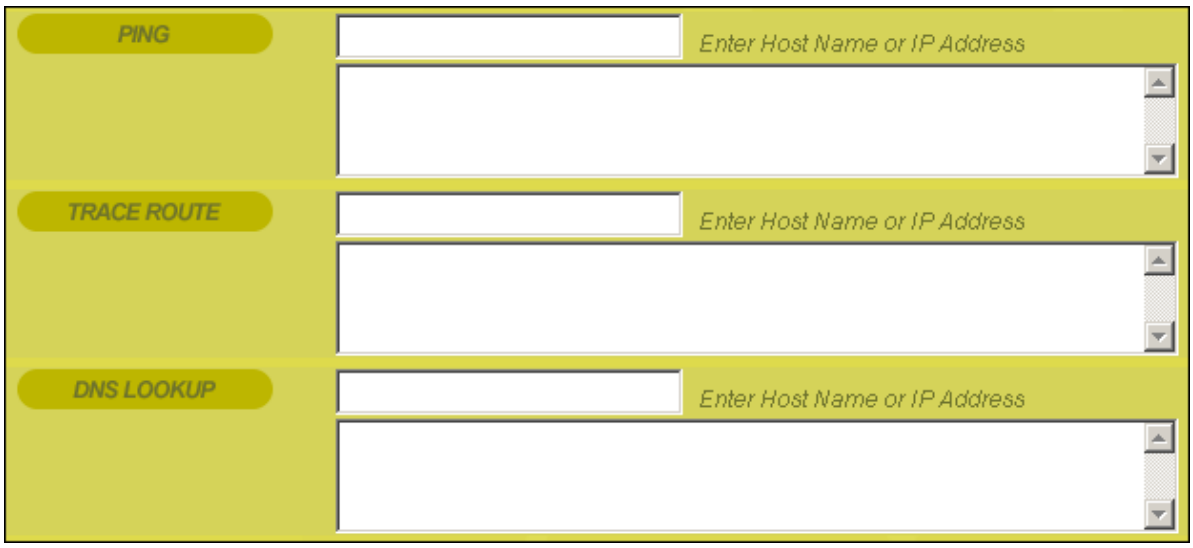


Field or Button	Description
WAN Interface	Select to enable the link to the Internet. By disabling this feature, your connection to the Internet is disconnected. The default is enabled.
Factory WAN MAC Address	The default MAC address of the WAN port. A MAC address is a 12-digit code assigned to a unique piece of hardware for identification. You can find the MAC address on the label on the bottom of your unit. Some ISPs require that you register the MAC address of your PC's network adapter.

Field or Button	Description
Cloned WAN MAC Address	Your router has the ability to duplicate the MAC address of your PC's network adapter into 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: **1** Click to **Enable** the displayed MAC address. **2** Enter a MAC address and click Apply.

Internet - Network Diagnostic

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



Field or Button	Description
Ping	An Internet utility used to determine whether a particular IP address is online by sending out a packet (block of data) and waiting for a response.
Trace Route	An Internet utility that traces the route from the client machine to the remote host being contacted. It reports the IP addresses of all the routers in between.

Field or Button	Description
DNS Lookup	An Internet utility that discovers the IP address of a website name. For example, if you enter www.yahoo.com, a DNS server returns the IP address of Yahoo.

All three utilities are initiated using the same method. Use the following procedure for each:

1 Enter the ***Host Name*** or ***IP Address*** for which you require information.

2 Click the **Ping**, **Trace Route**, or **DNS Lookup** button to activate the utility. The results of your query are displayed.

Configuring Wireless Network Settings

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

- Basic
- Security
- Site Monitor
- Advanced

Wireless - Basic

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

The default SSID is "*motorola XXX*", where *XXX* are the last 3 characters of your Wireless MAC address, found on the label on the bottom of the unit. It is strongly recommended that you change this to a unique name.

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

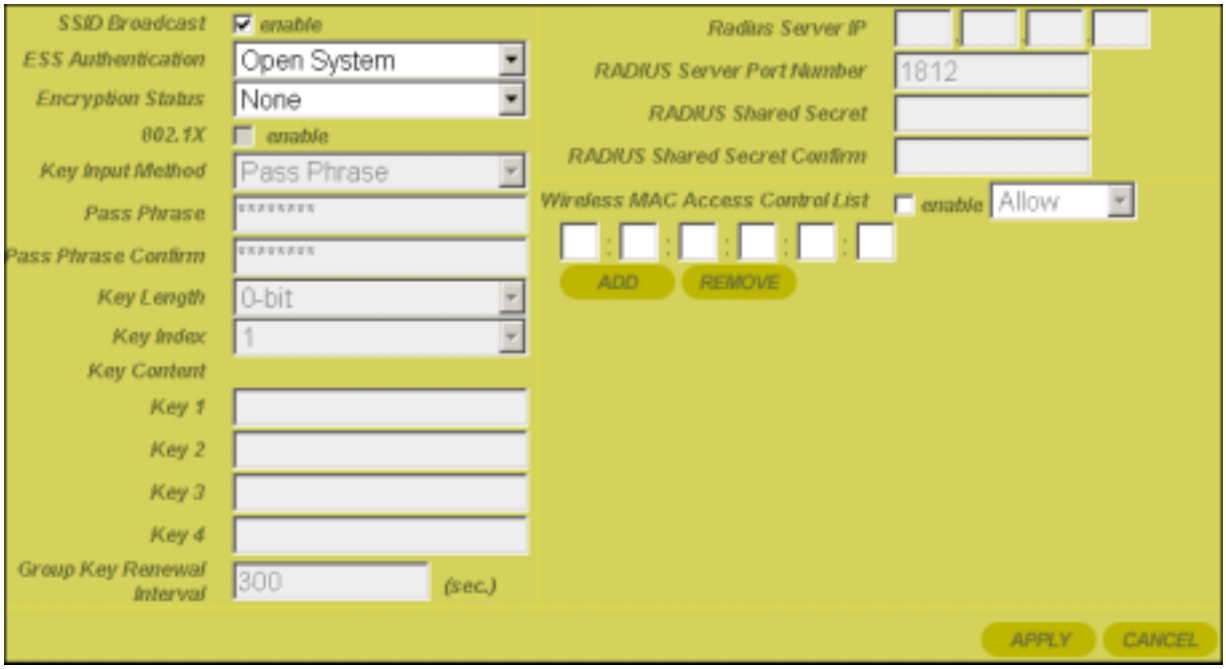
Click **Apply** to save your settings or **Cancel** to cancel changes.

Field or Button	Description
Network Name (SSID)	Enter a Network Name (SSID) of no more than 32 alphanumeric characters. This SSID must be entered on every wireless device on your wireless network to communicate with the router. The default SSID is "*motorola XXX*", 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. This can only be altered from a PC that is wired directly to the router, not wirelessly. The default is Channel 11.
Operation Mode	Enables you to select the type of transmission protocol your wireless network uses. The default is 802.11b/g The options are: ▪ Compatibility (802.11b/g) ▪ Performance (802.11g only) ▪ Legacy (802.11b only)
Wireless MAC Address	Displays the Wireless MAC address of the unit. This is different that the WAN MAC address.

Wireless - Security

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

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



Field	Description
SSID Broadcast	*Service Set Identifier (SSID)*. Broadcasts the SSID of the router to devices on your network. This enables wireless clients, like 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	*Extended Service Set (ESS*). Authentication differs from Encryption in that you are establishing either an open or secure verification of communication with an AP. This setting does not encrypt your transmission. The options are:

Open System	The Open System Authentication method is used, meaning no encryption is used
Pre-Shared Key (PSK)	The Pre-Shared Key (PSK) authentication method is used
WPA	Wi-Fi® Protected Access (WPA) authentication (802.1X) is used with an EAP type
WPA-PSK	WPA authentication (802.1X) is used with a pre-shared key

Select the option that best meets your needs. For home users, WPA-PSK is the best choice as it provides the strongest security without a RADIUS server.
The default is Open System.

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

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

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

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

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

Enable	Select to enable/disable the MAC Access Control List (ACL). When disabled, the MAC ACL is not active and any wireless station is allowed to communicate with the wireless 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.

To add a MAC address:

1. Check **Enable**.
2. Select **Allow** or **Deny**.
3. Enter a ***MAC address*** and click **Add** to enter the address into the ACL.
4. To alter a MAC address, remove and replace with the updated address.
5. After entering the MAC address(es), click **Apply** to save.

To delete a MAC address:

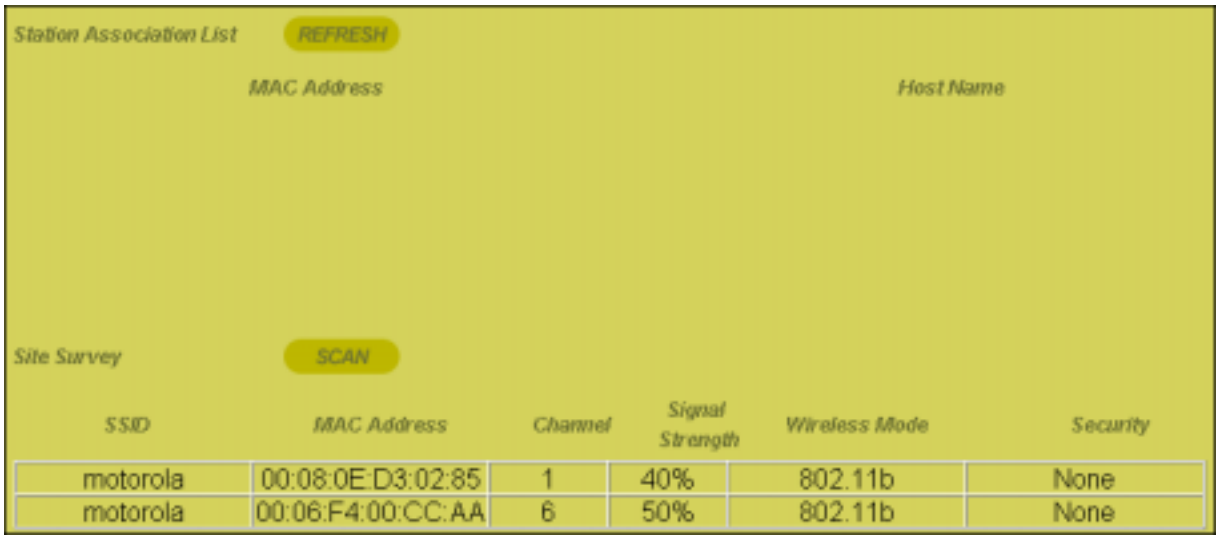
1. Click into the MAC address you wish to delete. Once activated, the field will change color.
2. Click **Remove** to clear the address.
3. Click **Apply** to save.

Wireless - Site Monitor

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

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

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



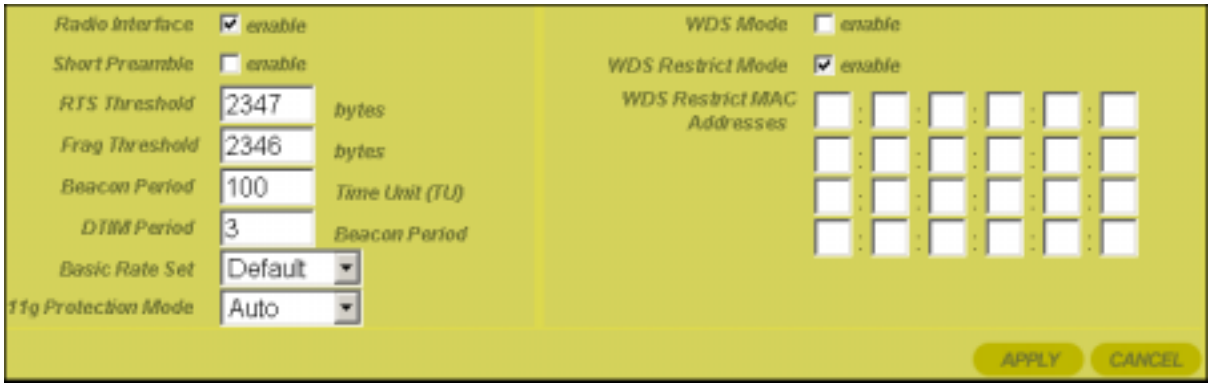
Field	Description
Station Association List	
MAC Address	Displays the MAC address of the client.
Host Name	Displays the name of the device attached.
Site Survey	
Scan	Click to search for more APs or clients.
SSID	Displays the SSID of the device found.
MAC address	Displays the MAC address of the device found.
Channel	Displays the channel upon which the device is broadcasting.

Field	Description
Signal Strength	Displays the Signal Strength of the device found.
Wireless Mode	Displays which protocol is used, 802.11b or 802.11g.
Security	Displays the security protocol used.

Wireless - Advanced

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

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



Field	Description
Radio Interface	Enables you to turn on and off the wireless feature. 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 special data such as voice, VoIP (Voice-over IP) and streaming video. The default is disabled.

Field	Description
RTS Threshold	The packet size at which an access point issues a request to send (RTS). The range is 0 to 2347 bytes. If you encounter inconsistent data flow, only minor modifications are recommended. If needed, enter a new value. The default is 2347.
Fragmentation Threshold	The size at which packets are fragmented and transmitted a piece at a time instead of all at once. The setting must be within the range of 256 to 2346 bytes. If needed, enter a new value. The default is 2346.
Beacon Period	The Beacon Period and Delivery Traffic Indicator Maps (DTIM) work together to keep power management in check. For example, if a client does not receive a beacon within a certain time period, it goes to sleep. This is why lowering the beacon period and DTIM period settings may keep sleepy clients awake. However, DTIM and Beacon settings do use additional bandwidth. So, setting them too low can have an effect on WI-FI performance. On the other hand, if no wireless clients use power management, then increasing the DTIM and Beacon settings may improve overall throughput. Usually the default settings are fine. A beacon is a packet broadcast by the AP to keep the network synchronized. You are able to set the Beacon Period value from 1 to 65535 in Time Units (TU). If needed, enter a new value and click **Apply** to save the setting. The default is 100.

Field	Description
DTIM Period	You are able to set the Delivery Traffic Indicator Maps (DTIM) period value from 1 to 255 in multiples of Beacon Periods. If needed, enter a new value and click **Apply** to save the setting. The default is 3.
Basic Rate Set	The router broadcasts different transmission rates so clients know which transmission rate to use to join the network. The default is Default. The options are: **1 to 2 Mbps** The slowest speed available. **Default** Ensures compatibility with 802.11b or 802.11g devices **All** Ensures compatibility with all devices.
11g Protection Mode	Ensures that your wireless router does not interfere with neighbor networks. 802.11b networks cannot hear 802.11g networks, but 802.11g networks can hear 802.11b 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. The default is Auto. The options are: **Disable** 802.11g Protection Mode is never used. **Auto** 802.11g Protection Mode is used if either an 802.11b client joins the network or the AP detects an 802.11b network on the same channel

Field	Description
WDS Mode	Wireless Distribution System (WDS) enables you to share and expand your network with other wireless Access Points (AP). The WDS fields, WDS Restrict Mode and WDS Restrict MAC address, become active once WDS is enabled. When enabled, any AP can connect if using your settings. The default is disabled.
WDS Restrict Mode	An activated WDS Restrict Mode enables you to protect your network by assigning access in the WDS Restrict MAC address field to only those APs you designate in the field below. The default is enabled.
WDS Restrict MAC address	To restrict a MAC address, enter up to four AP MAC addresses. To edit or delete an entry, highlight the number and perform the action.

Configuring Parental Control Settings

The settings described in this section enable you to tailor the type of content you want to allow your router to access. You create a policy that defines content access. Each policy can be associated with all the PCs the router supports. For example, a “Kids Policy” could be defined and assigned to all PCs that a child can access.

Also, a single policy can encompass multiple time schedules and multiple periods that can be assigned to any given PC. For example, a PC might be associated with a “Weekday Kids Policy” and a “Weeknight Parent” policy.

Each policy uses a content filter keyword list, meaning any sites with content containing these keywords are blocked. Each policy can also use a URL list that contains URLs that are specifically denied or allowed.

In this way, it is possible to explicitly block access to certain sites or to create a “walled garden” in which access is only granted to a select group of websites.

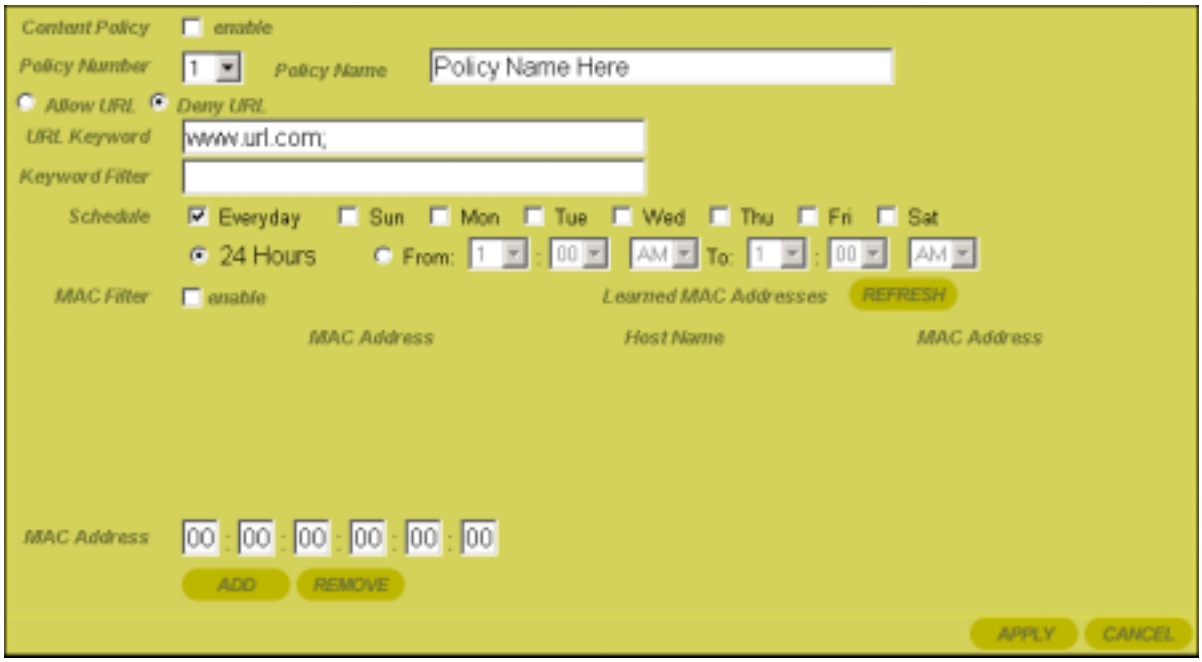
The following screens are available in Parental Control:

- Content Policy
- URL Log

Parental Control - Content Policy

From this screen you are able to define up to ten Policies that define what, when, and where the router accesses. Detailed directions for creating a policy appears after the field descriptions.

To access the screen, click **Parental Control** > **Content Filtering**. Steps for creating a Content Policy appear below the descriptions. Click **Apply** to save your settings or **Cancel** to cancel changes.



Field	Description
Content Policy	Enables or disables the Content Policy feature. The default is disabled.
Policy Number	Select the policy number.

Field	Description
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	The URL that the recipient of the policy is able to access. For example, a Kid Policy would be able to access: www.kids.com. The initial entry must end with a semicolon. Separate multiple URLs with semicolons.
Deny URL	The URL that the recipient of the policy isn't able to access. For example, a Kid Policy would not be able to access: www.xxx.com. The initial entry must end with a semicolon. Separate multiple URLs with semicolons.
URL Keyword	Enter the URL to which the policy will apply. You can enter multiple URLs, separate by semicolons.
Keyword Filter	Words that deny Internet access to the PC whenever the PC encounters them. For example, the word "cormorant" will deny the PC access to www.audubon.org.
Schedule	The time of day that the policy is in effect.
MAC Filter	Select to enable the MAC Filter. This will use the MAC addresses for filtering. ▪ You can enter multiple MAC addresses for a single policy or multiple policies for a single MAC address. ▪ 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, remove and add the revised MAC address.

Field	Description
Learned MAC Addresses	The MAC addresses discovered on the LAN appear here. Click **Refresh** to rediscover the MAC addresses available on the LAN.

To create a policy, follow this procedure:

1. Enter a Name in the Policy Name field.
2. Decide if you want to Allow or Deny a URL. You can add more than one URL, separated by semicolons. The initial 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. You can easily select a MAC address by clicking one in the Learned MAC Address table.
3. Click **Apply** to save the policy.

Parental Control - URL Log

This screen enables you to view URLs (web site addresses) that have been accessed by PCs on your network. To access the screen, click **Parental Control** > **URL Log**. Click **Apply** to save your settings or **Cancel** to cancel changes. Click **Refresh** to update the list with the latest URL Log.

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	The URL (website) that the PC has accessed.
LAN IP	The IP address of the machine 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.

Configuring Networking Settings

The Configuring Networking subsections describe the settings that enable you to configure your router to work with your Local Area Network (LAN). Generally use the default settings, as deeper knowledge of computer networking is required when adjusting these settings.

The following screens are available in Networking:

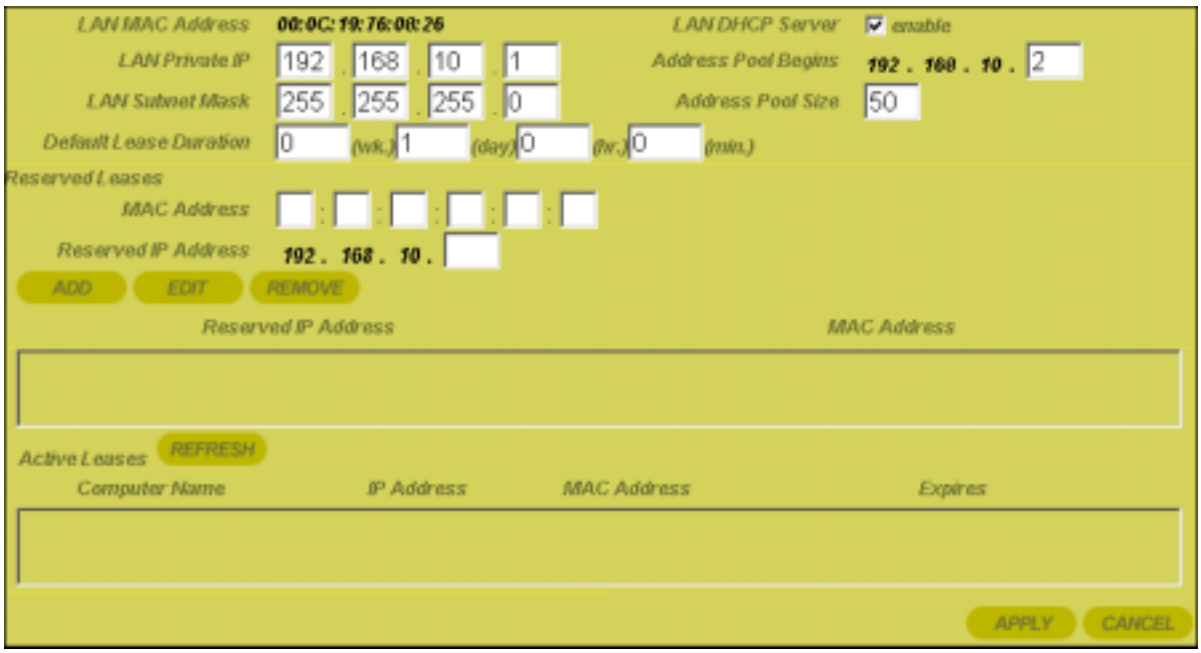
- DHCP Server
- DNS Proxy
- Routing
- DDNS
- NAT
- Port Trigger
- Virtual Server

- Firewall

Networking - DHCP Server

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



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

Field	Description
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
Default Lease Duration	Displays the Hours and Minutes of the default lease duration. Enter in a new duration. The default is 1 week.
LAN DHCP Server	Enables or disables the DHCP server. You can only run one DHCP server on your network. The default is enabled.
Address Pool Begins	Based on what is entered in the LAN Private IP field, the number entered here is where the router starts handing out IP numbers. So, using the default IP address, the next number provided would be 192.168.10.2. The default is 2.
Address Pool Size	You are able to 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. If you want to make available every number, enter 253. The default is 50.

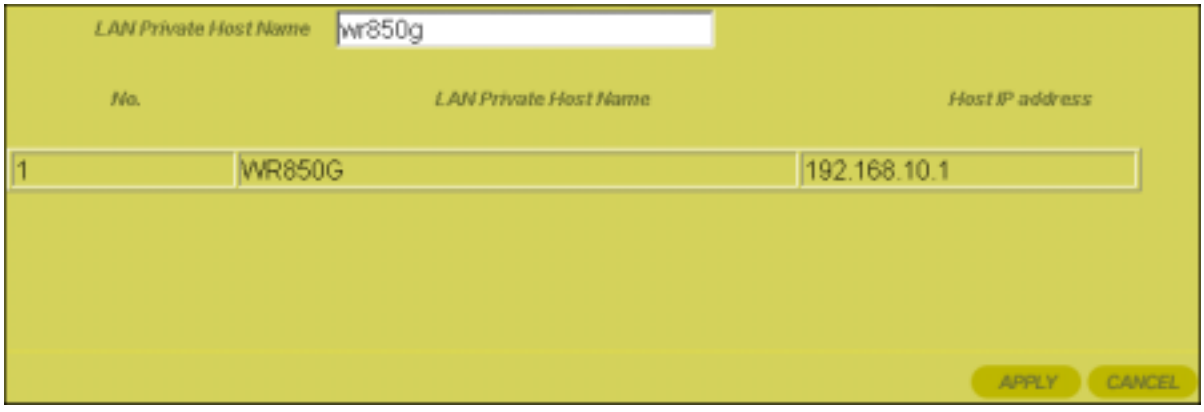
Field	Description
Reserved Leases	The DHCP reserves a set IP addresses. However, if you require a specific IP for a specific device, such as a print server, follow the directions below. To reserve a lease: **1** Enter a new MAC Address. **2** Enter the reserved IP Address. **3** Click **Add** to reserve the lease. To update or remove a lease, select it and then click **Edit** or **Remove**.
Reserved IP Address	Displays the current IP reservations along with their associated MAC address.
Active Lease	Displays the current clients that the DHCP server has assigned IP addresses. It displays the Computer Name, along with their IP and MAC address and the duration of its lease. Click **Refresh** to obtain the latest list.

Networking - DNS Proxy

This feature is used only on your Private network. The feature translates domain or website names into Internet addresses or URLs using the Domain Name System (DNS).

This feature can be used to add the mappings between a Static IP Address and a Host Name. This is most useful for devices like printer servers.

To access the screen, click **Networking** > **DNS Proxy**. Click **Apply** to save your settings or **Cancel** to cancel changes.



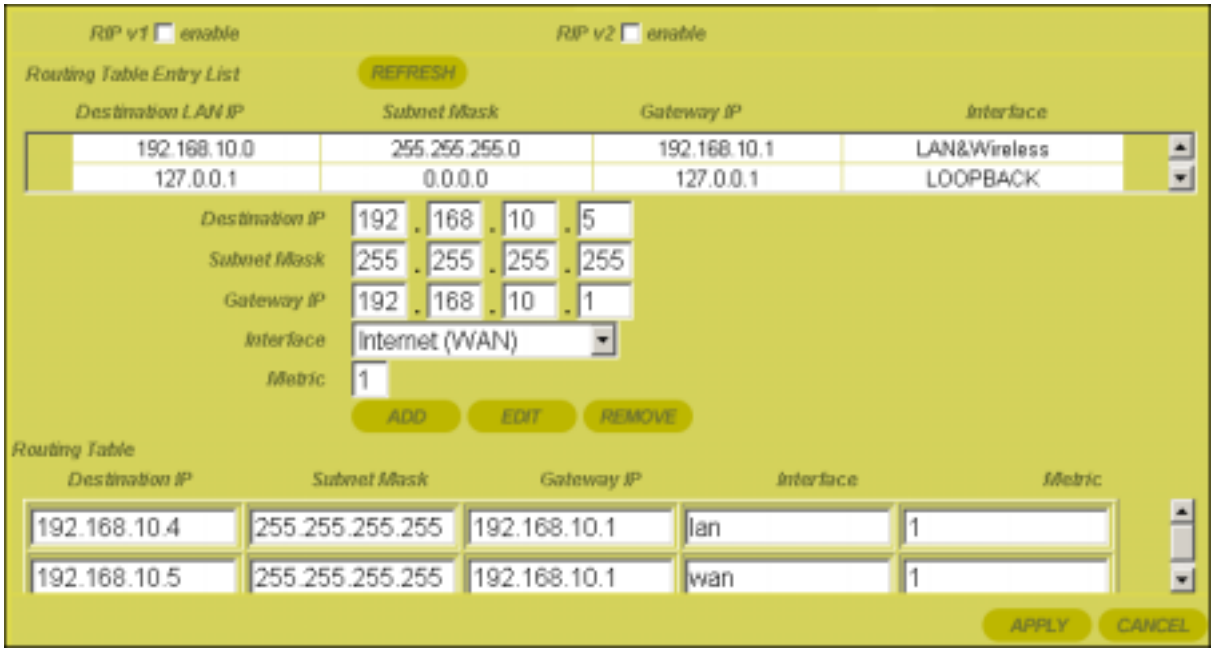
Field	Description
LAN Private Host Name	Displays the current Host name for the router. The default is “wr850g” (all lower case, without quotation marks).
Host Table	Displays the current active Host Name and its associated IP address.

Networking - Routing

You can define up to 20 static routes that specify the Destination IP, Subnet Mask, Gateway, Interface, and Metric (how many hops). You configure the Network Routing Table here. The IP address entered must be a Static IP address.

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**.



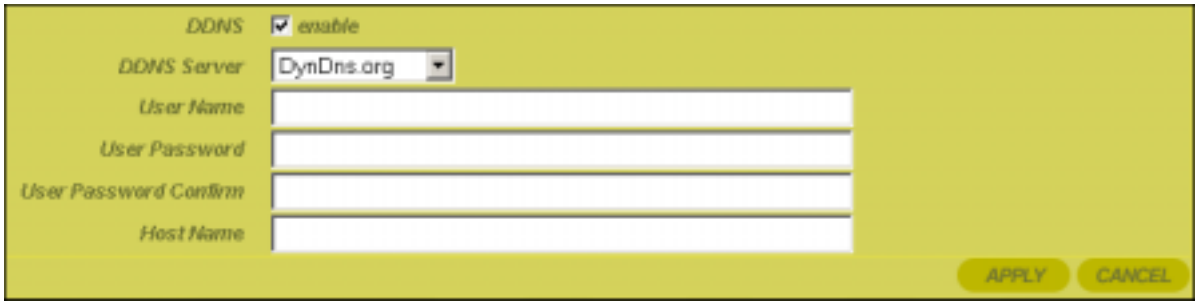
Field	Description
RIP V1	Enables or disables RIPv1. The default is disabled.

Field	Description
RIP V2	Enables or disables RIPv2. The default is disabled.
Routing Table Entry List	To add a Routing Entry: **1** Select a Destination IP number, which is the Static Routing IP address. **2** Enter Subnet Mask and Gateway IP. **3** Select LAN & Wireless or Internet (WAN) Interface. **4** Enter the Metric, or how many hops the routing can take. **5** Click **Apply** to enter the Routing Entry into the Routing Table. **6** To edit or remove an entry, click the desired entry and perform the requested action.

Networking - 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.

To access the screen, click **Networking** > **Dynamic DNS**. Click **Apply** to save your settings or **Cancel** to cancel changes.



Field	Description
DDNS	Enables or disables DDNS. The default is disabled.

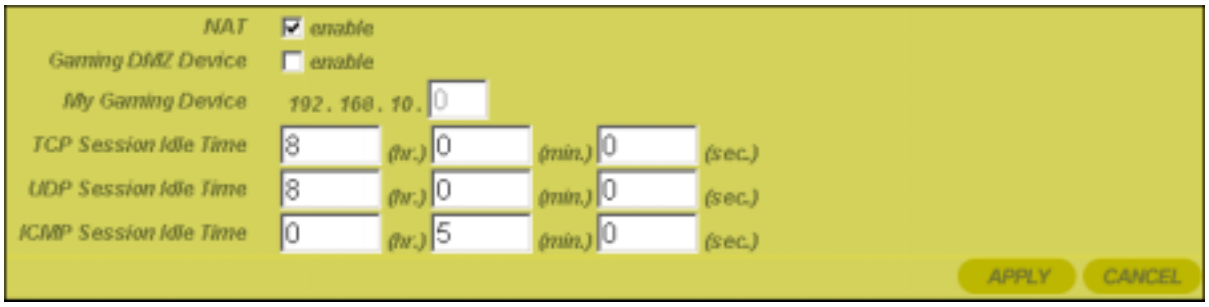
Field	Description
DDNS Server	Select the desired DDNS service provider.
User Name	Enter the User Name (up to 30 bytes) provided by the DDNS provider.
User Password	Enter the Password (up to 30 bytes) provided by the DDNS provider.
User Password Confirm	Re-enter the Password provided by the DDNS provider.
Host Name	Enter a desired Host Name for your WAN IP Address.

Networking - NAT

Network Address Translation (NAT) translates multiple IP addresses on a private LAN to one public address that is sent out to the Internet by your ISP. This adds a level of security since the address of a PC connected to the private LAN is never transmitted on the Internet.

A gaming Demilitarized Zone (DMZ) allows one IP address (computer or device) to be exposed to the Internet for online game playing or video conferencing.

To access the screen, click **Networking** > **NAT**. Click **Apply** to save your settings or **Cancel** to cancel changes.



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. For security purposes, turn off your gaming device when not in use so that it does not become the target of intrusion. The default is disabled.
TCP Session Idle Time	The TCP Session Idle Time. The time that elapses before it is assumed the session has timed out. The default is 8 hours.
UDP Session Idle Time	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. Used primarily for broadcasting messages over a network. The default is 8 hours.

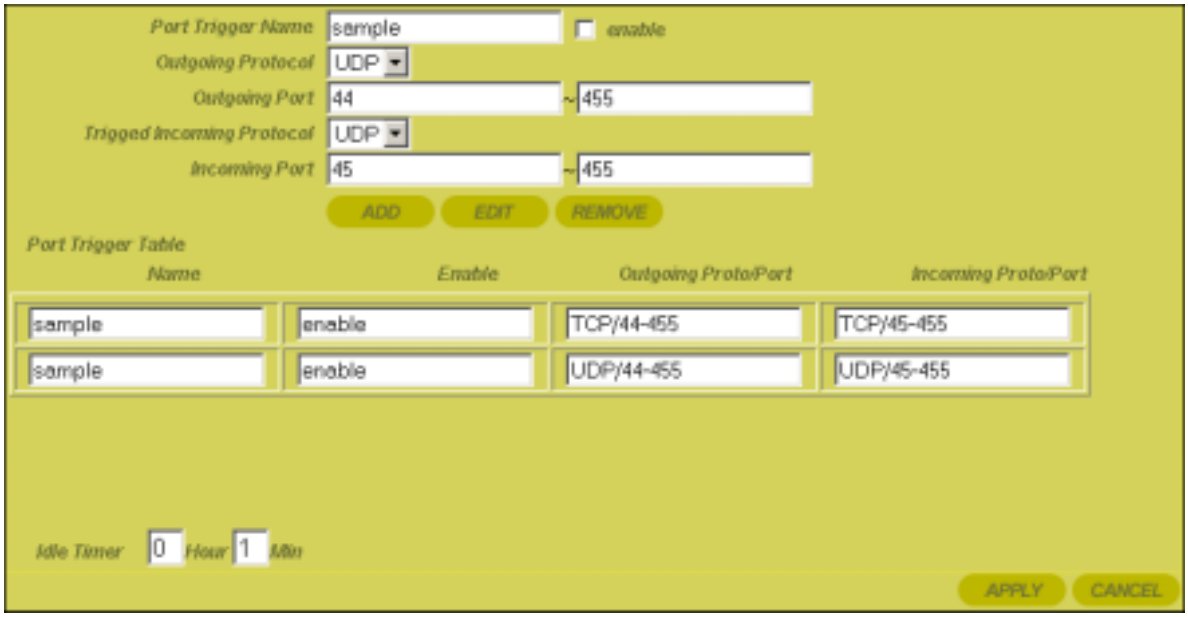
Field	Description
ICMP Session Idle Time	The Internet Control Message Protocol is a protocol used for error, problem, and informational messages sent between IP hosts and gateways. The default is 5 minutes.

Networking - Port Trigger

When you run a PC application that accesses the Internet, it typically initiates communications with a computer on the Internet. In some applications, especially gaming, the computer on the Internet also initiates communications with your PC. Because NAT does not normally allow these incoming connections to occur, the WR850G supports port triggering.

The WR850G is configured with port triggering for some common applications. You can also configure additional port triggers if needed. Configuring port triggers for an application requires a Port Trigger entry.

To access the screen, click **Networking** > **Port Trigger**. Click **Apply** to save your settings or **Cancel** to cancel changes.



To add a Port Trigger entry:

1 *Port Trigger Name*: Enter the name of the application. There is a limit of 32 characters for the name. Click to enable if you wish it to become active. Otherwise, you can save the information and enable it at later date. To enable at a later date, select the entry, check **enable**, then click **Add**.

2 *Outgoing Protocol*: From the drop down box, select either TCP or UDP.

3 *Outgoing Port*: Enter the *From* and *To* ranges (0 to 65535) for your application.

4 *Trigger Inbound Protocol*: From the drop down box, select either TCP or UDP.

5 *Incoming Port*: Enter continuous value(s) (0 to 65535), separated by dashes, for your application. You can also enter multiple non-continuous values, separated by semicolons.

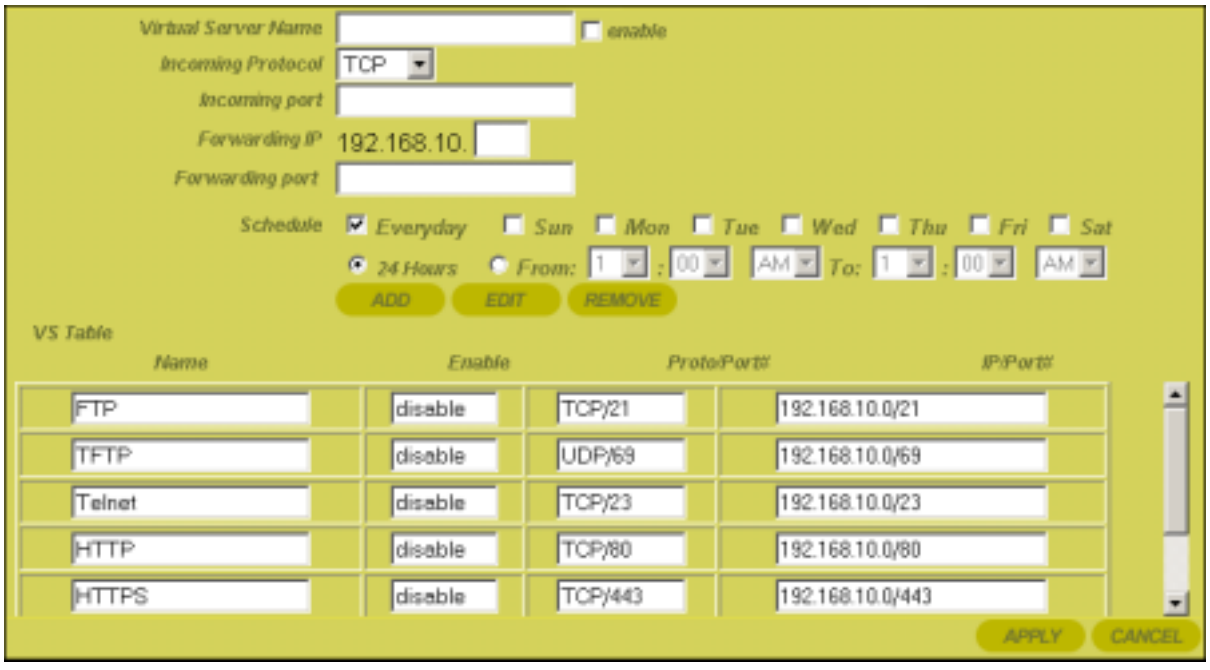
Idle Time: Enter the elapsed time before the Port Trigger mapping closes for all of the listed entries.

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

Networking - Virtual Server

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. When you use this service, it is suggested that you use Static IP and not DHCP, because the DHCP server may change the IP address during usage. You may use DHCP and then reserve the IP address.

The table below lists the current Port Forwarding rules. To access the screen, click **Networking** > **Virtual Server**. Click **Apply** to save your settings or **Cancel** to cancel changes.



To add a Virtual Server entry:

1. *Virtual Server Name*: Enter the name of the server. There is a limit of 32 characters for the name. Click to enable if you wish it to become active. Otherwise, you can save the information and enable it at later date. To enable at a later date, select the entry and then check enable.
2. *Incoming Protocol*: From the drop down box, select from TCP, UDP, or BOTH.
3. *Incoming Port*: Enter the port value (0 to 65535).
4. *Forwarding IP*: Enter the IP Address of the server to which you will forward.
5. *Forwarding Port*: Enter the port value (0 to 65535).
6. *Schedule Filter:* This is an optional feature. Click to enable. Select the time for the forwarding service to be active.

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

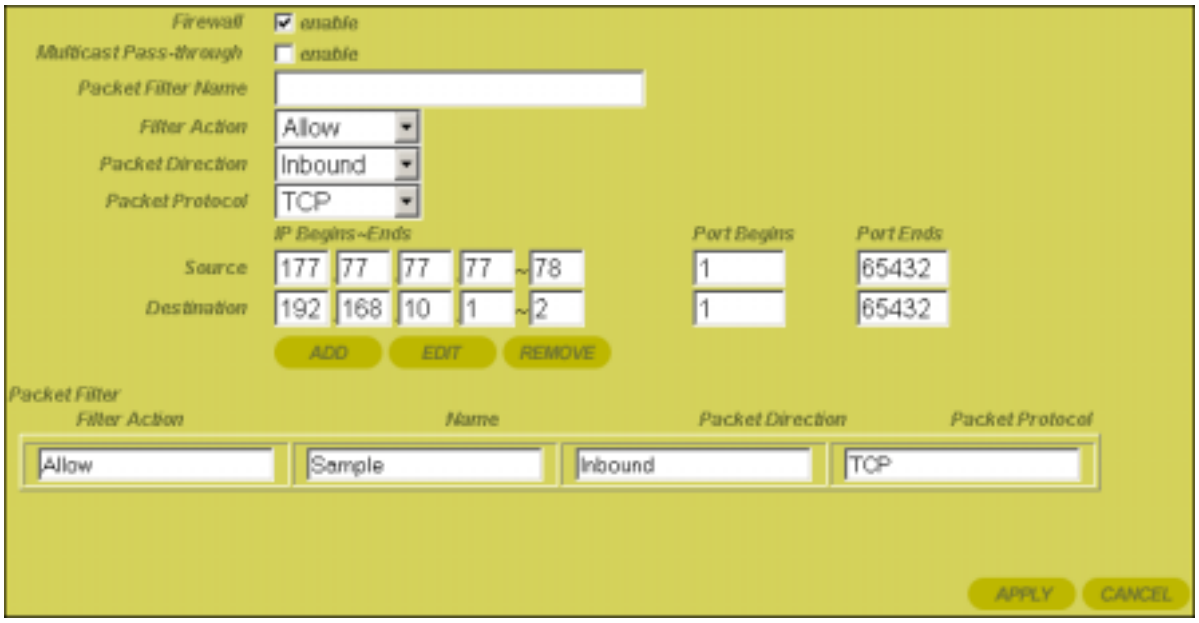
Networking - Firewall

This security device shields your network from the Internet. A firewall, working closely with a router, examines each network packet to determine whether to forward it toward its destination. The router allows further customization of this packet sniffing by allowing you to modify how and what can or cannot enter the router.

Additionally, the position of the rule within the table determines the priority of the rule. For example, the first rule in the table applies, then the second, etc. If the first rule deletes a ‘bad’ packet of information, then the remaining rules are not invoked.

Multicast Pass-through is typically used for work-related activities, such as video conferencing access.

To access the screen, click **Networking** > **Firewall**. Click **Apply** to save your settings or **Cancel** to cancel changes.



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.

To add a Packet Filter entry:

1. *Packet Filter Name:* Enter a descriptive name.
2. *Filter Action:* Select Allow or Deny. Allow: permits data that meets the criteria selected. Deny: blocks the data that meets the selected criteria.
3. *Packet Direction*: From the drop down box, select either Inbound or Outbound, based on whether you want to monitor incoming or outgoing packets.
4. *Packet Protocol:* Select the type of protocol to monitor, TCP, UPD, ICMP, or ALL.
5. *Source IP Range*: Enter the IP range.
6. *Source Port Begins* and *Ends*: Enter the Port range.
7. *Destination IP Range*: Enter the Destination IP range.
8. *Destination Port Begins* and *Ends*: Enter the Destination Port range.
9. Click **Add** to add the entry.

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 User Name/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

Control Panel - Device Security

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

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

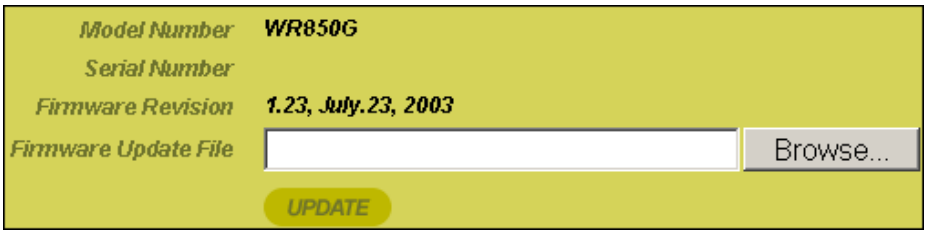
Field	Description
Login User ID	Changes the User ID used for logging into the router's web-based utility. It cannot be longer than 63 bytes. A blank user name is not allowed. The default is "admin".
Login Password	Use this option to change the Password, used to log into the router's web based utility. It cannot be longer than 63 bytes. A blank password is not allowed. The default is "motorola".
Login Password Confirm	Re-enter the same Login Password.
WAN Web Login	This 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	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.

Control Panel - Firmware Update

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

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

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



To update the firmware:

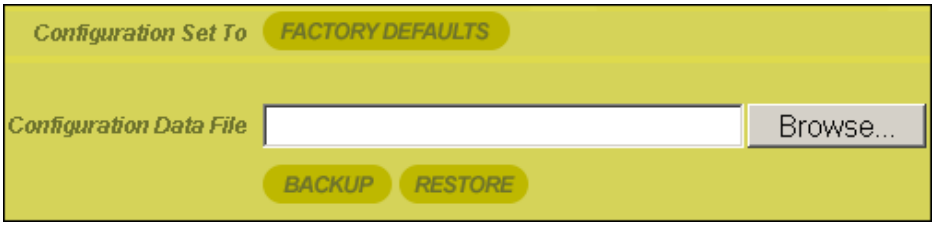
1. Download the latest firmware file to your computer from Motorola.
2. To locate the file you downloaded, type the path to the file or click **Browse** and navigate to it.
3. Click **Update** to update the router with the selected firmware file.
4. The router informs you that you successfully updated the unit.

5. Follow the prompts for restarting.

Control Panel - Configuration Data

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

To access the screen, click **Admin 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:

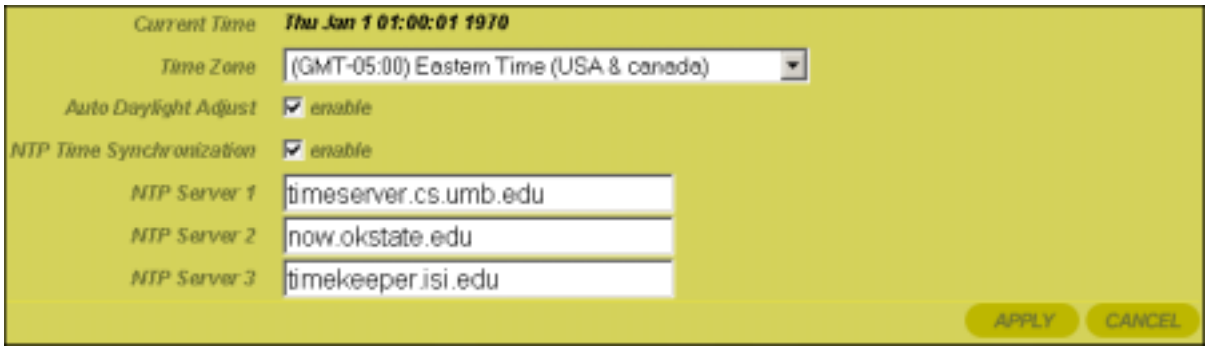
1 Locate the Configuration file on your computer by entering the path to the file or click **Browse** and navigating to it.

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

Control Panel - Time

This screen enables you to adjust time settings.

To access the screen, click **Admin Control Panel** > **Time**. Click **Apply** to save your settings or **Cancel** to cancel changes.



Field	Description
Current Time	The current time is displayed.
Time Zone	Select your local time zone. The default is EST.
Auto Daylight Adjust	If you want to have the unit adjust automatically for Daylight Savings Time, select to enable this feature. The default is enabled.
NTP Time Synchronization	If you want the unit to automatically check the current time, select to enable this feature. The default is enabled.

Field	Description
NTP Server List Table	Lists the current Network Time Protocol (NTP) servers from which you can choose for synchronization. Or, enter the host name or IP address for a desired Time Server.

Control Panel - UPnP

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

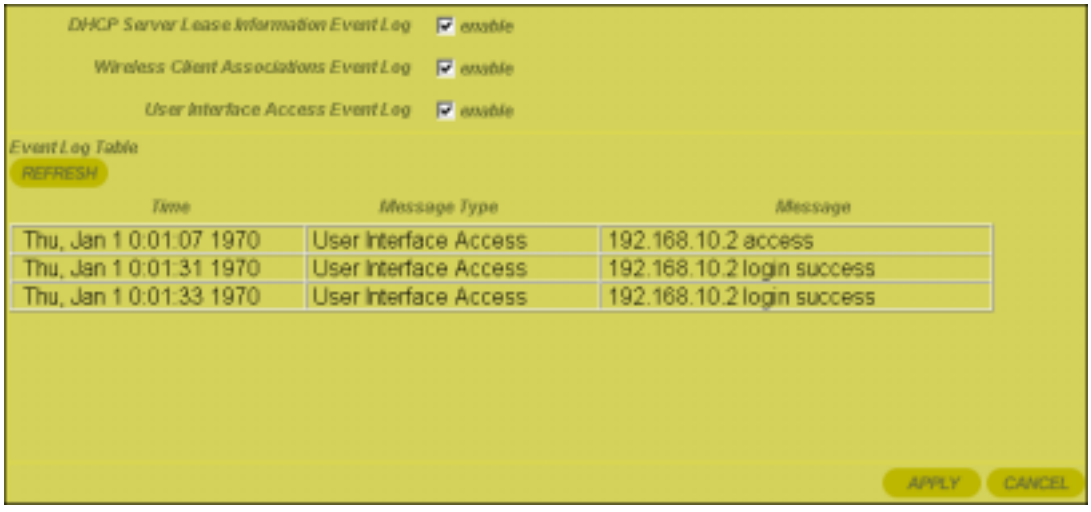
To access the screen, click **Admin Control Panel** > **UPnP**. Click **Apply** to save your settings or **Clear** to cancel changes.

Field	Description
LAN UPnP Device	Click to enable this feature. The default is disabled.

Control Panel - Event Log

The Event Log window enables you to view events (network activity, when it occurred, and a textual description) that occur on your wireless network.

To access the screen, click **Admin Control Panel** > **Event Log**. Click **Apply** to save your settings or **Cancel** to cancel changes.



Click to enable the different types of Event Log information to track.

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.

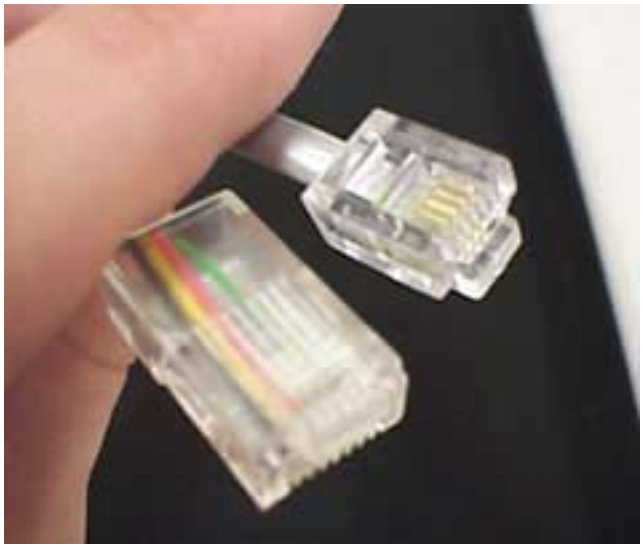
Hardware Solutions

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. Section 3: Wireless > Security section details how to adjust security settings.
- Ensure that your wireless adapter is within range of your router or is not behind obstruction, for example metal structures will interfere with the signal, as will 2.4 GHz cordless phones, and microwaves.
- Ensure that your 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.

- Check all of your cabling connections that they are tight and secured. 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. Ethernet cables use a wider RJ-45 style plug using 8 wires where telephone style plugs use the smaller RJ-11 style plug using 4 to 6 wires.



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

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

My broadband modem already uses a built-in router.

Because the two routers will cancel each other out, turning off the NAT function in the modem will 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 alive.

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

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

```
Ethernet Adapter Local Area Connection:

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

IP Address. . . . . . . . . . . . : 192.168.10.1

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

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

3. In the *Command* window, type **ping** *the Router's IP address* and press the **Enter** key. Also, there is a good possibility that the Default Gateway's IP address is the router's IP address. You can verify the router's IP address on the **Internet** > **Basic** screen.
   - If you receive a reply (the first word will be *Reply…*), then your computer is connected to the router. Proceed to *Step 4*.
   - If you do NOT receive a reply, try from a different computer to verify that the first PC is not the cause of the problem.
4. In the *Command* window, type **ping** and your ISP's default gateway and press the **Enter** key.
   - If you receive a reply (It might look something like this: *Reply from 216.109.125.72…*), then your connection to the internet is alive and well. You can verify the ISP's IP address at the Default Gateway field on the **Internet** > **Basic** screen.
   - If you do NOT receive a reply, try from a different computer to verify that the first PC is not the cause of the problem.

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: 192.168.10.3 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). Refer to Section 2: Configuration > Configure Your Computers on how to adjust the IP address for your PC.
- 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.

Section 5:Glossary

A

Access Point (AP)

A device that provides wireless LAN connectivity to wireless clients (stations). The WR850G 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 WR850G is simultaneously a DHCP client and a DHCP server.

- A DHCP server at the system headend assigns a public IP address to the WR850G.
- The WR850G contains a built-in DHCP server that assigns private IP addresses to clients.

DMZ

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

DNS

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

Domain Name

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

Download

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

Driver

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

DSL

Digital Subscriber Line

DSSS

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

Dynamic IP Address

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

E

ESS

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

Ethernet

The most widely used LAN type, also known as IEEE 802.3. The most common Ethernet networks are 10Base-T, which provide transmission speeds up to 10 Mbps, usually over unshielded, twisted-pair wire terminated with RJ-45 connectors. Fast Ethernet (100Base-T) provides speeds up to 100 Mbps. “Base” means “baseband technology” and “T” means “twisted pair cable.”’

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

Event

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

F

Firewall

A security software system on the WR850G 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 WR850G 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 WR850G 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 WR850G 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 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

494205-001
07/03

MGBI