WIRELESS ACCESS POINT (P/N 364711-01)

OWNER'S MANUAL

1307734 REV.0

Innovations in Home Living.

301 Fulling Mill Road, Suite G
Middletown, PA 17057
(800)-321-2343

www.onqhome.com

The On-Q Home Wireless Access Point includes components from ©Motorola Inc., which maintains the following compliances:

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 WA840G, the Motorola device incorporated into the On-Q Home Wireless Access Point, complies 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 On-Q Home Wireless Access Point product 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 WA840G, 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 WA840G 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.
To comply with the FCC RF exposure compliance requirements, the separation distance between the antenna and any person's body (including hands, wrists, feet and ankles) must be at least 20 cm (8 inches).

Canada - Industry Canada (IC)
The wireless radio of this device complies with RSS 210 and RSS 102 of Industry Canada.
This Class B digital device complies with Canadian ICES-003 (NMB-003).
Cet appareil numérique de la classe B respects toutes les exigences du Règlement sur le matériel brouilleur du Canada

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 WATER.

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.

CAUTION: 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.

WARNING: POSTPONE INSTALLATION UNTIL THERE IS NO RISK OF THUNDERSTORM OR LIGHTNING ACTIVITY IN THE AREA.

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 the power supply, and disconnect the CAT5e to the WAP at the POE. This will prevent damage to the product due to lightning and power surges. 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. A Data Surge Conditioning Unit is also available from On-Q Home (364598-01) to help protect the Ethernet connection from the POE to the WAP.
- Operate this product only from the type of power source indicated on the product's marking label.
- If you are not sure of the type of power supplied to your home, consult your dealer or local power company.
- Upon completion of any service or repairs to this product, ask the service technician to perform safety checks to determine that the product is in safe operating condition.

Installation of this product must be in accordance with national wiring codes and conform to local regulations.

Place POE Inserter 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.

Do not directly cover the device, or block the airflow to the device with insulation or any other objects.

Keep the device away from excessive heat and humidity and keep the device free from vibration and dust.

TABLE OF CONTENTS

I. Introduction

Your On-Q Home Wireless Access Point (WAP) uses a radio transmission technology defined by the Institute of Electrical and Electronics Engineers (IEEE) called 802.11 or Wi-Fi (Wireless Fidelity). This standard is subdivided into distinct categories of speed and the frequency spectrum used, designated by the lower case letter after the standard. Your On-Q Home WAP supports both the 802.11b and 802.11g 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 speeds so your performance may vary. The radio waves radiate out in a donut-shaped pattern. The waves travel through walls and floors, but transmission power and distance are affected.

Both standards operate in the 2.4 GHz range, meaning other electrical appliances also might interfere with the WAP. Televisions, radios, microwave ovens, and 2.4 GHz cordless telephones are examples of devices that might interfere with the WAP. Thus, positioning your WAP where it encounters the least interference gains the greatest benefit to maintaining a quality connection. Typically, the best performance can be expected by positioning it in the ceiling at a central location on the top floor of the home.

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

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

Your On-Q WAP is powered over the single CAT5e cable that connects it to the service provider using a technology called Power Over Ethernet (POE). A power supply inserts power onto the CAT5e cable through an inserter module, and then this power is extracted for use at the WAP location. In this way, unsightly power cables are avoided at the WAP location.

II. Product Overview

A. Features

- Compatibility with both 802.11g and 802.11b standards
- Wireless security using WPA, 802.1X Authentication, and Advanced Encryption Standard (AES)
- Wireless Distribution System (WDS) mode supporting peer-to-peer communication with other On-Q WAP units
- Firmware upgrades available to stay current with latest specification

B. Components Included

The On-Q Home WAP includes the following components (see *Figure 1*):

- WAP Assembly
- WAP Mounting Ring
- WAP Cover
- WAP 48VDC Power Supply with AC cord
- WAP Power Over Ethernet (POE) Inserter Module
- CAT5e Jumper Cable
- This WAP Manual on CD
- WAP IS Sheet and User Guide

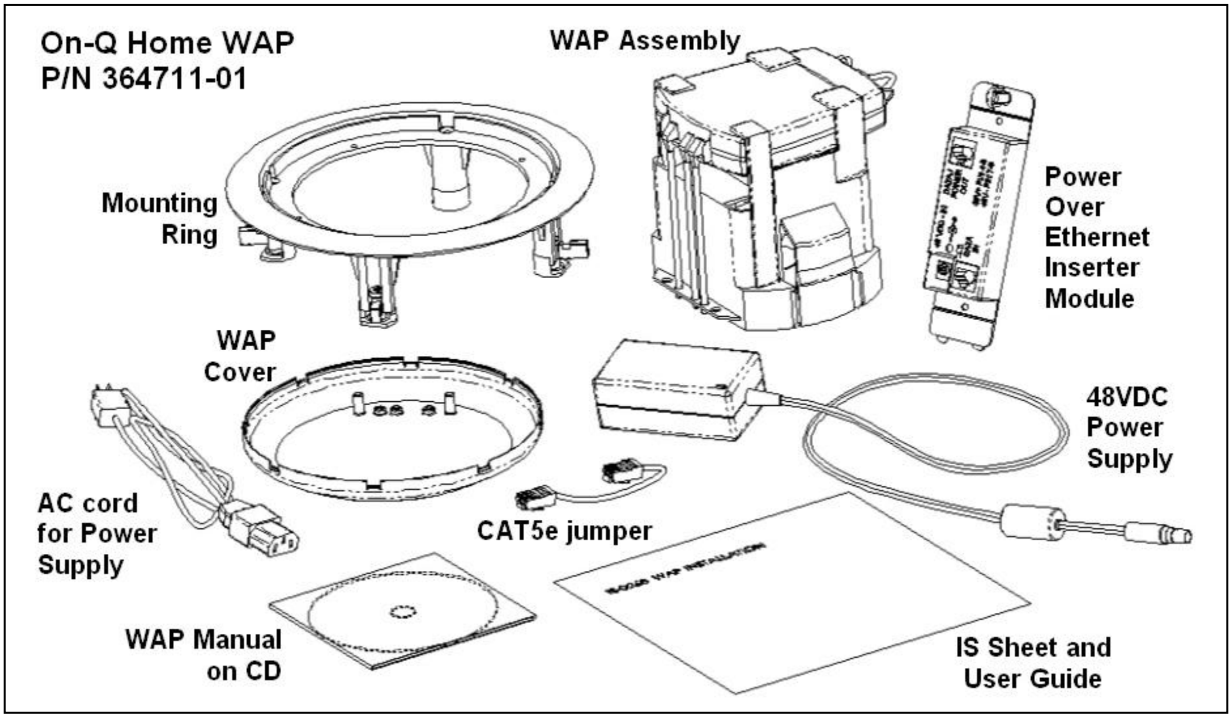


Figure 1

C. Replacement Parts

Replacement parts available for the On-Q Home WAP include:

- WAP 48 VDC Power Supply with AC cord (P/N 364723-01)
- WAP Power Over Ethernet (POE) Inserter Module (P/N 364719-01)
- WAP Cover (P/N 364724-01)

D. On-Q Home WAP Detailed Physical Description

The following information describes the physical characteristics of the WAP Assembly.

1. WAP Assembly Connections

Figure 2 shows the WAP Assembly connection area including:
Power Receptacle
LAN Port
Reset Button
Antenna Connection
CAT5e to POE

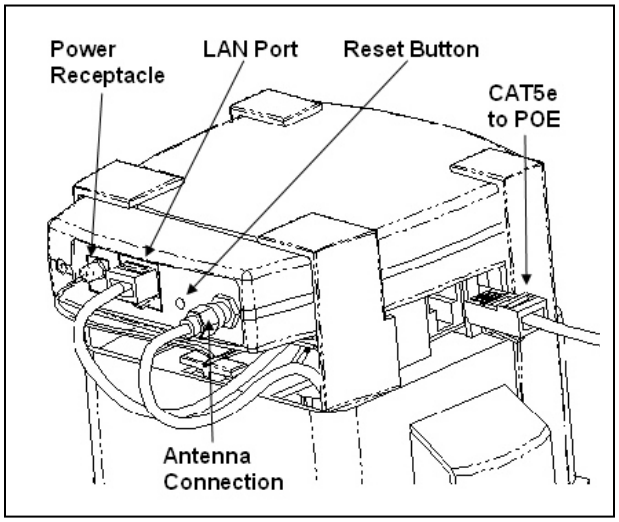


Figure 2

2. Connection Area Detailed Description

Power Receptacle – Five volt DC power is extracted from the POE Extractor Module in the WAP Assembly (the 5VDC is derived from the 48VDC fed to the WAP Assembly over the single CAT5e from the POE Inserter Module in the Enclosure).

LAN Port – Ethernet data is extracted from the POE Extractor Module in the WAP Assembly. The LAN port supports either 10BASE-T or 100BASE-T transmission speeds as well as straight-through and crossover Ethernet cables (the Ethernet data is derived from the single CAT5e fed to the WAP Assembly from the POE Inserter Module in the Enclosure).

Reset Button - A dual-function button. A brief button press resets the WAP unit, while a longer button press resets the WAP unit to the default login settings. If the WAP is experiencing trouble connecting to the Internet, briefly press and release the Reset button to reset the WAP. The WAP will retain its configuration information during this reset operation. To reset the unit to the factory defaults, while the unit is powered, press and hold the Reset button for more than 10 seconds. This clears the WAP's user settings, including User ID, Password, IP Address, and Subnet Mask.

NOTE: Refer to the *Section IV Initial Configuration Steps* for re-configuring the WAP.

Antenna Connection – Cable connects to the On-Q WAP antenna used for wireless connections.

NOTE: When initially removed from the box, a stub antenna will be connected to this connector. For better coverage, it should be removed and replaced by the On-Q WAP antenna cable.

3. **WAP Assembly Status Indications**

Figure 3 shows the WAP Assembly status indicators, which are visible from directly below when the WAP cover is properly installed:

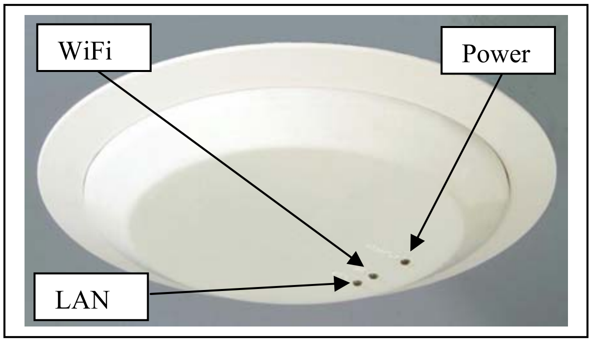


Figure 3

4. **Status Indicators Detailed Description:**

Power Indicator

ON **Green** The device is powered on and operating normally.
Blinking **Green** Firmware update is in progress.
Blinking/ON **Red** The power LED turns RED as soon as the reset button is depressed. If the reset button is held down for more than 5 seconds, the LED starts to blink during which the WAP's default user name, password and IP address will be restored. The LED then turns OFF until the reset button is released. The power LED keeps blinking RED if the firmware is corrupted indicating that the firmware needs to be restored.

WiFi Indicator

OFF **No Light** No mobile station or WAP has associated with this device.
ON **Red** The wireless interface has been disabled by the firmware.
ON/Blinking **Green** 802.11b/802.11g connection exists in this wireless domain/active traffic present.

LAN Indicator

OFF **No Light** No external Ethernet device has been attached or detected. The Ethernet link is down.
ON/Blinking **Amber** 10BaseT link detected/active traffic present.
ON/Blinking **Green** 100BaseT link detected/active traffic present.

5. **WAP Power Over Ethernet Inserter Module**

Figure 4 shows the WAP POE Inserter Module components:

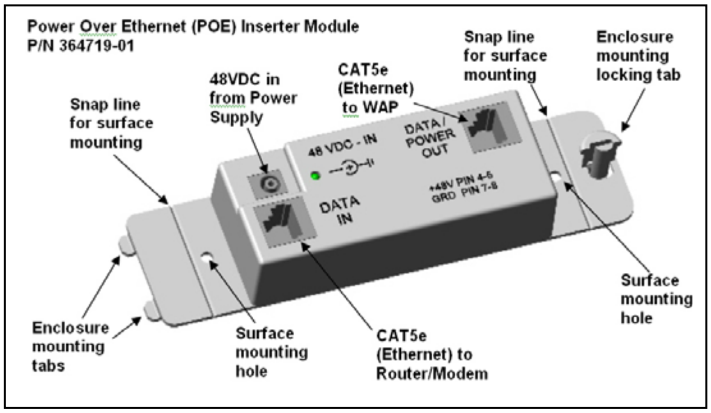

Power Over Ethernet (POE) Inserter Module
P/N 364719-01
Snap line for surface mounting
48VDC in from Power Supply
CAT5e (Ethernet) to WAP
Snap line for surface mounting
Enclosure mounting locking tab
48 VDC - IN
DATA / POWER OUT
DATA IN
+48V PIN 4-5
GRD PIN 7-8
Surface mounting hole
Enclosure mounting tabs
Surface mounting hole
CAT5e (Ethernet) to Router/Modem

Figure 4

III. Installation

The On-Q Home Wireless Access Point is best installed during new construction in two steps; at “rough-in” after the Electricians are done, but prior to drywall being installed, and at “trim-out” after the drywall is installed and painted. These steps are detailed below:

A. “Rough-in” steps:

1. A single CAT5e should be run in the walls from the location in the home where the On-Q Home Wireless Access Point (WAP) will be installed to the location where the POE Inserter Module will be located (leave extra cable at both ends).

NOTE: The preferred location for the WAP is in the ceiling of the top floor, centrally located in the home (see *Figure 5*). If multiple WAPs are used, they should be located centrally, in overlapping areas.

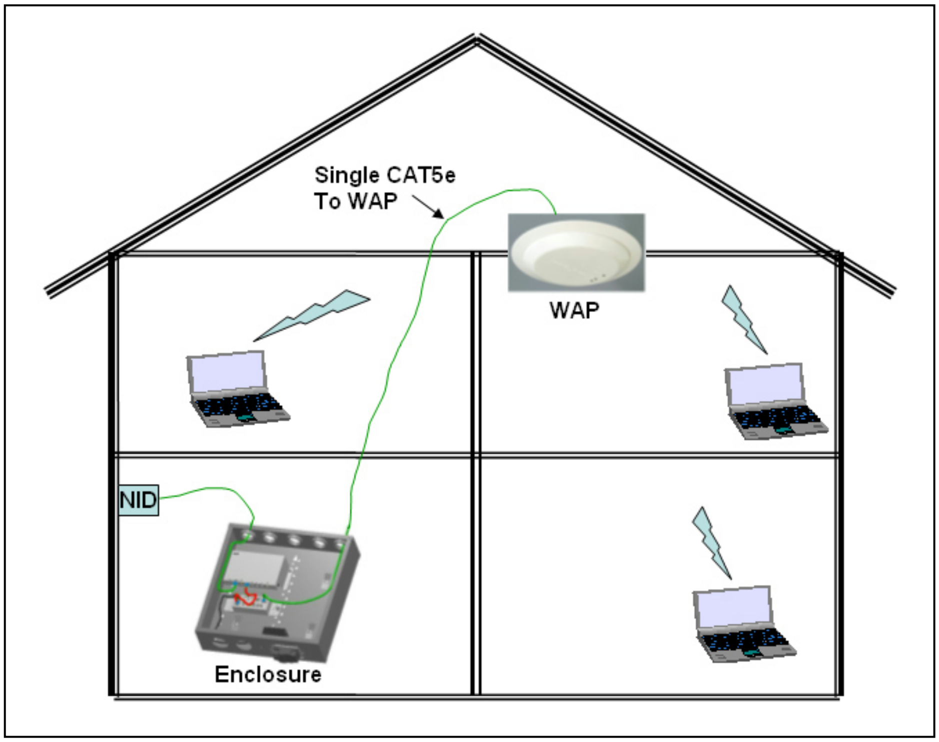


Figure 5

NOTE: Although the On-Q Home Wireless Access Point (WAP) may be installed in ceilings or walls, it requires a minimum of 5” of mounted depth. This means that the WAP cannot be installed in 2x4 walls.

2. (*Optional Step for New Construction*) At the selected WAP location, the On-Q Home Wireless Access Point Pre-Construction Bracket, is installed with two screws from the floor side across the exposed ceiling studs (for more detail, refer to IS-0269).

3. (*Optional Step for New Construction*) The CAT5e can be coiled around the top of the bracket, to be pulled through after the sheetrock is installed. There are clips on the top of the bracket to tie off the CAT5e cable (for more detail, refer to IS-0269).

B. "Trim-out" steps:

1. The WAP mounting ring should be installed first, using a Phillips screwdriver to tighten the four mounting tabs against the drywall or optional Pre-Construction Bracket (see *Figure 6*).

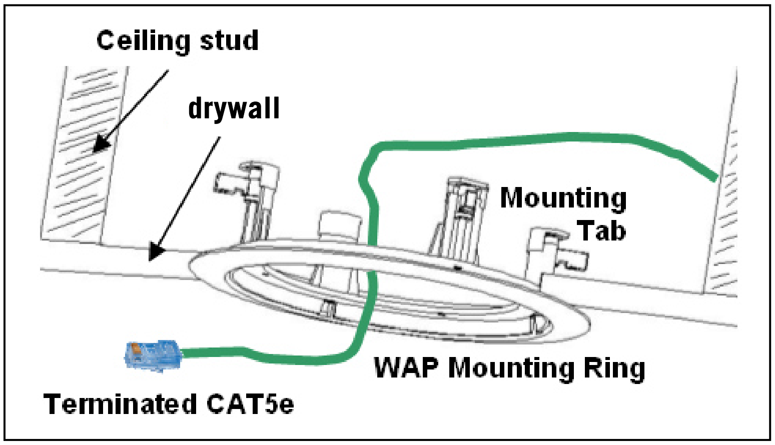


Figure 6

2. The CAT5e that was tied off at the bracket should then be pulled through the hole in the bracket and terminated with an EZ RJ45 plug (P/N 364554-01).

NOTE: Use proper tools and standard TIA 568A rules to prep and terminate the CAT5e cable, such as the On-Q Home CAT5 Cable Stripper (P/N 363292-01) and the On-Q Home EZ RJ45 Crimp Tool (P/N 364555-01).

3. The On-Q Home Wireless Access Point (WAP) is shipped with an attached stub antenna. For better coverage in the typical residential installation, remove the stub antenna and connect the coaxial cable from the included On-Q Home antenna (see *Figure 7*).

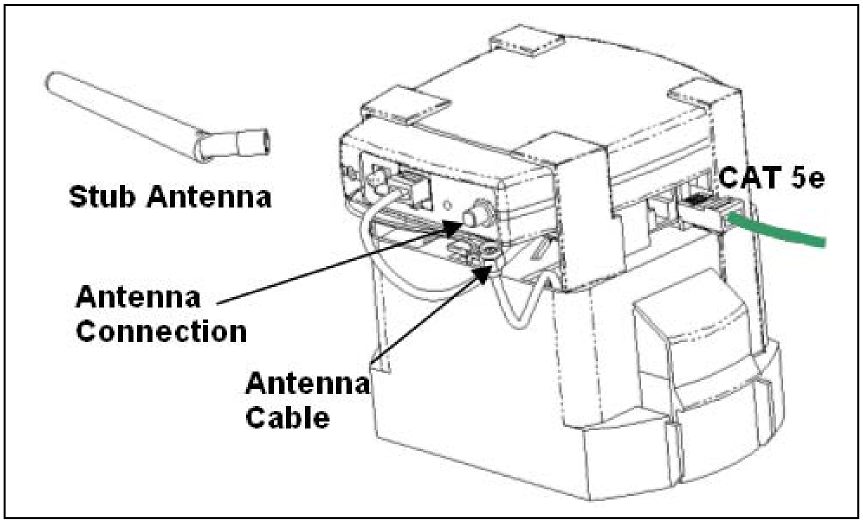


Figure 7

4. Next, connect the EZ RJ45 terminated CAT5e cable to the WAP Assembly.

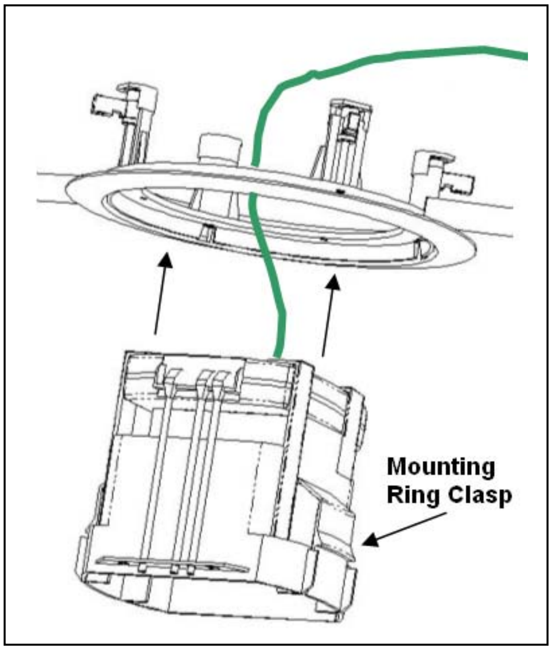


Figure 8

5. To physically install the WAP Assembly, push the unit through the mounting ring until the Mounting Ring Clasps snap into place (see *Figure 8*).

6. Then install the center cover, making sure the tabs in the cover line up with the holes on the WAP Assembly. This will insure that the light pipes from the status lights on the WAP are properly aligned (see *Figure 9*).

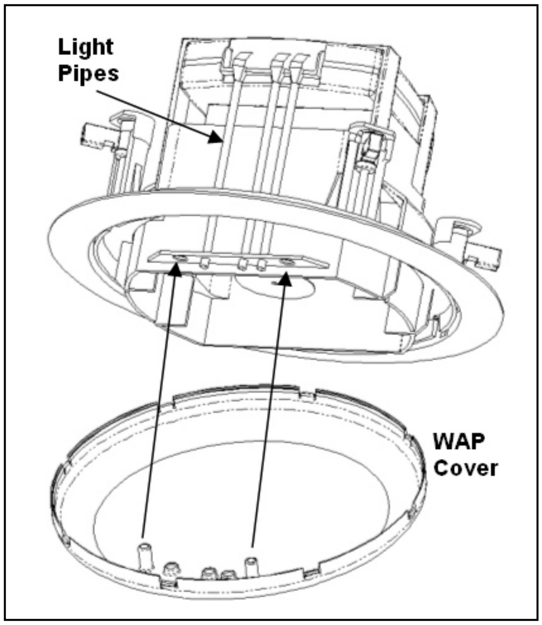


Figure 9

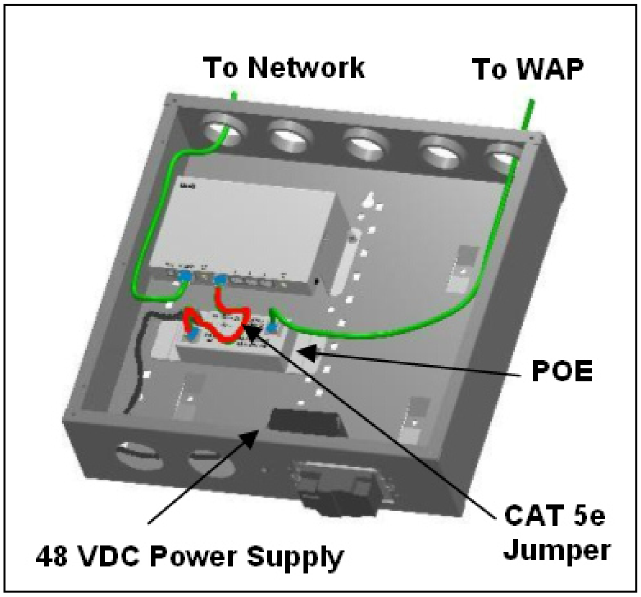


Figure 10

7. In the structured wiring enclosure (see *Figure 10*) the CAT5e from the WAP can be terminated at a Network Interface Module (P/N 363486-01) or with an EZ RJ45 plug (P/N 364554-01) which is then connected directly to the output of the Power over Ethernet (POE) Inserter Module.

8. A supplied CAT5e patch cable is then connected from the input RJ-45 jack of the Power over Ethernet Module to one of the LAN ports on the On-Q Home or third party Router, or directly to a Broadband Modem.

9. The Power over Ethernet Inserter Module is powered with a 48 Volt DC power supply which needs to be plugged in to an AC source.

10. When the 48 VDC Power Supply is plugged in to an active AC Source, verify that the Power LED is lit on the POE.

11. Next, verify that the Power LED is lit on the WAP.

12. If you connected to an active network, verify that the Network Activity LED is lit on the network access device and on the WAP.

13. Then, verify the Wireless LED is lit on the WAP.

IV. Initial Configuration Steps

The On-Q Home WAP is typically configured in one of two ways; (1) From a portable PC connected through the "Data In" port of the POE Inserter Module in the enclosure which is then connected through its "Data/Power Out" port to a CAT5e cable to the WAP, or (2) From a PC in one of the rooms of the house, connected through an outlet in the room to the enclosure where it is patched to the "Data In" port of the POE Inserter Module in the enclosure which is then connected through its "Data/Power Out" port to a CAT5e cable to the WAP (see *Figure 11*). In either case, the PC must have an Ethernet Network Interface Card to communicate with the WAP.

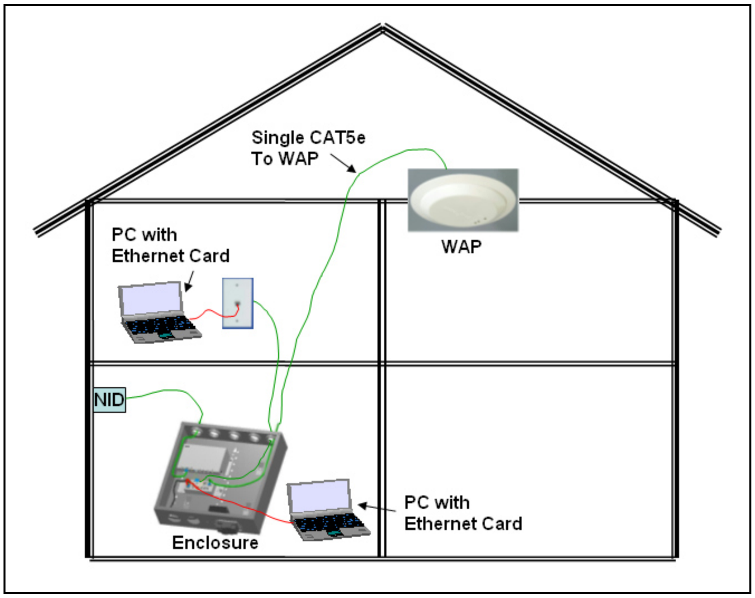


Figure 11

NOTE: The On-Q Home WAP can also be configured from a PC containing a Wireless Network Interface Card (Motorola WPCI810G wireless PCI card for your desktop PC, or Motorola WN825G wireless PCMCIA card for your laptop PC), but this is not recommended because it is not secure until you have configured security levels on the WAP. To connect the PC to the WAP through a wireless connection, ensure the PC.s wireless adapter SSID (Service Set Identifier) is set to the WAP's default setting of "motorola" appended with the last 3 characters of the Wireless MAC address (an example SSID: motorola345) and that no encryption is enabled.

NOTE: Before configuring the On-Q Home WAP, you must first temporarily configure your computer (with installed Ethernet Network Interface Card) to talk to the WAP. The WAP comes configured to a specific IP subnetwork (192.168.40.xxx) and its default IP address in that subnetwork is 192.168.40.1, so your PC's Ethernet Card must be assigned an IP address, (like 192.168.40.10), on that same subnetwork to talk to and configure the WAP. Giving the PC a specific IP address is also called assigning it a Static IP address, as compared to a Dynamic IP address that is typically assigned by a service provider through a process called Dynamic Host Configuration Protocol (DHCP).

NOTE: Before doing any PC IP Address re-configuration, make sure you first write down all of the current IP settings.

NOTE: After initially configuring the WAP, using that Static IP Address that you assign, you may need to return the PC's IP Address setting to be dynamically assigned by DHCP, if that is what the service provider requires. If you are using a router, you will also want to change your WAP's IP address and Gateway settings to be compatible with the router. These steps are covered at the end of this section.

A. Configuring a Windows XP Ethernet Network Interface Card to talk to the WAP

This section includes information on configuring computers with the Windows XP operating system (differences for 98SE, ME and 2000 will be sited).

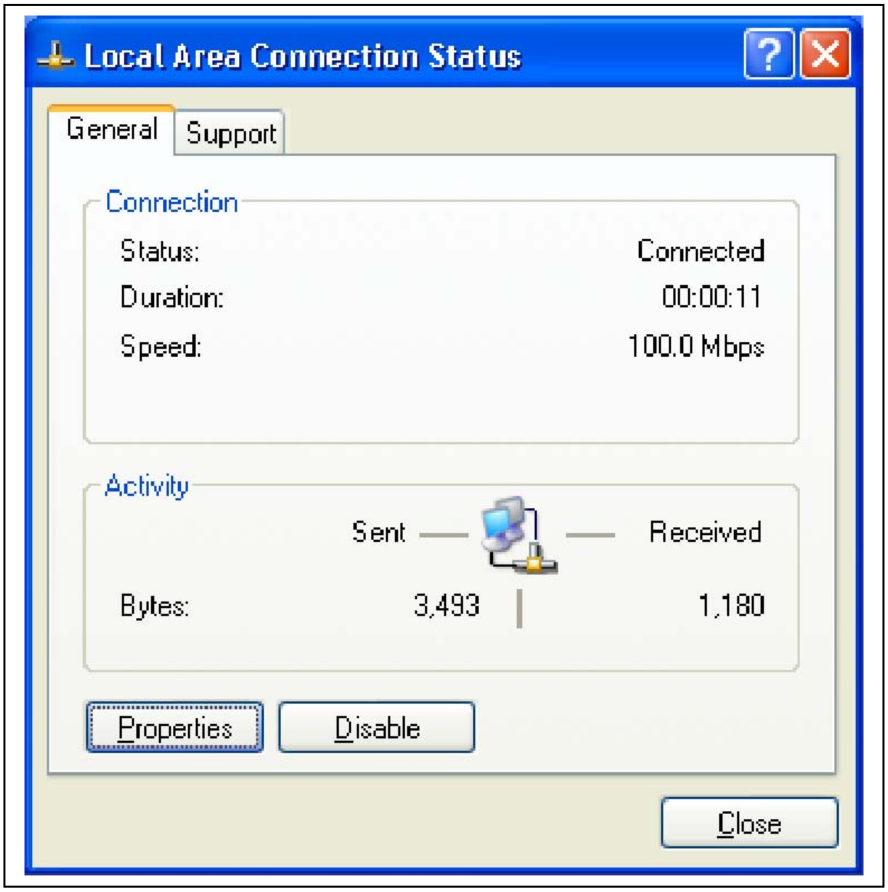
NOTE: This configuration assumes you have retained the default interface for Windows XP. If you are running the .Classic. interface, please note any sited differences for Windows 2000.

1. Click **Start**.

2. Select **Control Panel**.
   (For Windows 98SE, ME and 2000, select Settings first)

3. Double-click **Network and Dial-Up Connections.**
   (Double Click Network for Windows 98SE and ME and the Network Window is displayed)

4. Double-click **Local Area Connection**. The Local Area Connection Status window appears (see *Figure 12*).
   (*Step 5 is not applicable for Windows 98SE or ME*)



Status: Connected

Duration: 00:00:11

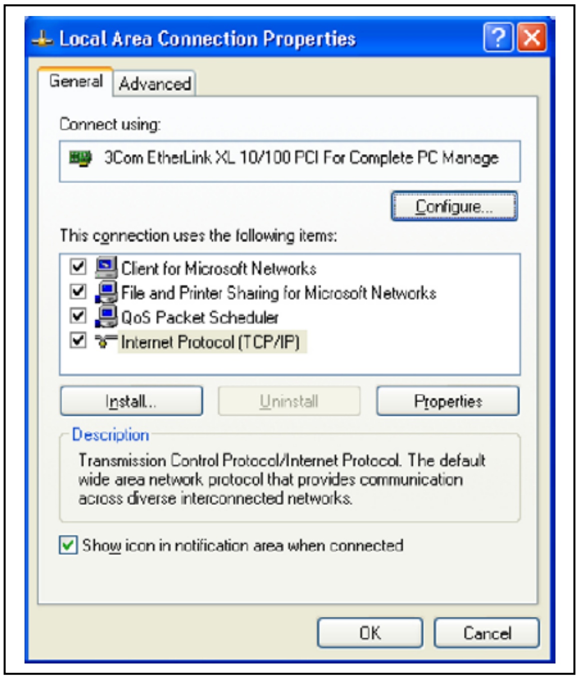
Speed: 100.0 Mbps

Sent — — Received

Bytes: 3,493 | 1,180

Figure 12

5. Click the **Properties** button to go to the *Local Area Connection Properties* screen.
   (*Step 6 is not applicable for Windows 98SE or ME*)



Local Area Connection Properties

General | Advanced

Connect using:

3Com EtherLink XL 10/100 PCI For Complete PC Manage

Configure...

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

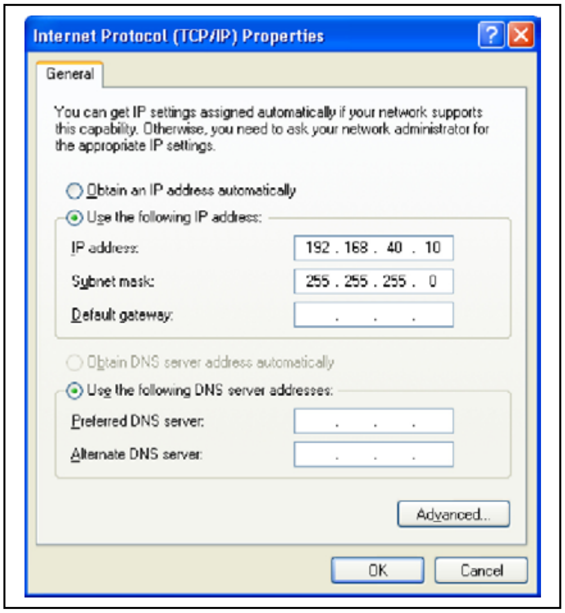
☑ Show icon in notification area when connected

OK | Cancel

Figure 13

6. Ensure the box next to *Internet Protocol (TCP/IP)* is selected (see *Figure 13*).

7. Click to highlight **Internet Protocol** (**TCP/IP**) and click the **Properties** button to go to the *Internet Protocol (TCP/IP) Properties* screen.
(***For Windows 98SE or ME, from the Network Window's configuration tab, select the TCP/IP line the for the appropriate Ethernet adapter and Click Properties. From the TCP/IP Properties Window, Click on the IP Address tab.)***



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 40 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

Advanced...

OK | Cancel

Figure 14

8. Click on "**Use the following IP Address**:" so that the circle is filled (see *Figure 14*).

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

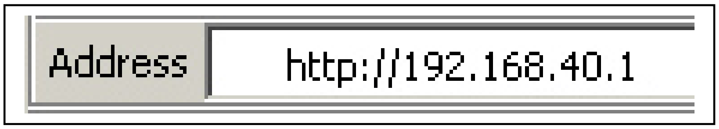
10. Enter **255.255.255.0** into the Subnet Mask field.

11. Click **OK** twice to exit and save your settings.
    (*For Windows 98SE, ME, or 2000 you will have to restart the computer to save these settings).*

12 After the reboot (if appropriate), proceed to the next section to set up the WAP security settings.

B. Logging on to the WAP

1. Once the PC's Ethernet Interface Card is configured on the WAP's subnetwork, open your web browser and Enter into the URL field **http://192.168.40.1** (the WAP's default IP address) and press **Enter** (see *Figure 15*).



Address http://192.168.40.1

Figure 15

The login screen will appear (see *Figure 16*).

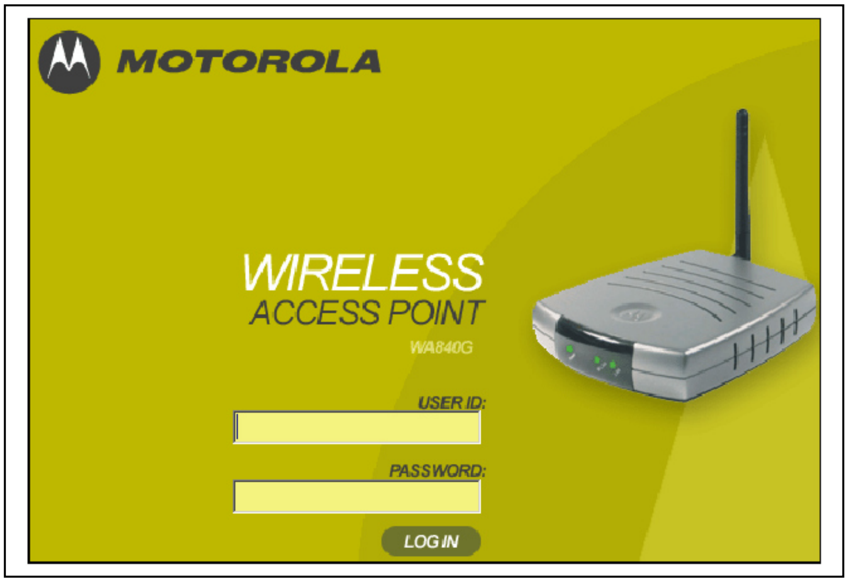


Figure 16

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

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

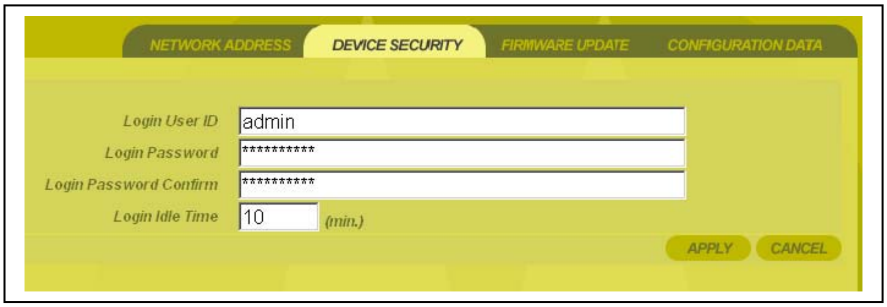
NOTE: Once you have logged in, for security reasons, you should change the User ID and Password. Be sure to document the new User ID and Password. For details, see next section.

4. Click the **Log In** button to enter the WAP's Configuration Utility.

C. Wireless Security Setup

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

1. Select **Control Panel** > **Device Security** (see *Figure 17*).



Login User ID: admin
Login Password: **********
Login Password Confirm: **********
Login Idle Time: 10 (min.)

Figure 17

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

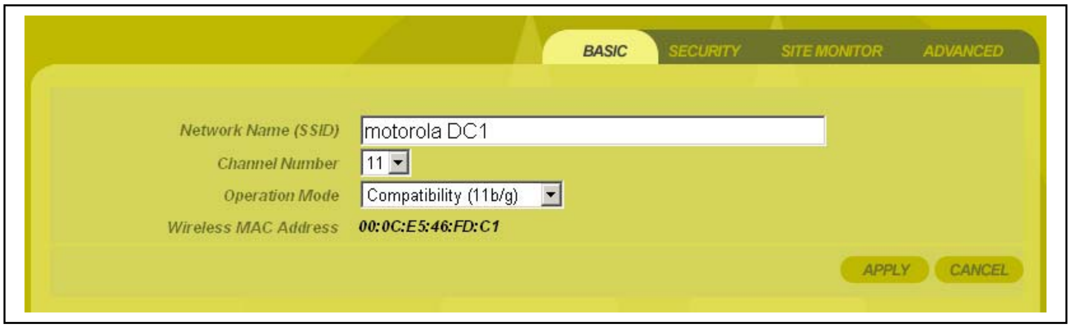
3. In the Login User Password field, enter in the desired ***Login Password.*** For strong security, select a password that contains multiple case-sensitive characters as well as numbers and symbols like ._ +).. It cannot be longer than 64 characters.

4. Re-enter the same Password.

5. Click **Apply**.

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

7. Navigate to **Wireless** > **Basic** (see *Figure 18*).



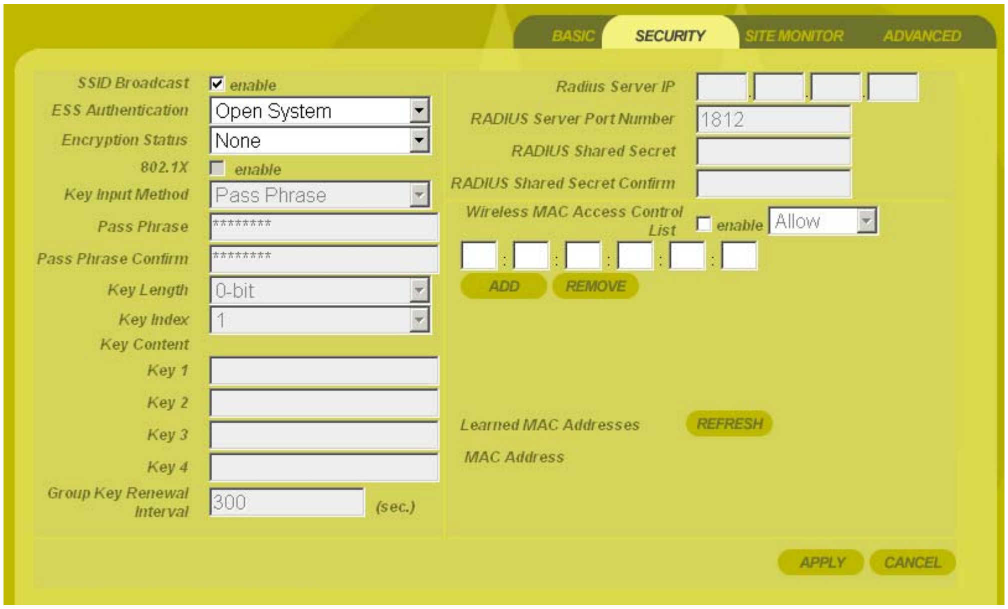
Network Name (SSID): motorola DC1
Channel Number: 11
Operation Mode: Compatibility (11b/g)
Wireless MAC Address: 00:0C:E5:46:FD:C1

Figure 18

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

NOTE: The Channel Number identifies the channel on which the WAP communicates, and each associated wireless client must use the same channel number in order to communicate (The default channel is 11).

9. Navigate to **Wireless** > **Security** (see *Figure 19*).



SSID Broadcast ☑ enable

ESS Authentication: Open System

Encryption Status: None

802.1X □ enable

Key Input Method: Pass Phrase

Pass Phrase: ********

Pass Phrase Confirm: ********

Key Length: 0-bit

Key Index: 1

Key Content

Key 1

Key 2

Key 3

Key 4

Group Key Renewal Interval: 300 (sec.)

Radius Server IP

RADIUS Server Port Number: 1812

RADIUS Shared Secret

RADIUS Shared Secret Confirm

Wireless MAC Access Control List □ enable Allow

Learned MAC Addresses

MAC Address

Figure 19

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

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

NOTE: The Extended Service Set (ESS) Authentication selection and Encryption Status selection determine how secure your WAP will be. You may have to match the security settings of your chosen Wireless Network Interface card to insure operability. The WAP is defaulted to Open System ESS (no authentication) and None (no security) for Encryption Status. The choices from least secure to most secure are:

Extended Service Set (ESS)	**Encryption Status**
Open System	**None**
Pre-Shared Key (PSK)	**WEP64**
WPA	**WEP128**
WPA-PSK	**TKIP**
	AES

NOTE: Higher encryption levels are inversely related to data transmission speed.

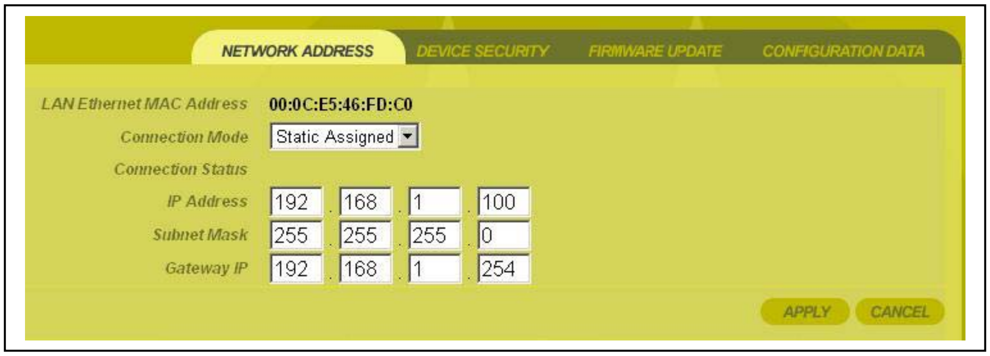
12. Enter a new **Pass Phrase** and again in **Pass Phrase Confirm**. Remember this Pass Phrase so that you can enter the same phrase for the Motorola client devices on your wireless LAN. Pass Phrase must be between 8 and 63 characters.

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

D. Configuring the WAP to work with a Router

If you are connected to the Internet through a Router, you will want to change the IP Address of the WAP to also be a member of the Router's subnetwork. This will allow you to access the WAP at a future date, if you need to re-configure its security or login settings.

1. Navigate to the Control Panel > Network Access Screen (see *Figure 20).*



LAN Ethernet MAC Address 00:0C:E5:46:FD:C0
Connection Mode Static Assigned
Connection Status
IP Address 192 . 168 . 1 . 100
Subnet Mask 255 . 255 . 255 . 0
Gateway IP 192 . 168 . 1 . 254

Figure 20

2. Enter **192.168.1.xxx** (**example subnetwork for the router**) into the IP Address field. Use an address (like **100**) that is higher than the number of PCs you are likely to attach to this router.

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

4. Enter **192.168.1.254** into the Gateway IP field and click Apply.

5. To verify that you can access the WAP at its new IP address, run the Ping command (**ping 192.168.1.100**) from any router attached PC.

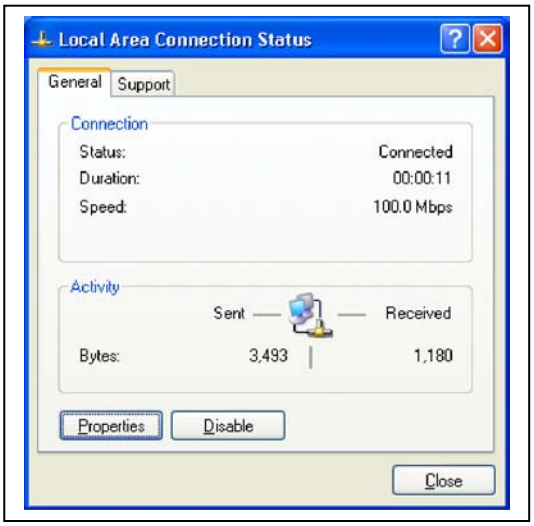
E. Returning the PC used to configure the WAP to DHCP control

1. Click **Start**.

2. Select **Control Panel**.
(For Windows 98SE, ME and 2000, select Settings first)

3. Double-click **Network and Dial-Up Connections.**
(Double Click Network for Windows 98SE and ME and the Network Window is displayed)

4. Double-click **Local Area Connection**. The Local Area Connection Status window appears (see *Figure 21*).
(*Step 5 is not applicable for Windows 98SE or ME*)



Connection

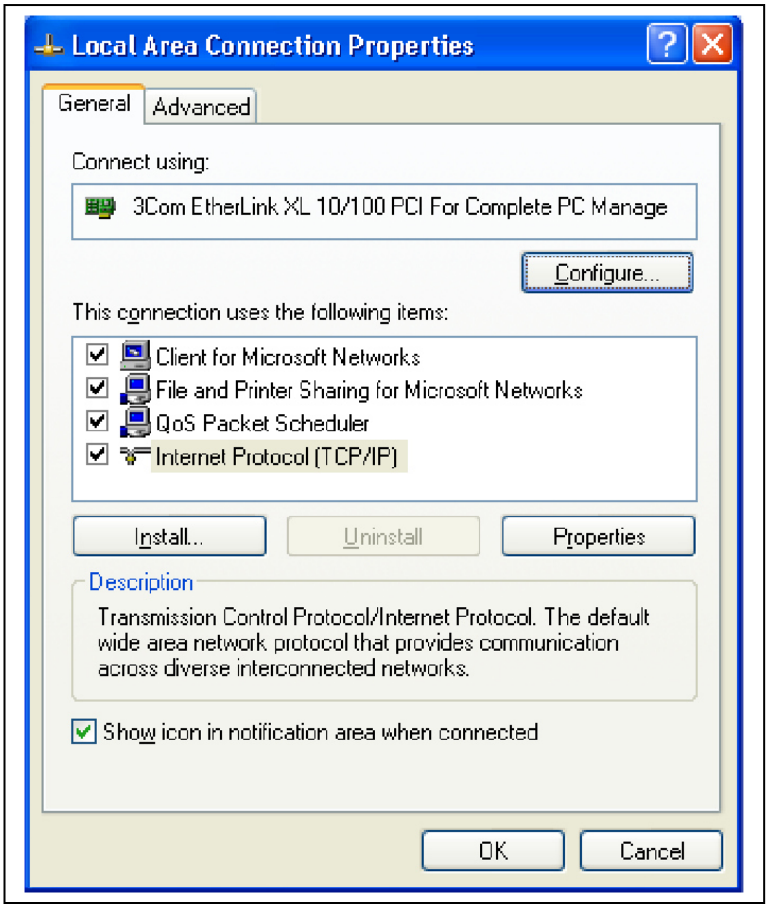
Status:	Connected
Duration:	00:00:11
Speed:	100.0 Mbps

Activity

	Sent	Received
Bytes:	3,493	1,180

Figure 21

5. Click the **Properties** button to go to the *Local Area Connection Properties* screen. (*Step 6 is not applicable for Windows 98SE or ME*)



Connect using:

3Com EtherLink XL 10/100 PCI For Complete PC Manage

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

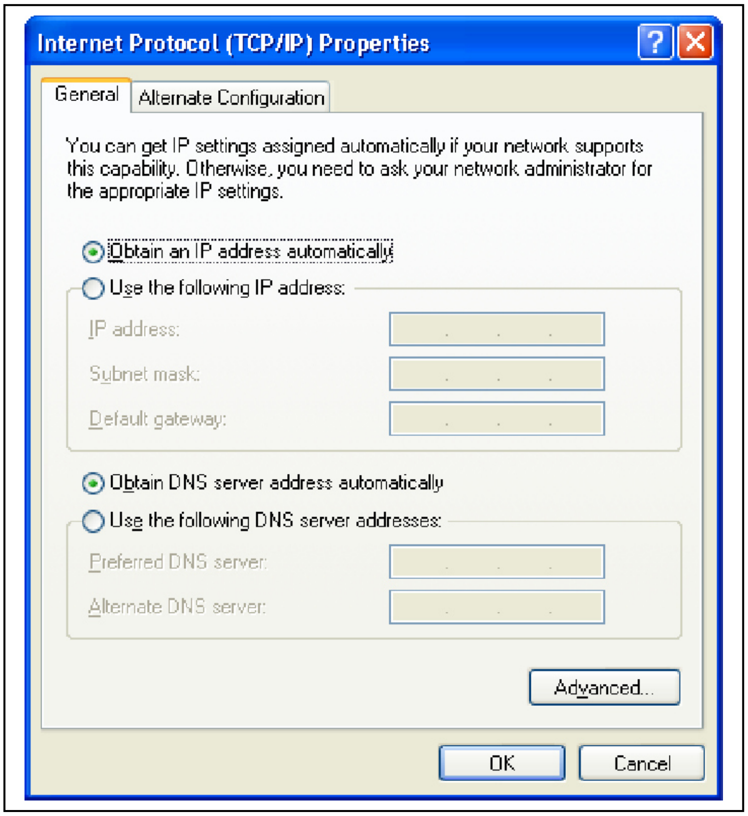
☑ Show icon in notification area when connected

Figure 22

6. Ensure the box next to *Internet Protocol (TCP/IP)* is selected (see *Figure 22*).

NOTE: Although this series of steps is used to re-configure the PC from direct WAP configuration back to its previous use as a DHCP controlled PC on the Router network, they can also be used to configure the WAP Network Interface Card for DHCP control by selecting the WAP NIC at the top of this screen.

7. Click to highlight **Internet Protocol** (**TCP/IP**) and click the **Properties** button to go to the *Internet Protocol (TCP/IP) Properties* screen.
(***For Windows 98SE or ME, from the Network Window's configuration tab, select the TCP/IP line the for the appropriate Ethernet adapter and Click Properties.*** From the TCP/IP Properties Window, Click on the IP Address tab.)



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Figure 23

8. Select Obtain an IP address automatically (see *Figure 23*).

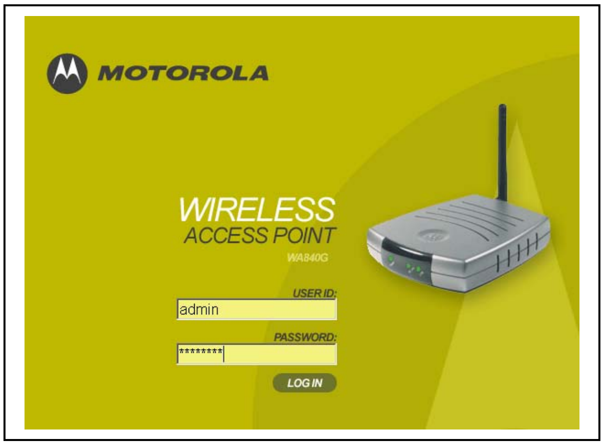
9. Click **OK** twice to exit and save your settings.
(***For Windows 98SE, ME, or 2000 you will have to restart the computer to save these settings).***

10. After the reboot (if appropriate), your PC should be now be ready for operation as before, directly through the Router, or through the WAP (if a Wireless NIC card was installed).

V. Configuration Utility Details

You can use the information in this section to modify the On-Q Wireless Access Point (WAP) 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. Once your PC is configured as part of the WAP's subnetwork (192.168.40.xxx), and you have used your browser to access the WAP at **http://192.168.40.1** (the WAP's default IP address), the login screen appears (see *Figure 24*).

NOTE: See *Section IV Initial Configuration Steps*, for initial configuration details.



USER ID: admin

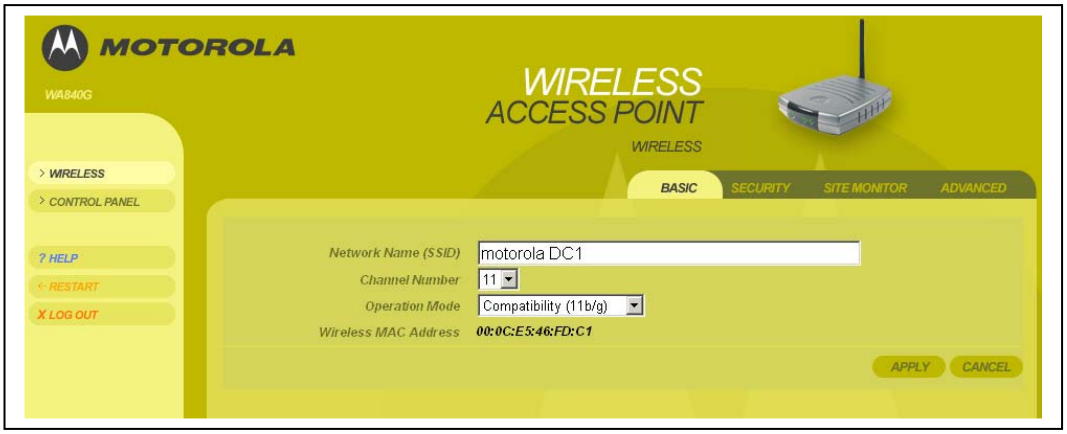
PASSWORD: ********

Figure 24

Enter the ***User ID***. The default factory setting is "admin", without the quotation marks. Enter the ***Password***. The default factory setting is "motorola", without the quotation marks. Click **Log In** to enter the WAP's **Configuration Utility**.

A. Navigation

The On-Q WAP Configuration Utility has two major sections (*Wireless* and *Control Panel* on the left, detailed in sections B. and C. below), each with sub-section tabs at top right (see *Figure 25*).



Network Name (SSID) motorola DC1

Channel Number 11

Operation Mode Compatibility (11b/g)

Wireless MAC Address 00:0C:E5:46:FD:C1

Figure 25

To navigate, click on a major section on the left and then the associated subsection (tab). For example, to adjust the **User Login ID**, click **CONTROL PANEL** on the left, then the **DEVICE SECURITY** tab at top on the right.

NOTE: This Configuration Utility uses Javascript. Your web browser's Javascript needs to be enabled.

Below the two major sections are three other selections, (*Help*, *Restart* and *Logout*). Click on the appropriate command to execute the associated action.

Help If assistance is required in using the WAP, click Help.

Restart To restart your session with the Configuration Utility, click Restart.

NOTE: 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.

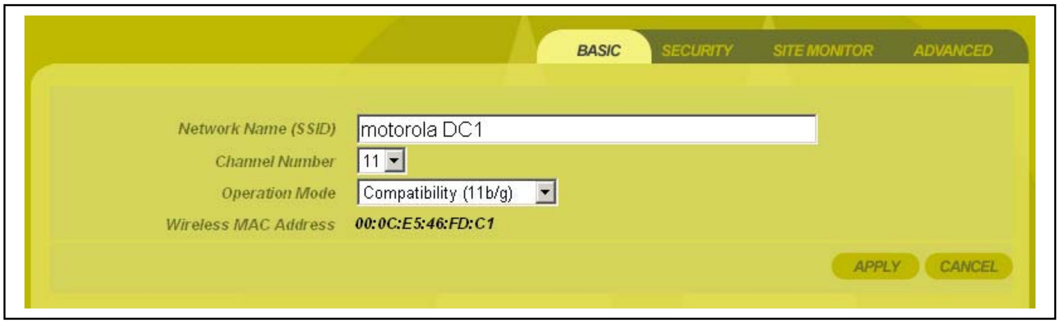
Logout To logout out of the WAP's Configuration Utility, click Logout.

B. Wireless Settings

The Wireless Network screens enable you to adjust settings for your wireless connection.

1. Basic Settings

This screen (see *Figure 26*) enables you to setup your Service Set Identifier (SSID) parameters for your network.



Network Name (SSID) motorola DC1
Channel Number 11
Operation Mode Compatibility (11b/g)
Wireless MAC Address 00:0C:E5:46:FD:C1

Figure 26

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

a. **Network Name (SSID)** - Enter a Network Name (SSID) of no more than 32 alphanumeric (case sensitive) characters. This SSID has to be entered and must be identical on every wireless device on your wireless network. The default SSID is "motorola" appended with the last three characters the unit's MAC address. It is recommended that you change this to a name easy for you to remember.

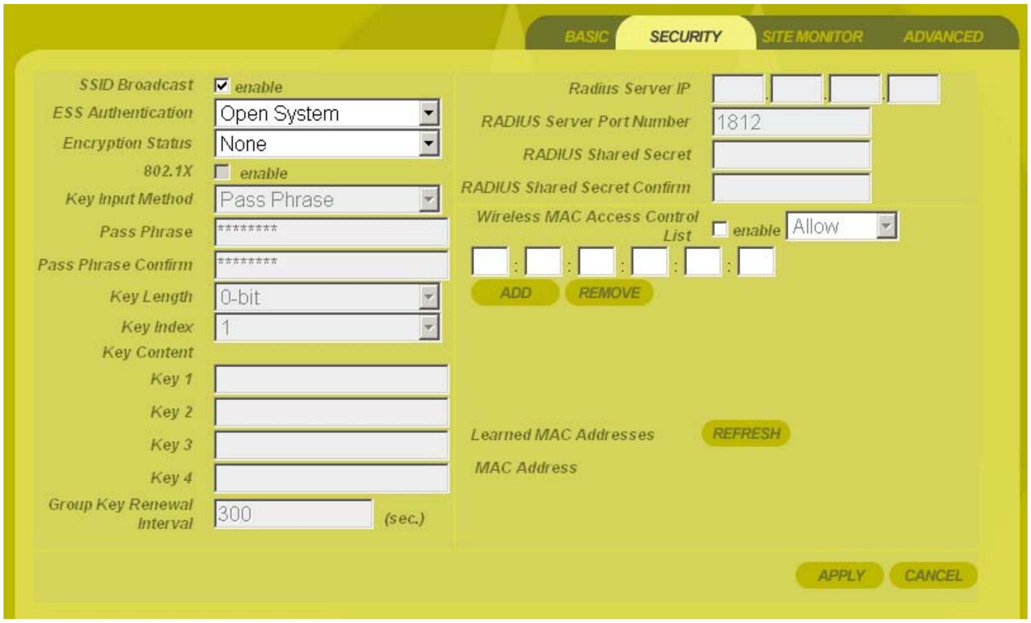
b. **Channel Number** - Identifies the channel on which the WAP communicates. Each wireless client must use the same channel to enable communication. This can only be altered from a PC that is wired directly to the WAP, not wirelessly. For an Ad-hoc network, select a channel to broadcast. The default is Channel 11.

c. **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)

d. **Wireless MAC Address** - Displays the MAC address of the unit.

2. **Security Settings**
This screen (see *Figure 27*) enables wireless security settings. Some fields activate other options. Refer to the descriptions for details.



SSID Broadcast ☑ enable
ESS Authentication: Open System
Encryption Status: None
802.1X □ enable
Key Input Method: Pass Phrase
Pass Phrase: ********
Pass Phrase Confirm: ********
Key Length: 0-bit
Key Index: 1
Key Content
Key 1
Key 2
Key 3
Key 4
Group Key Renewal Interval: 300 (sec.)
Radius Server IP
RADIUS Server Port Number: 1812
RADIUS Shared Secret
RADIUS Shared Secret Confirm
Wireless MAC Access Control List □ enable Allow
Learned MAC Addresses
MAC Address

Figure 27

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

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

b. **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 WAP. This setting does not encrypt your transmission.

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

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

c. **Encryption Status** - Determines the type of security encryption algorithms for the Key Index. This security setting encrypts your wireless transmission.

NOTE: None, WEP64, and WEP128 are available only when Open System or Pre-Shared KEY (PSK) is selected. TKIP and AES are available only when WPA and WPA-PSK are selected.

The options are:
None - No security
WEP64 (Wired Equivalent Privacy 64-bit strength) - (provides 4 Keys)
WEP128 (Wired Equivalent Privacy 128-bit strength) - (provides 2 Keys)
TKIP (Temporal Key Integrity Protocol) - changes the temporal key often (provides 1 Key)
AES (Advanced Encryption Standard) - (provides 1 Key)

Select the option that best matches your needs. AES (which requires WPA or WPA-PSK selected) is recommended when the strongest security algorithm is desired. The default is None.

d. **802.1X mode** - Can only be enabled when the ESS Authorization is set to Open or PSK and either WEP64 or WEP128 is selected (see the Encryption Status field). During the Authentication process, the server verifies the identity of the client attempting to connect to the network. When WPA-PSK is selected in the ESS Authentication field, this option is automatically selected.

If not already enabled, select to activate this feature. When enabled, Dynamic Key generation occurs. That is, when the client requests a key, this function dynamically generates one. The default is disabled.

e. **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.

NOTE: If you are using other non-Motorola wireless products and a security algorithm other than WPA-PSK, you must enter your WEP keys manually in hexadecimal format for the non-Motorola wireless products.

Select the option that best matches your needs. The default is Pass Phrase.

f. **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.

g. **Key Length** - Only available when ESS Authentication is set PSK and the Encryption Status is set to None. The option selected determines the strength of the key. There are two options:
128-bit
64-bit.

Select the option that best matches your needs.

h. **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 Encryption Authentication and Encryption Status field. You are selecting one of the Key Content fields below. The Key selected here must match between the WAP 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.

i. **Key Content (Key 1, Key 2, Key 3 and 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).

NOTE: If entering a key manually, don't leave a key field blank or enter all 0.s. These are not secure keys.

j. **Group Key Renewal Interval** - Only available if ESS Authentication is set to WPA. This is the number of seconds that pass until your WAP sends out a new group key. Enter in the option that best matches your needs. The default is 300 seconds.

k. **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 these conditions need to exist:
Open System is selected, along with either WEP64 or WEP128, and 802.1X is enabled
WPA is selected and TKIP or AES is selected.

Enter the RADIUS Server IP and Port number. The default RADIUS Port Number is 1812.

l. **RADIUS Shared Secret / RADIUS Shared Secret Confirmation** - A password that is entered twice for confirmation.

m. **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 WAP.
Allow - Allows only the wireless devices in the ACL to communicate with the WAP.
Deny - Denies wireless devices in the ACL from communicating with the WAP.

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

To edit a MAC address:
1 Remove and replace with the updated address.
2 Click **APPLY** to save.

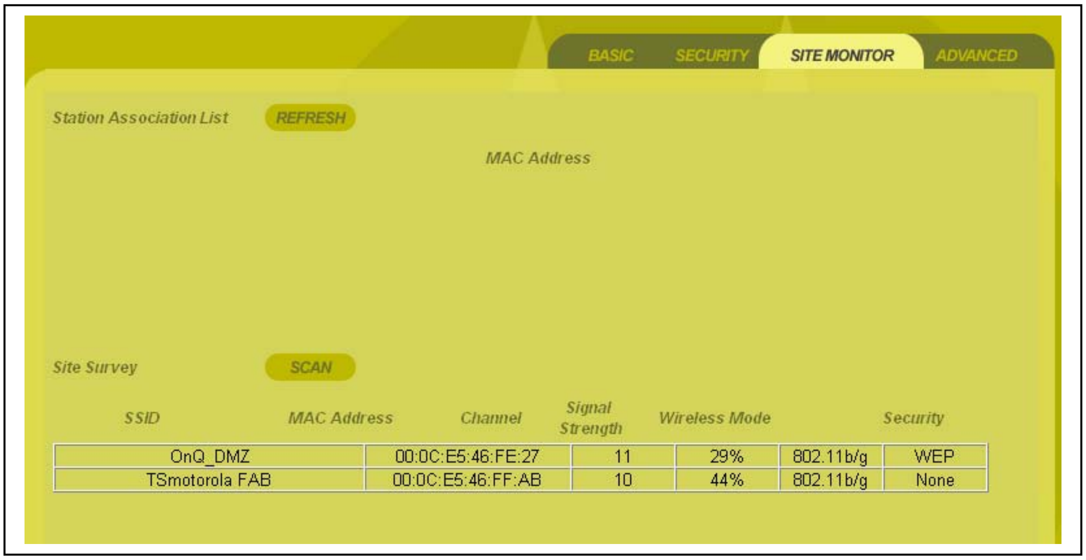
To delete a MAC address:
1 Click into the MAC address you wish to delete. Once activated, the field will change color.
2 Click **REMOVE** to clear the address.
3 Click **APPLY** to save.

3. **Site Monitor**

This screen (see *Figure 28*) displays information about Wireless Access Points (WAPs) and stations, and their associated information:

Station Association List - Identifies only those stations that are connected to your WAP.

Site Survey - Reveals information about other WAPs in the area.



SSID	MAC Address	Channel	Signal Strength	Wireless Mode	Security
OnQ_DMZ	00:0C:E5:46:FE:27	11	29%	802.11b/g	WEP
TSmotorola FAB	00:0C:E5:46:FF:AB	10	44%	802.11b/g	None

Figure 28

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

a. **Station Association List -**

MAC Address - Displays the MAC address of the client.

Host Name - Displays the name of the device attached.

b. **Site Survey**

Scan - Click to search for more WAPs or clients.

SSID - Displays the SSID of the device found.

MAC Address - Displays the MAC address of the device found.

Channel - Displays the channel upon which the device is broadcasting.

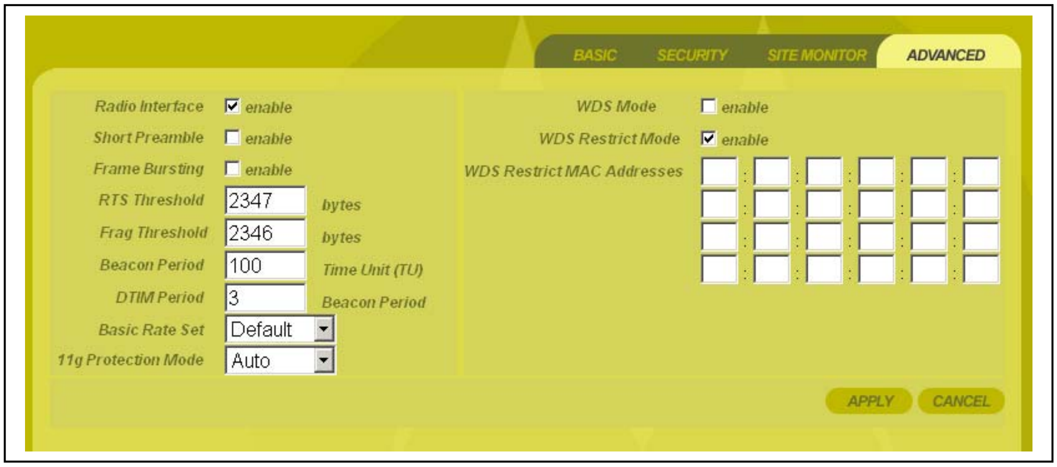
Signal Strength - Displays the Signal Strength of the device found.

Wireless Mode - Displays which protocol is used, 802.11b or 802.11g.

Security - Displays the security protocol used.

4. Advanced Settings

This screen (see *Figure 29*) enables you to turn on and off your wireless network and adjust wireless parameters. Generally, the settings here should remain at their default values.



Radio Interface ☑ enable
Short Preamble ☐ enable
Frame Bursting ☐ enable
RTS Threshold 2347 bytes
Frag Threshold 2346 bytes
Beacon Period 100 Time Unit (TU)
DTIM Period 3 Beacon Period
Basic Rate Set Default
11g Protection Mode Auto
WDS Mode ☐ enable
WDS Restrict Mode ☑ enable
WDS Restrict MAC Addresses

Figure 29

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

a. **Radio Interface** - Enables you to turn on and off the wireless feature. The default is enabled.

b. **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.

c. **RTS Threshold** - The packet size at which a WAP issues a request to send (RTS). The range is 0 to 2347 bytes. The default is 2347. If you encounter inconsistent data flow, only minor modifications are recommended. If needed, enter a new value.

d. **Fragmentation Threshold** - The size at which packets are fragmented and transmitted a piece at a time instead of all at once. The setting must be within the range of 256 to 2346 bytes. The default is 2346. If needed, enter a new value.

e. **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 WAP to keep the network synchronized. You are able to set the Beacon Period value from 1 to 65535 in Time Units (TU). The default is 100. If needed, enter a new value.

f. **DTIM Period** - You are able to set the Delivery Traffic Indicator Maps (DTIM) period value from 1 to 255 in multiples of Beacon Periods. The default is 3. If needed, enter a new value.

g. **Basic Rate Set** - The WAP 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.

h. **11g Protection Mode** - Ensures that your WAP does not interfere with neighbor networks. 802.11b networks cannot hear 802.11g networks, but 802.11g networks can hear 802.11b networks. The Protection Mode improves performance when 802.11b and 802.11g stations coexist in the network. The default is Auto. The options are:
Disable - 802.11g Protection Mode is never used.
Auto - 802.11g Protection Mode is used if either an 802.11b client joins the network or the WAP detects an 802.11b network on the same channel

i. **WDS Mode** - Wireless Distribution System (WDS) enables you to share and expand your network with other WAPs. The WDS fields, WDS Restrict Mode and WDS Restrict MAC address, become active once WDS is enabled. When enabled, any WAP can connect if using your settings. The default is disabled.

j. **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 WAPs you designate. The default is enabled.

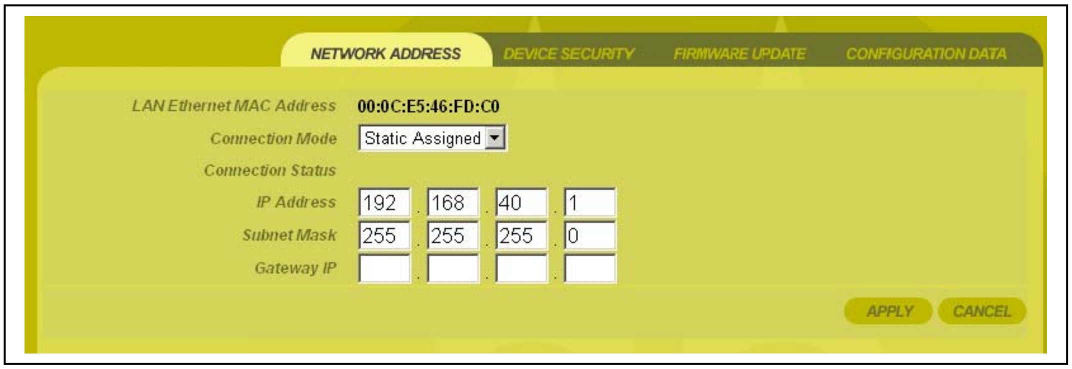
k. **WDS Restrict MAC address** -
1 Enter up to four WAP MAC addresses.
2 To edit an entry, highlight the number and change.
3 To delete a number, delete each field.

C. Control Panel

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

1. Network Access

This screen (see *Figure 30*) enables you to change your Connection Mode and IP settings.



LAN Ethernet MAC Address 00:0C:E5:46:FD:C0
Connection Mode Static Assigned
Connection Status
IP Address 192 . 168 . 40 . 1
Subnet Mask 255 . 255 . 255 . 0
Gateway IP . . .

Figure 30

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

a. **LAN Ethernet MAC Address** - Displays the unit's MAC address.

b. **Connection Mode** - The WAP supports two connection modes:
Cable Modem (DHCP)
Static Assigned

Select the appropriate connection method for your ISP (Internet Service Provider). Based on which connection type you select, different areas are grayed out (become inaccessible), leaving you only the appropriate fields to fill in. For details on each Connection Mode type, refer to *Section 2:Installation.*

c. **Connection Status** - Provides current information about the connection status of the WAP.

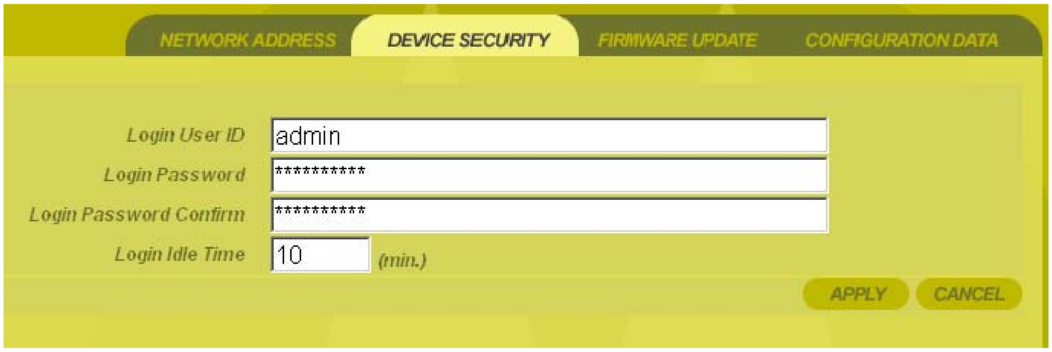
d. **IP Address** - The WAP's IP Address used to connect to your ISP or router. It is either automatically displayed or manually entered from information provided by the provider.

If DHCP is selected, this is the IP Address that your WAP is currently using to access the Internet. If using Static Assigned, then you would enter the IP Address here.

e. **Subnet Mask** - Is either automatically displayed or manually entered from information provided by your ISP.

f. **Gateway IP** - Is either automatically displayed or manually entered from information provided by your ISP.

2. Device Security
This screen (see *Figure 31*) enables you to change your User ID and password and enables you to manage your WAP remotely.



Login User ID: admin
Login Password: ***********
Login Password Confirm: ***********
Login Idle Time: 10 (min.)

Figure 31

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

a. **Login User ID** - Changes the User ID used for logging into the WAP's web-based utility. It cannot be longer than 63 bytes. A blank user name is not allowed. The default is "admin".

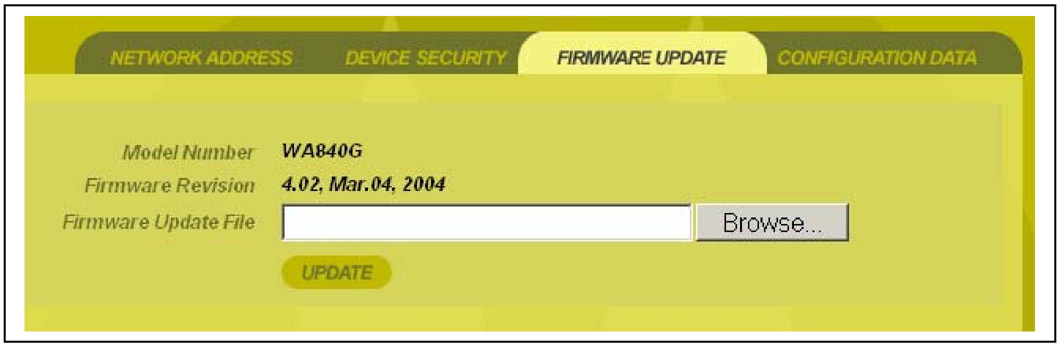
b. **Login Password** - Use this option to change the Password, used to log into the WAP's web based utility. It cannot be longer than 63 bytes. A blank password is not allowed. The default is "motorola".

c. **Login Password Confirm** - Re-enter the User Password.

d. **Login Idle Time** - The amount of idle time (no actions occur) that elapses before the WAP automatically logs you off. The default is 10 minutes.

3. **Firmware Update**
This screen (see *Figure 32*) enables you to update the firmware (WAP'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 the On-Q Home website at www.onqhome.com for the latest firmware.



Model Number WA840G
Firmware Revision 4.02, Mar.04, 2004
Firmware Update File

Figure 32

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

To update the firmware:

a. Download the latest file to your computer.

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

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

d. Follow the prompts for restarting.

4. **Configuration Data (also Reset to Factory Default)**
This screen (see *Figure 33*) enables you to save and restore the settings, that you have currently configured for your WAP, to a file. You are also able to reset the WAP to the factory default settings.

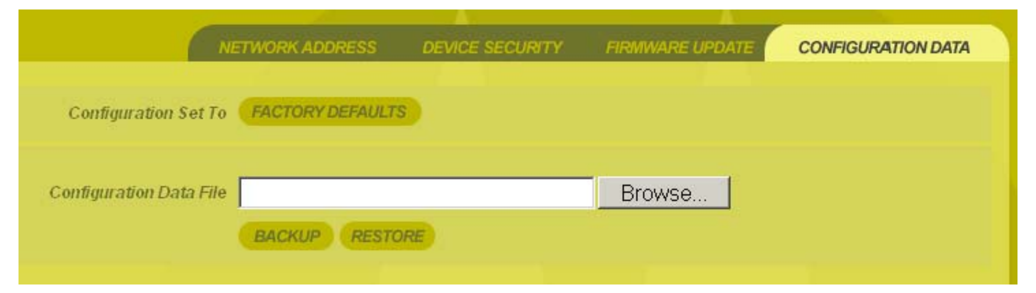


Figure 33

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

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

To backup your settings:

a. Click **BACKUP**.
b. From the pop up window, choose the destination for the file.
c. Enter a descriptive file name.

To restore your settings:

d. Locate the Configuration file on your computer by entering the path to the file or click **Browse** and navigate to it.
e. Click **RESTORE** to reapply the saved settings with the selected file.

VI. Troubleshooting

This section will detail possible solutions to common problems that might occur in using the On-Q Wireless Access Point (WAP).

A. Contact Information

If you are unable to locate a solution here, please access our website at www.onqhome.com for the latest information. You can also reach us at 1-800-321-2343.

B. Hardware Situations

Some of the steps in this section may require removal of the WAP cover, or the WAP Assembly unit to verify cabling. Use a small pointed object, like a paper clip to remove the WAP cover by gently prying in the slot near the Power indicator (see *Figure 21).*

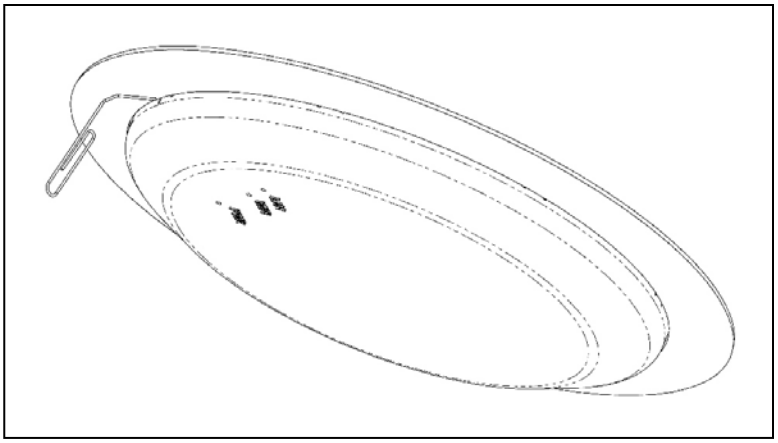


Figure 21

The WAP Assembly itself is removed by pressing the mounting ring clasp extensions toward each other (see *Figure 22 and Figure 23*) and carefully pulling the WAP Assembly out of the Mounting Ring.

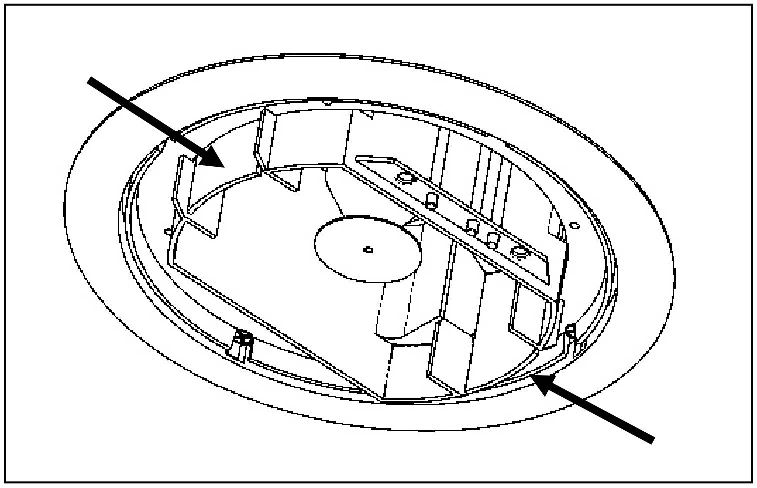


Figure 22

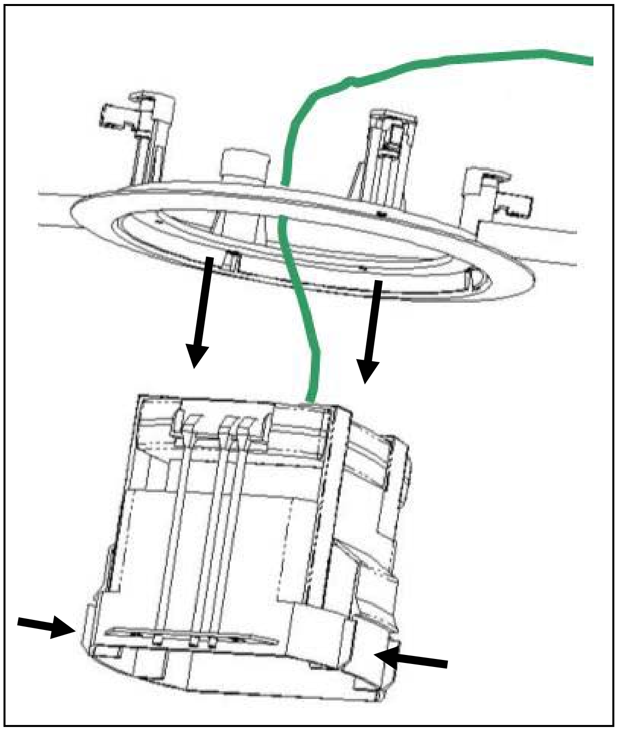


Figure 23

When the WAP has been removed from the mounting ring, the following connections can be verified (see *Figure 24*):

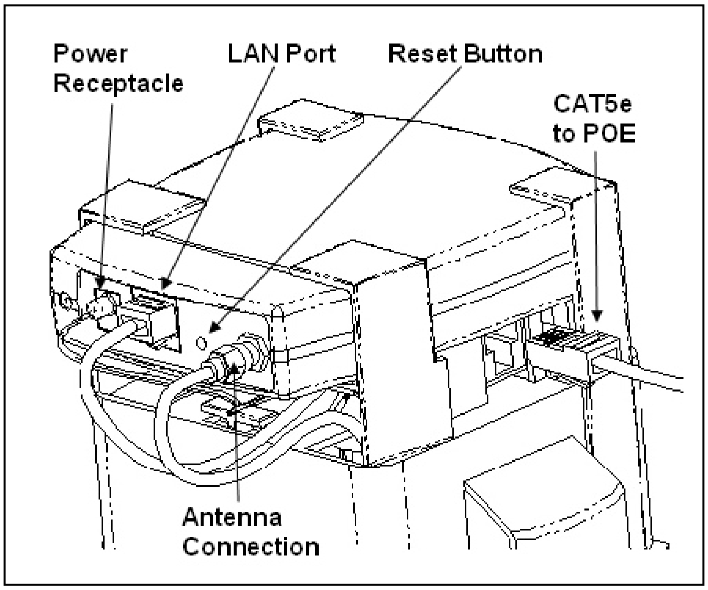


Figure 24

Power Receptacle – Five volt DC power is extracted from the POE Extractor Module in the WAP Assembly (the 5VDC is derived from the 48VDC fed to the WAP Assembly over the single CAT5e from the POE Inserter Module in the Enclosure).

LAN Port – Ethernet data is extracted from the POE Extractor Module in the WAP Assembly. The LAN port supports either 10BASE-T or 100BASE-T transmission speeds as well as straight-through and crossover Ethernet cables (the Ethernet data is derived from the single CAT5e fed to the WAP Assembly from the POE Inserter Module in the Enclosure).

Reset Button - A dual-function button. A brief button press resets the WAP unit, while a longer button press resets the WAP unit to the default login settings. If the WAP is experiencing trouble connecting to the Internet, briefly press and release the Reset button to reset the WAP. The WAP will retain its configuration information during this reset operation. To reset the unit to the factory defaults, while the unit is powered, press and hold the Reset button for more than 10 seconds. This clears the WAP's user settings, including User ID, Password, IP Address, and Subnet Mask.

NOTE: Refer to the *Section IV Initial Configuration Steps* for re-configuring the WAP.

Antenna Connection – Cable connects to the On-Q WAP antenna used for wireless connections.

NOTE: When initially removed from the box, a stub antenna will be connected to this connector. For better coverage, it should be removed and replaced by the On-Q WAP antenna cable.

After connections have been verified, or the unit has been reset, insure the CAT5e cable from the POE Inserter Module is connected, and push the unit through the mounting ring until the Mounting Ring Clasps snap into place (see *Figure 25*).

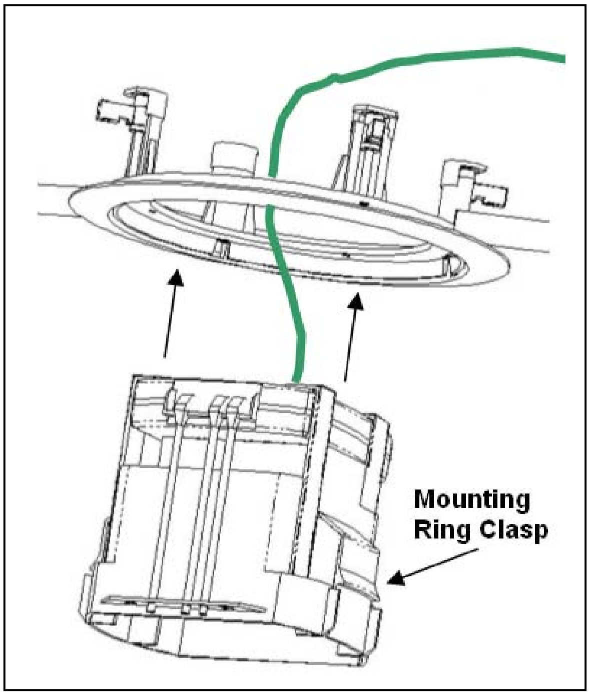


Figure 25

Then install the center cover, making sure the tabs in the cover line up with the holes on the WAP Assembly. This will insure that the light pipes from the status lights on the WAP are properly aligned (see *Figure 26*).

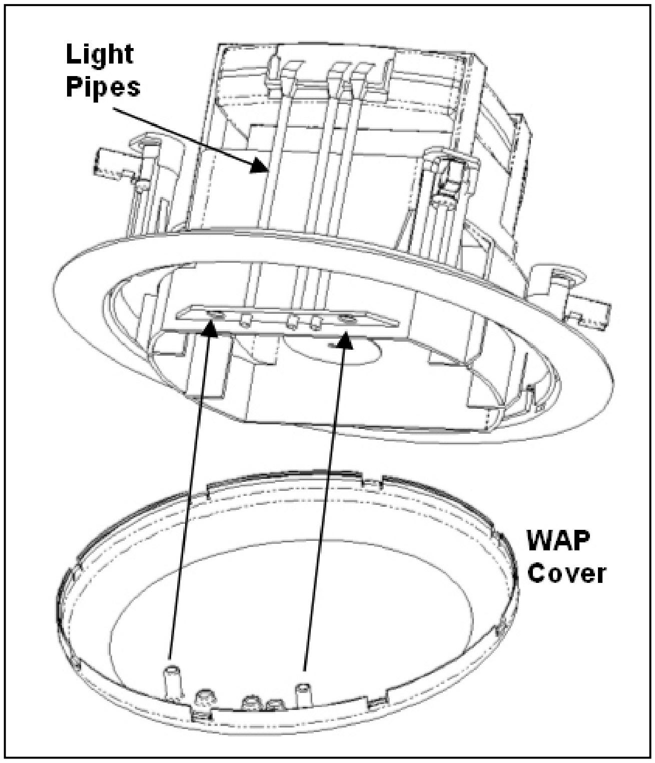


Figure 26

1. **My computer is experiencing difficulty connecting to the wireless network.**
   a. Ensure that your Wireless Access Point (WAP) is powered on and that the Wireless LED is lit.
   b. Ensure that your wireless adapter (PCI card, Notebook or Ethernet adapter) is installed correctly and is active.
   c. Ensure that your wireless adapter's radio signal is enabled and set to the same channel on which the WAP is communicating. Review your adapter's documentation for further instructions.
   d. Ensure that your wireless adapter for your PC and the WAP have the same security settings that will allow your computer to access the wireless network. Section 3: Wireless > Security details how to adjust security settings.
   e. Ensure that your WAP is within range of your router or is not behind an obstruction, for example metal structures will interfere with the signal, as will 2.4 GHz cordless phones, and microwaves.
   f. Ensure that your antenna is connected.

2. **My computer is experiencing difficulty in connecting to the WAP.**
   a. Check that all of your cable connections are tight and secured. This includes the cables to your modem, the router, the WAP and to your PC.
   b. Ensure that your LEDs are not lit Red or not at all. For further information about LED descriptions, see *Section II: Product Overview.*
   c. Ensure that you are using Ethernet cables and not telephone cables (see *Figure 31*). Ethernet cables use a wider RJ-45 style plug using 8 wires where telephone style plugs use the smaller RJ-11 (4 pin) or RJ-25 (6 pin) style plugs.

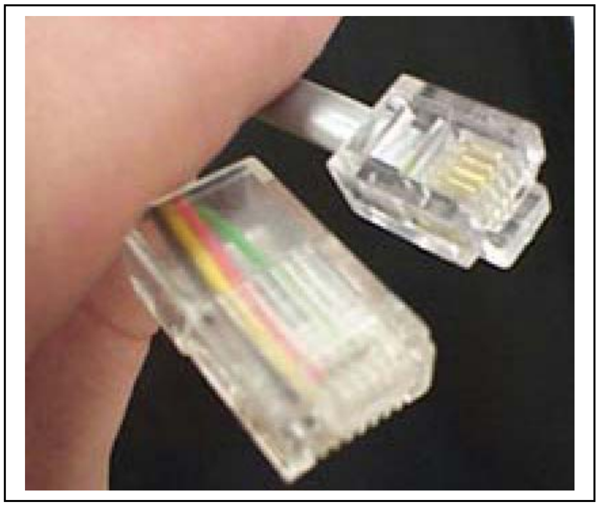


Figure 31

NOTE: The plug on the left is RJ-45; the plug on the right is RJ-11. Use only RJ-45.

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

C. Software Situations

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

a. 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 III: Configuration > Configure Your Computers, for further details.

b. 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**.)*

c. In the Command window, type **ipconfig**.
You should see an IP address for your network adapter similar to the following example:

```
IP Address. . . . . . . . . . . . : 192.168.40.3
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.40.1
```

d. In the *Command* window, type **ping** followed by the WAP's ***IP address*** and press **Enter**. For example type: **ping 192.168.40.3**.
There is a good possibility that the Default Gateway's IP address is the WAP's IP address. You can verify the WAP's IP address on the Control Panel > Network Access screen.
If you receive a reply (the first word will be *Reply*.), then your computer is connected to the WAP. Proceed to *Step e*.
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.

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

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

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

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

2. **I cannot access the Web-Based Configuration Utility for the WAP.**
   a. Verify your Ethernet connection to the WAP.
   b. Verify that the IP address of the PC being used to configure the WAP is on the same network as the WAP's configuration IP address.
   c. The IP address of your network adapter must be on the same network and not a duplicate of any others on the network (for example: 192.168.40.3 and using a subnet mask of 255.255.255.0 can be used to login to the WAP's default IP address of 192.168.40.1). Refer to Section III: Configuration > Configure Your Computers on how to adjust the IP address for your PC.
   d. Verify that you can ping the WAP on this IP address. In the *Command* window, type **ping** and your WAP's default ***IP address*** and press **Enter**. For example type: **ping 192.168.40.3.**
   e. If you have changed the factory configured default IP address of the WAP, you will need to set your network adapter accordingly.
   f. Verify you are entering the correct URL in the browser. The default is http://192.168.40.1.
   g. If you think you have changed the IP address used to configure the WAP 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 WAP's user settings, including User ID, Password, IP Address, and Subnet mask.
   h. Once the WAP is reset to factory default, re-verify the Ethernet connectivity and IP address issues.
   i. Verify you are using the latest version of IE or Netscape. IE 5.2 and below are not supported.

VII. Glossary

A

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

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

Address translation
See *NAT*.

Ad-Hoc Network
A temporary local area network connecting WAP clients together, usually just for the duration of the communication session. The clients communicate directly to each other and not through an established link, 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 Wireless 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 wireless access point. Also called a CPE. A wireless client is also called a .station.. Also see *server.*

Coaxial Cable
A type of cable consisting of a center wire surrounded by insulation and a grounded shield of braided wire. The shield minimizes electrical and radio frequency interference. Coaxial cable has high bandwidth and can support transmission over long distances.

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

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

D

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

DHCP
A Dynamic Host Configuration Protocol server dynamically assigns IP addresses to client hosts on an IP network. DHCP eliminates the need to manually assign static IP addresses by "leasing" an IP address and subnet mask to each client. It enables the automatic reuse of unused IP addresses.

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

DNS
The Domain Name System is the Internet system for converting domain names (like www.onqhome.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 onqhome.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, and many others.

DSL
Digital Subscriber Line

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

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

E

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

Ethernet
The most widely used LAN type, also known as IEEE 802.3. The most common Ethernet networks are 10Base-T, which provide transmission speeds up to 10 Mbps, usually over unshielded, twisted-pair wire terminated with RJ-45 connectors. Fast Ethernet (100Base-T) provides speeds up to 100 Mbps. .Base. means .baseband technology. and .T. means .twisted pair cable. Each Ethernet port has a physical address called the MAC address. Also see *MAC address*.

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

F

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

FTP
File Transfer Protocol is a standard Internet protocol for exchanging files between computers. FTP is commonly used to download programs and other files to a computer from web pages on Internet servers.

G

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

GUI
Graphical User Interface

H

Hexadecimal
A base-sixteen numbering system that uses sixteen sequential numbers (0 to 9 and the letters A to F) as base units before adding a new position. On computers, hexadecimal is a convenient way to express binary numbers.

Host
In IP, a host is any computer supporting end-user applications or services with full two-way network access. Each host has a unique host number that combined with the network number forms its IP address. Host also can mean: A computer running a web server that serves pages for one or more web sites belonging to organization(s) or individuals; A company that provides this service; or 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 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 Inter-Net Groper.

POE

Power Over Ethernet

A technique used to supply low voltage operating power to devices connected with a twisted pair CAT5e Ethernet interface cable.

Port Triggering

A mechanism that allows incoming communication with specified applications.

PPP

Point-to-Point Protocol is used to transport other protocols, typically for simple links over serial lines. It is most commonly used to access the Internet with a dial-up modem.

PPPoE

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

PPTP

Point-to-Point Tunneling Protocol encapsulates other protocols. It is a new technology to create VPNs developed jointly by several vendors.

Private IP Address

An IP address assigned to a computer on a LAN by the DHCP server for a specified lease time. Private IP addresses are invisible to devices on the Internet. See also *Public IP Address*.

Protocol
A formal set of rules and conventions for exchanging data. Different computer types (for example PC, UNIX, or mainframe) can communicate if they support common protocols.

Public IP Address
The IP address assigned to the router or WAP 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 WAP to another WAP seamlessly.

ROM
Read-Only Memory.

Router
On IP networks, a device connecting at least two networks, which may or may not be similar. A router is typically located at a gateway between networks. A router operates on OSI network layer 3. It filters packets based on the IP address, examining the source and destination IP addresses to determine the best route on which to forward them. A router is often included as part of a network switch. A router can also be implemented as software on a computer.

Routing Table
A table listing available routes that is used by a router to determine the best route for a packet.

RTS
Request To Send.

S

Server
In a client/server architecture, a dedicated computer that supplies files or services such as file transfer, remote login, or printing to clients. Also see *client.*

Service Provider
A company providing Internet connection services to subscribers.

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

Static IP Address
An IP address that is permanently assigned to a host. Normally, a static IP address must be assigned manually. The opposite of *Dynamic IP Address.*

Station
IEEE 802.11b term for wireless client.

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

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

Switch
On an Ethernet network, a switch filters frames based on the MAC address, in a manner similar to a bridge. A switch is more advanced because it can connect more than two segments.

T

TCP
Transmission Control Protocol on OSI transport layer four, provides reliable transport over the network for data transmitted using IP (network layer three). It is an end-to-end protocol defining rules and procedures for data exchange between hosts on top of connectionless IP. TCP uses a timer to track outstanding packets, checks error in incoming packets, and retransmits packets if requested.

TCP/IP
The Transmission Control Protocol/Internet Protocol suite provides standards and rules for data communication between networks on the Internet. It is the worldwide Internetworking standard and the basic communications protocol of the Internet.

Tunnel
To place packets inside other packets to send over a network. The protocol of the enclosing packet is understood by each endpoint, or tunnel interface, where the packet enters and exits the network. VPNs rely on tunneling to create a secure network. Tunneling requires the following protocol types: A carrier protocol, such as TCP, used by the network that the data travels over; An encapsulating protocol, such as IPSec, L2F, L2TP, or PPTP, that is wrapped around the original data; and A passenger protocol, such as IP, for the original data

U

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

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

USB
Universal Serial Bus is a computer interface for add-on devices such as printers, scanners, mice, modems, or keyboards. USB 1.1 supports data transfer rates of 12 Mbps and plug-and-play installation. You can connect up to 127 devices to a single USB port. USB 2.0 supports data rates of 480 Mbps.

V

VoIP
Voice over Internet Protocol is a method to exchange voice, fax, and other information over the Internet. Voice and fax have traditionally been carried over traditional telephone lines of the Public Switched Telephone Network (PSTN) using a dedicated circuit for each line. VoIP enables calls to travel as discrete data packets on shared lines. VoIP is an important part of the convergence of computers, telephones, and television into a single integrated information network.

VPN
A virtual private network is a private network that uses "virtual" connections (tunnels) routed over a public network (usually the Internet) to provide a secure and fast connection; usually to users working remotely at home or in small branch offices. A VPN connection provides security and performance similar to a dedicated link (for example, a leased line), but at much lower cost.

W

WAN
A wide-area network provides a connection over a large geographic area, such as a country or the whole world. The bandwidth depends on need and cost, but is usually much lower than for a LAN.

WAP
Wireless Access Point or Wireless Access Protocol. See also *Access Point*.

WEP
Wired Equivalent Privacy encryption protects the privacy of data transmitted over a wireless LAN. WEP uses keys to encrypt and decrypt transmitted data. The access point must authenticate a client before it can transfer data to another client. WEP is part of IEEE 802.11b.

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

WLAN
Wireless LAN.

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

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